Topic no 106: CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

1. Limit registration by extensions to your local subnet.

- Restrict the IP addresses your extensions can register onto the local subnet. Asterisk PBXs can use the ACL (permit/deny) in SIP.conf to block IP addresses. This can fend off brute force registration attempts.

2. Disable channels and services that are not in use

- Disable channels that you aren't using like skinny and MGCP. For Asterisk PBXs, you can "unload" these modules in the /etc/modules.conf file

3. Make it harder for sip scanners (Set "alwaysauthreject=yes")

- Set "alwaysauthreject=yes" in your sip configuration file. What this does is prevent Asterisk from telling a sip scanner which extensions are valid by rejecting authentication requests on existing usernames with the same rejection details as with nonexistent usernames. If they can't find you they can't hack you!

- Another way to make it hard for SIP scanners is to install a SIP port firewall. This will block "scanning" of port 5060 and 5061 and can disable the attempting endpoint for a specific time when it detects a violation.

4. Limit and restrict routing and phone number dial plans

- Restrict calling to high-cost calling destination and don't allow calling to 0900 + Premium numbers)

5. Audit your system security regularly

Topic no 107: Version Control For IT Assets

- Benefits of version control
- Security implications

• Benefits of version control

- http://its.unl.edu/bestpractices/version-management

1. Organized, coordinated management of changes to software assets by one or many individuals, some of whom may be geographically dispersed
2. Organized, coordinated management of changes to software assets for emergency hot-fixes, routine maintenance, upgrades …& new features with potentially overlapping dev timeframes (e.g., work on new features occurs simultaneously with work on routine maintenance and/or hot-

fixes)

3. An auditable change history (e.g., what changed, when, and by whom)
4. A reliable master copy of what assets are currently in production
5. A reliable master copy of assets from which to build and/or configure the production environment
6. Reliable copies of previous production versions of assets
7. Ability to see the specific differences between distinct versions of a given asset

- Security controls:
  - Access control measures
  - Privileged management
  - Backups

Topic no 108: Version Control Best Practices

- **Version control best practices**
  - https://intland.com/blog/sdlc/source-control-management-best-practices/

1. Starting with the basics, choose a source control system.
2. Keep your source code in source control (but not files generated / compiled from it).
3. Ensure the working file is from the latest version of the source file.
4. Only Check-out the file being worked upon.
5. Check in immediately after alterations are completed.
6. Review every change before committing, utilize the diff function!
7. Commit often, – every commit provides a rollback position.
8. Make extensive, – detailed notes in the check-in comments about why the changes were made.
9. Developers must commit their own changes (only).
10. Use the ignore button for files that should not be committed, consider adding pre-commit filters to prevent the wrong kinds of file (such as accidental check-in of personal user settings docs) from entering the source control
11. Ensure external dependencies are added to the source control, a common problem where everything works great on the contributing developers system but not elsewhere because they forgot to add

dependent files to the system.

Topic no 109: SECURITY HARDENING - SECURE SOFTWARE IMAGES

- CIS 20 CRITICAL SECURITY CONTROLS
- CONTROL 5, VERSION 7
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish Secure Configurations

- Maintain documented, standard security configuration standards for all authorized operating systems and software.

Maintain Secure Images

- Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.

Securely Store Master Images

- Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

Deploy System Configuration Management Tools

- Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

Implement Automated Configuration Monitoring Systems

- Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

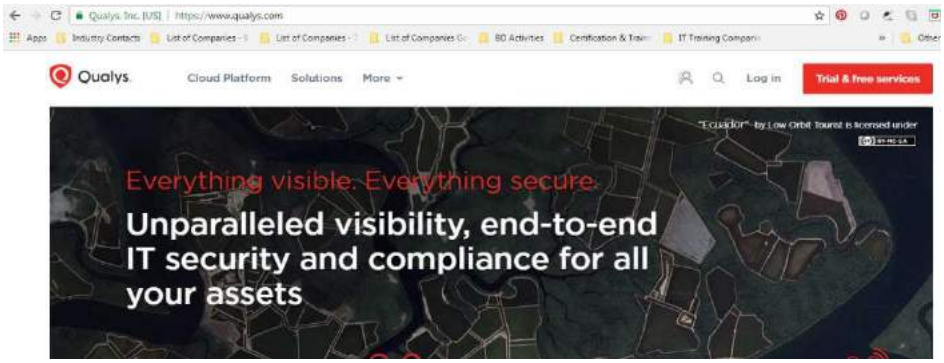
Topic no 110: SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Manual & Automated mechanisms for security hardening & validation
- **Step 1:** Scan an IT asset using Qualys compliance scan, NESSUS compliance scan, or CIS CAT PRO Tool
    - Acquire report of failed controls

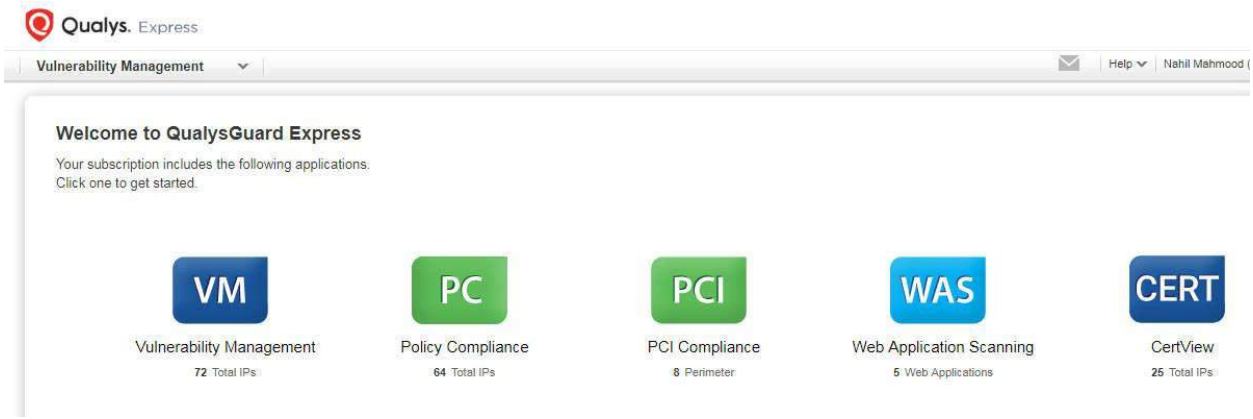
- **Step 2:** Apply the failed controls using AD (for Windows) or manually for other systems & devices
- **Step 3:** Use the automated feature of Qualys compliance scan, Nessus compliance scan or CIS CAT Pro Tool to verify that the applied controls are in place
  - Compare the ‘before’ and ‘after’ report
- **Step 4:** Manually verify if any discrepancy is found (control should be in place but not being validated by the tool)
- **Step 5:** For any system or device for which the Qualys compliance scan, Nessus compliance scan, or CIS CAT Pro Tool scan cannot be performed, conduct the validation of control implementation manually
  - Use sampling where necessary during manual validation work to reduce workload
  - For example, 15-20 % of assets may be checked at random
  - Or 15-20% of controls may be checked on an asset

Topic no 111 & 112 : QUALYS DEMO – SECURITY HARDENING

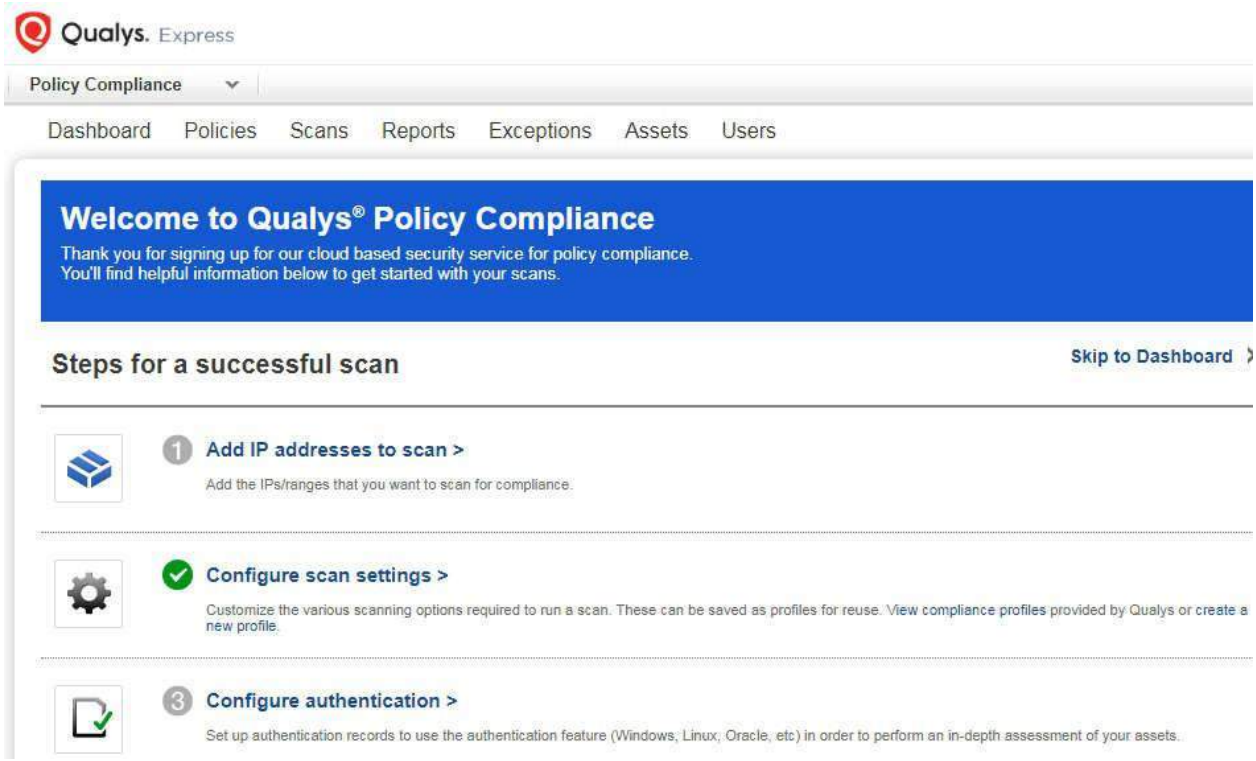
- Lets have a look at how Qualys can aid in the security hardening process



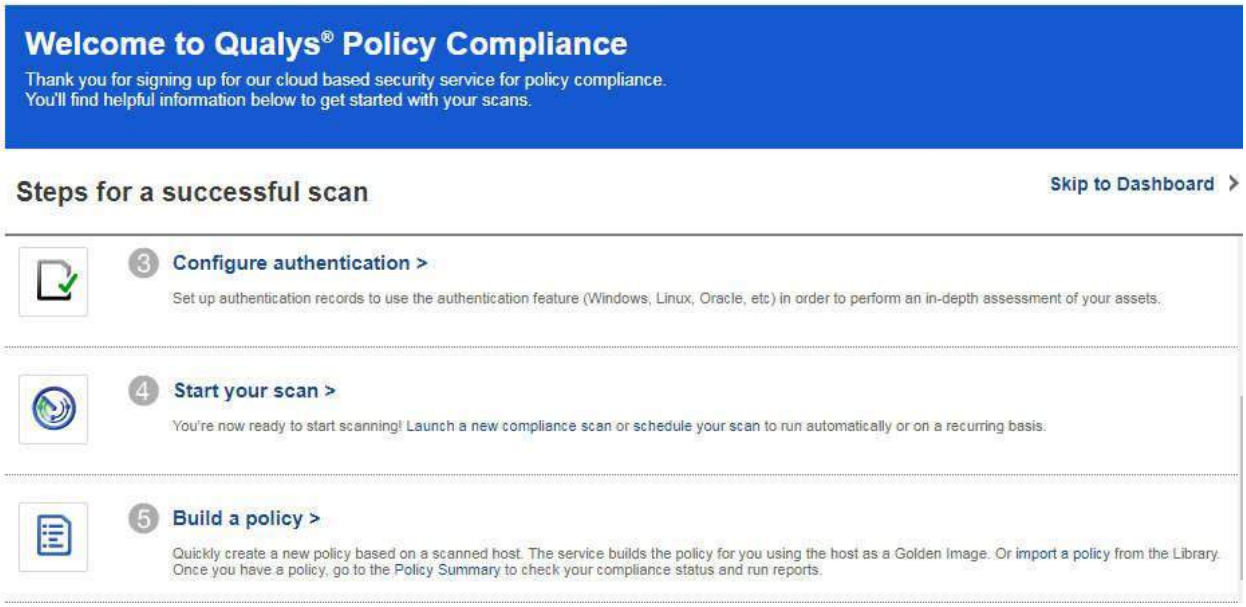
QUALYS WEBSITE – FREE TRIAL



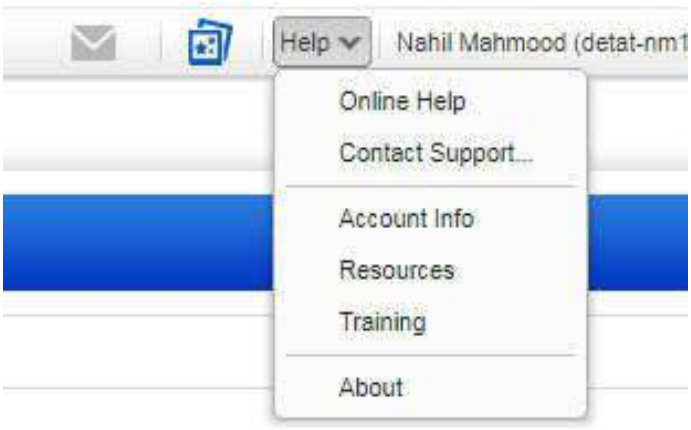
QUALYS GUARD – HOME SCREEN



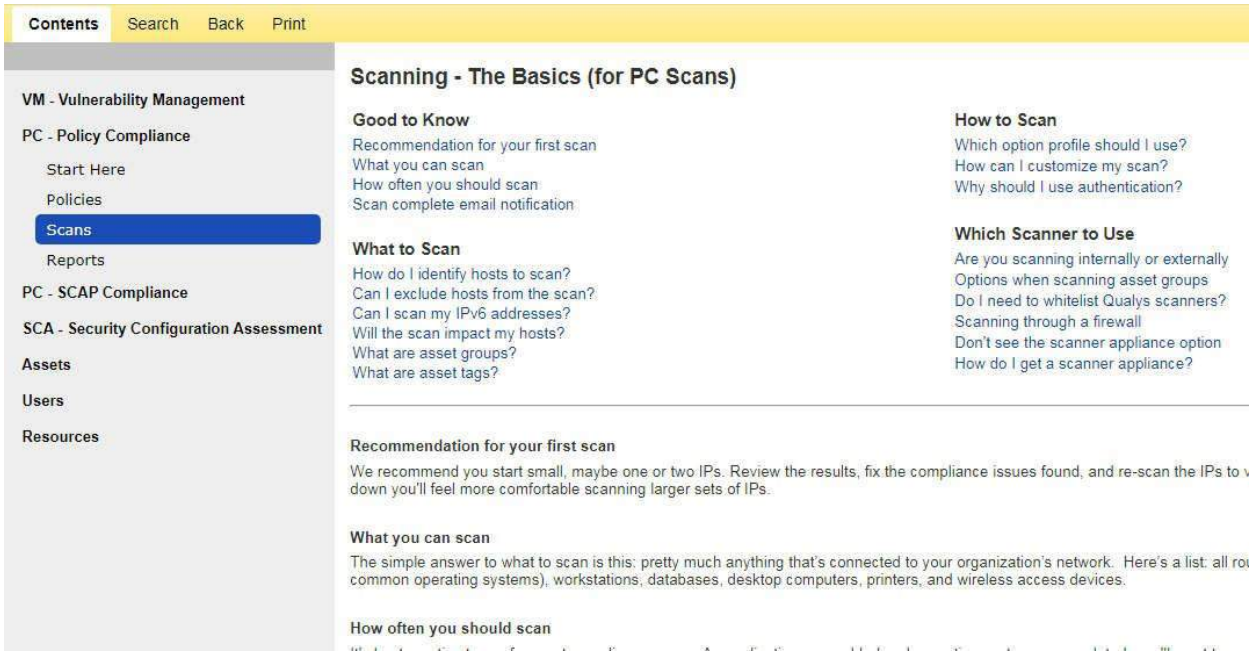
POLICY COMPLIANCE – HOME SCREEN



POLICY COMPLIANCE – 5 STEPS



HELP OPTIONS



ONLINE HELP – POLICY COMPLIANCE

Resources

Look to these resources to help you with our cloud security and compliance solutions.

Get Started

Quick Tour
Evaluator's Guide
Community Edition
Securing Amazon Web Services with Qualys

Watch Videos

VM | PC | WAS | WAF | AWS EC2 | Express Lite | More Videos

Get started with your applications

CloudView
Container Security
Indication of Compromise
Web Application Scanning
- Crawling REST services using WAS
- Jenkins Plugin for WAS: user guide | download
- Qualys Browser Recorder: user guide | download
Web Application Firewall
Policy Compliance
SCAP Compliance
Security Configuration Assessment
PCI Compliance
File Integrity Monitoring

Scan Authentication

Get system and account requirements for supported technologies below.

Cloud Agents

Cloud Agent Getting Started Guide
Windows Installation Guide
Linux Installation Guide
Unix Installation Guide
Mac Installation Guide

Using a scanner appliance?

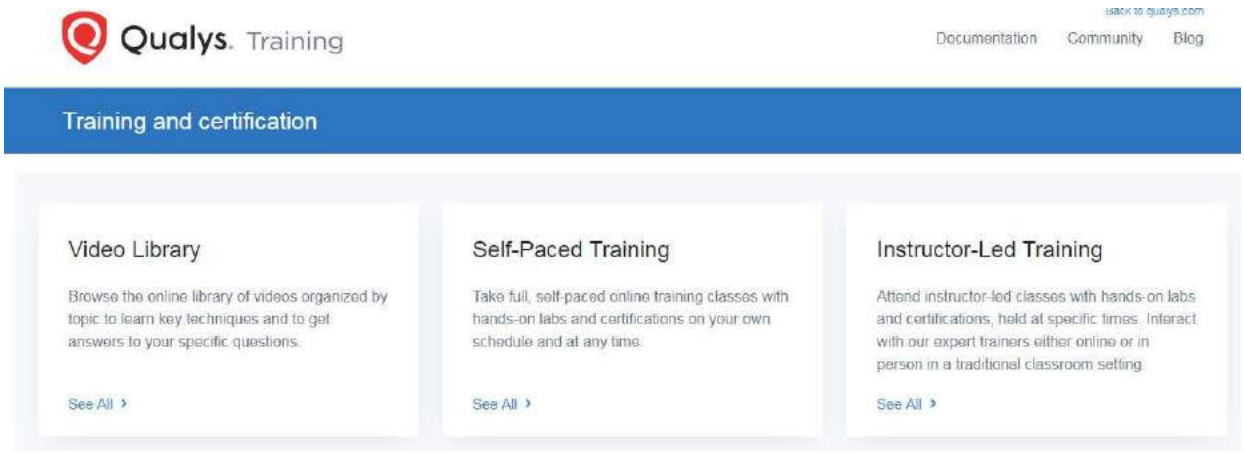
Scanner Appliance User Guide
Scanner Appliance Quick Start (prior version)
Virtual Scanner Appliance User Guide
Offline Scanner Appliance User Guide
Consultant Scanner Personal Edition User Guide
Cloud Platforms: AWS | Azure | GCE | OpenStack
Qualys Scanner - Static Route Configuration
Qualys Scanner - VLAN Scanning Guide
Scanner Appliance FAQs

API Documentation

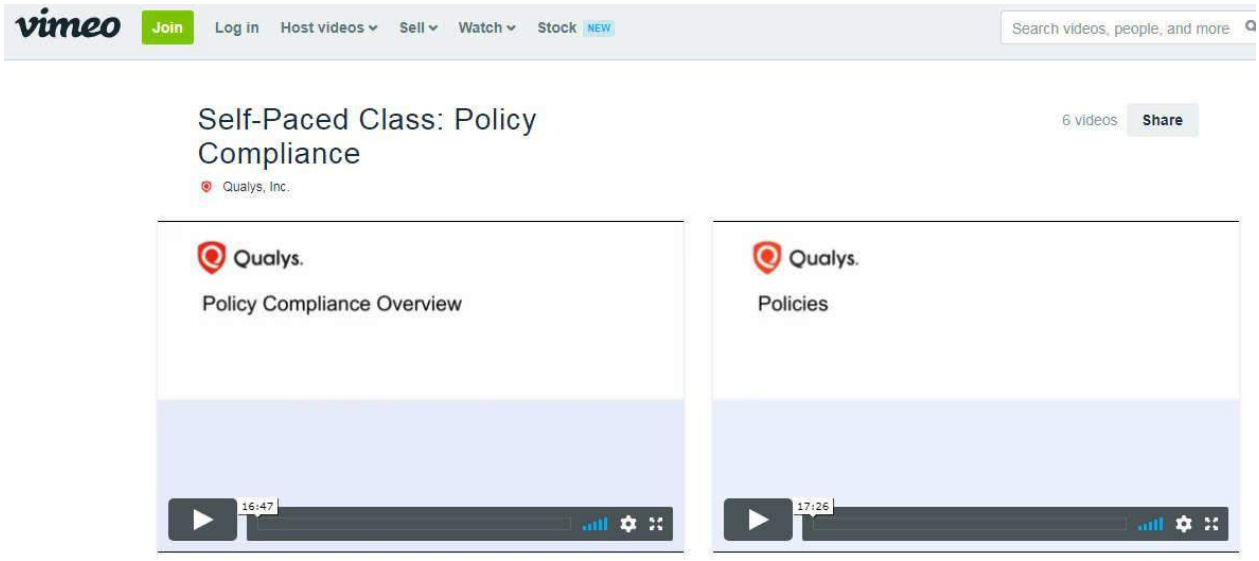
Qualys API Quick Reference for all APIs
Qualys API (VM, SCA, PC)

Cloud Agent (CA) API
Web Application Scanning (WAS) API
Web Application Firewall (WAF) API
Malware Detection (MD) API

RESOURCES

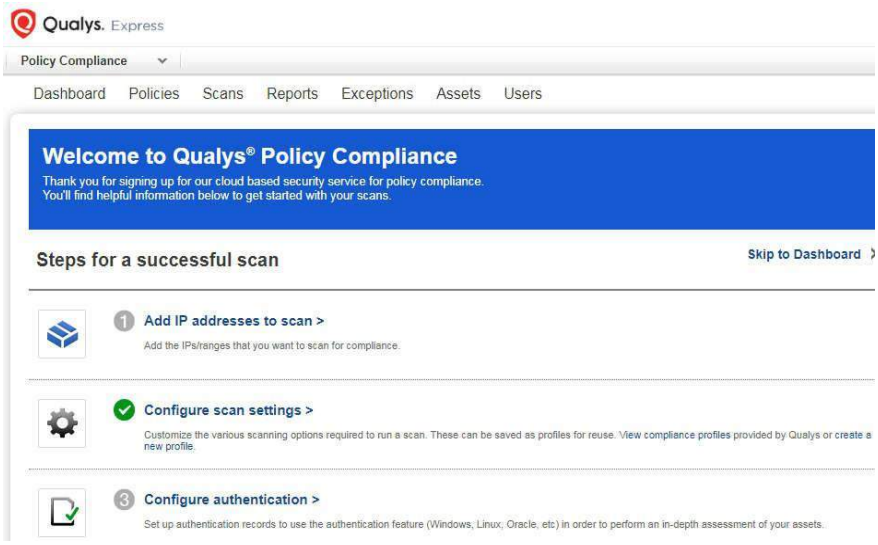


QUALYS WEBSITE - TRAINING

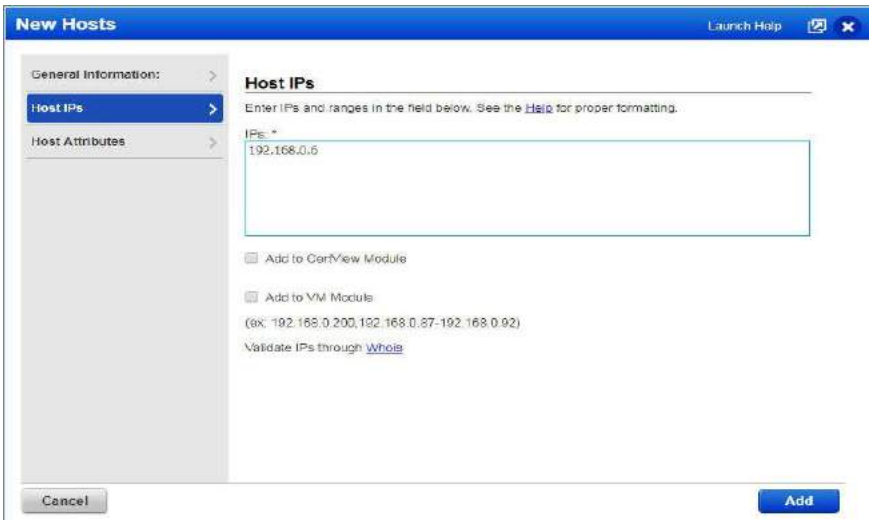


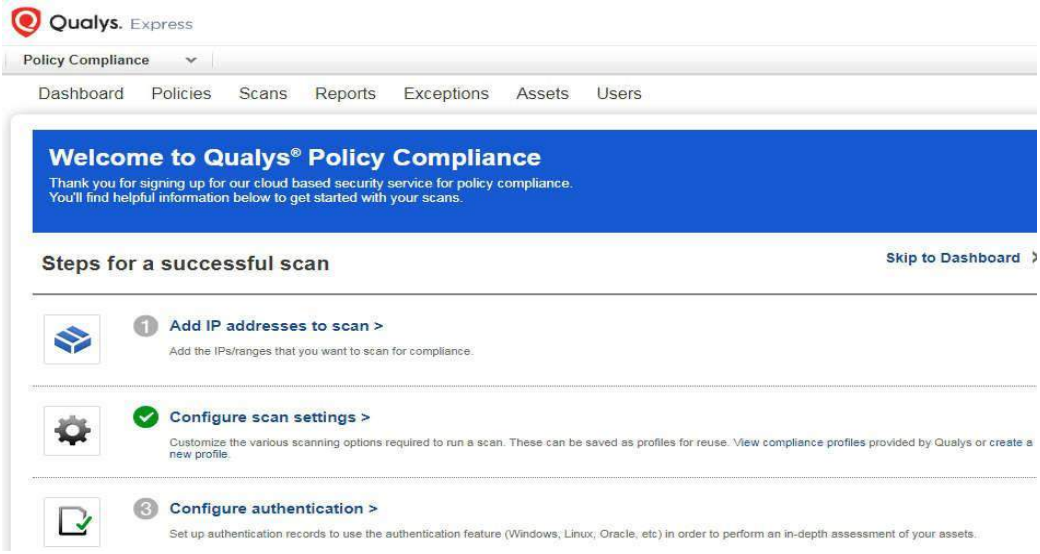
TRAINING VIDEOS - VIMEO

- Qualys is an excellent tool with detailed online help, training, and resources to aid the new user

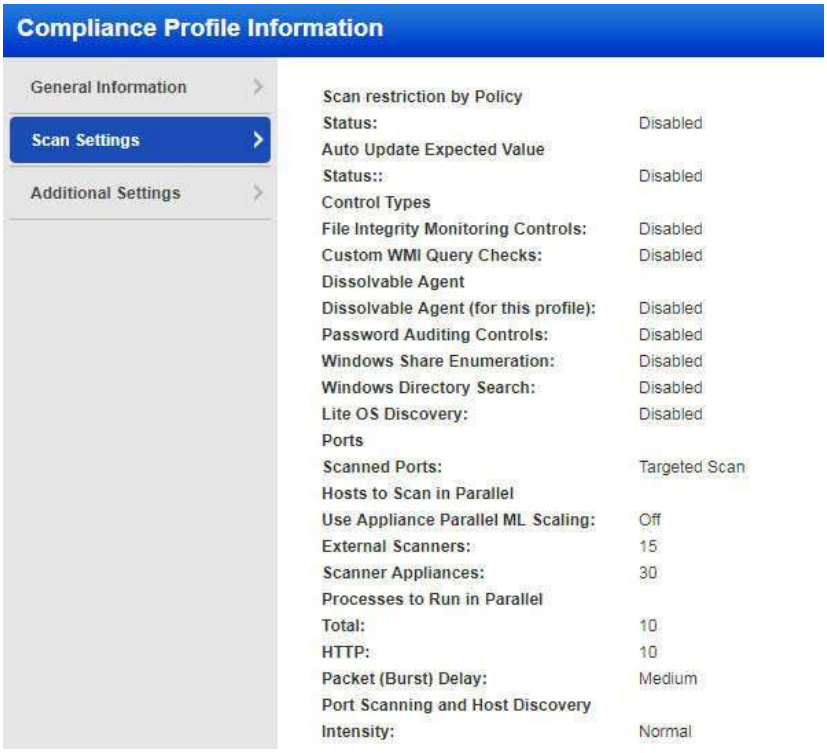


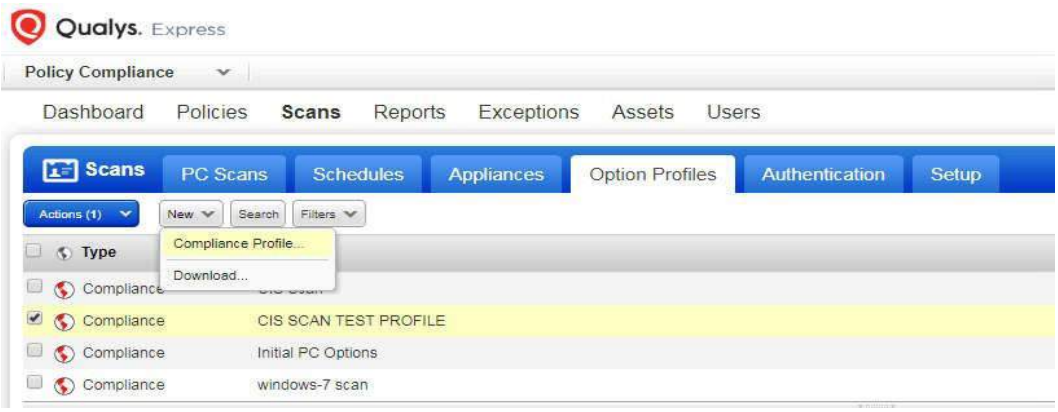
1. ADD IP ADDRESSES TO SCAN



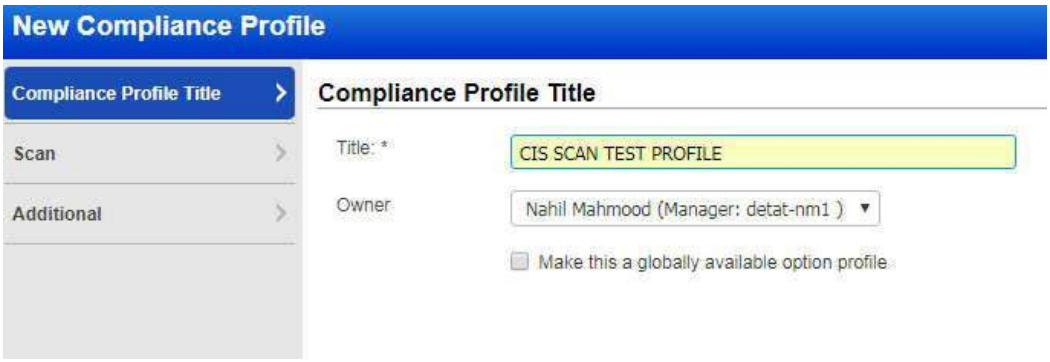


1. CONFIGURE SCAN SETTINGS

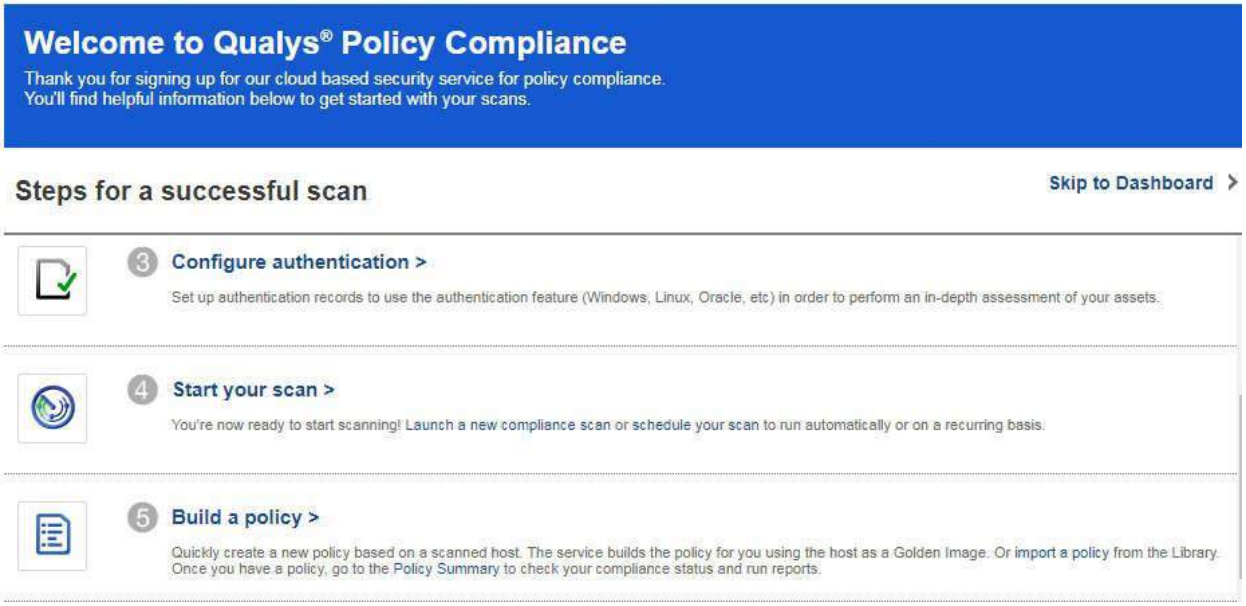




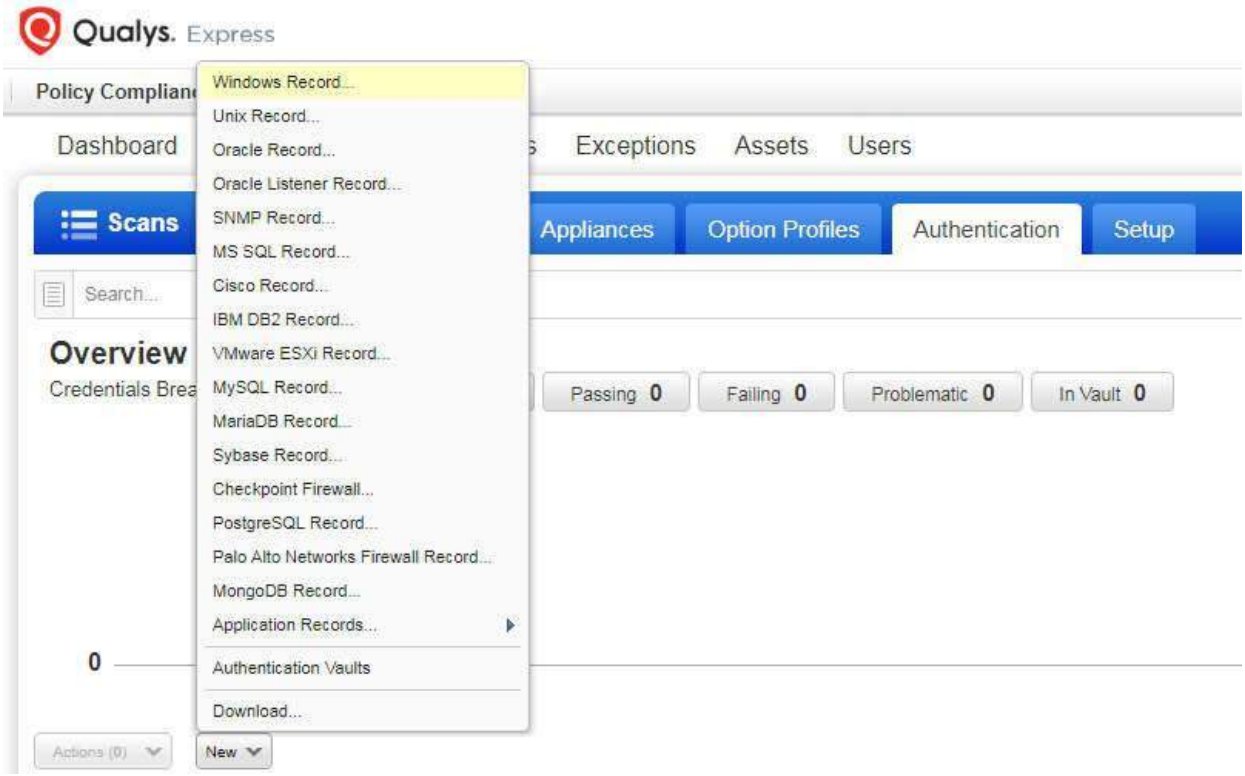
NEW COMPLIANCE PROFILE

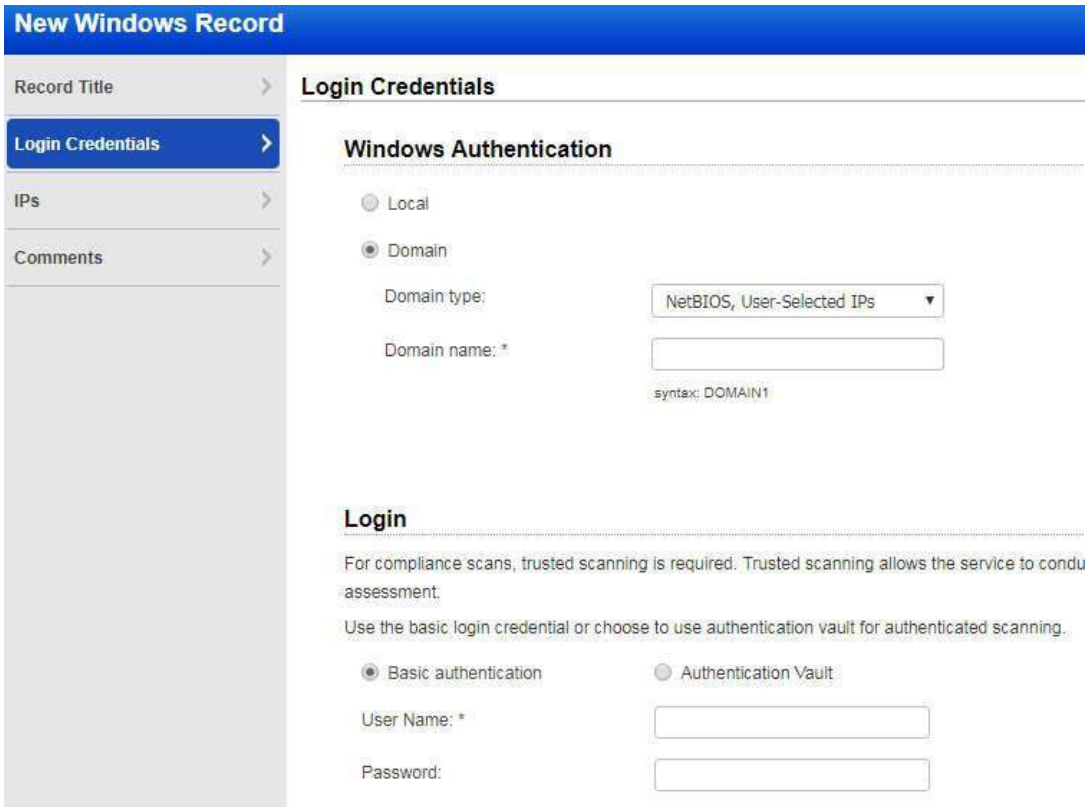


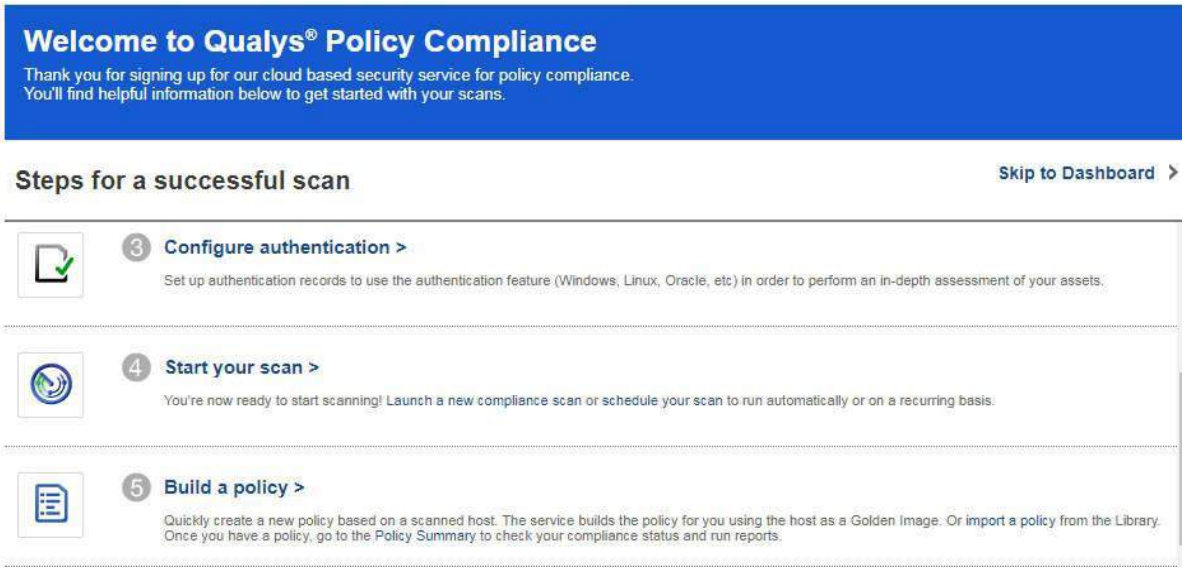
‘CIS SCAN TEST PROFILE’ CREATED

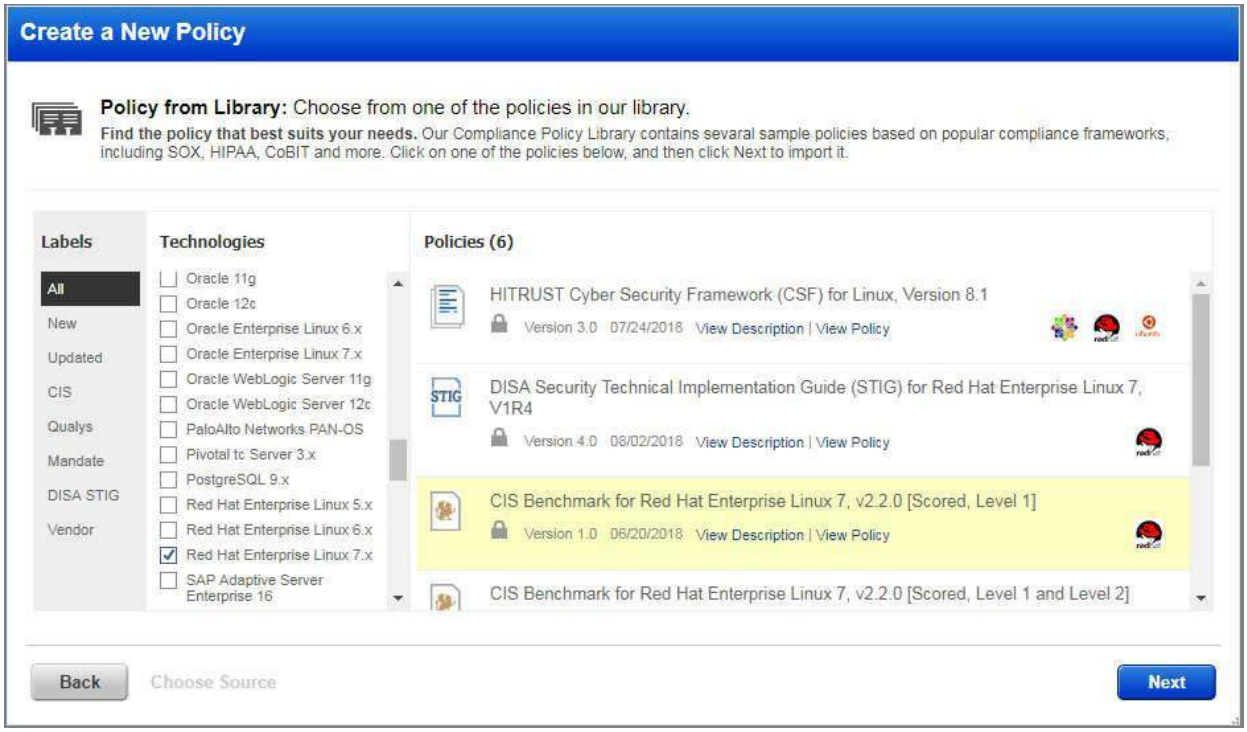


2. CONFIGURE AUTHENTICATION

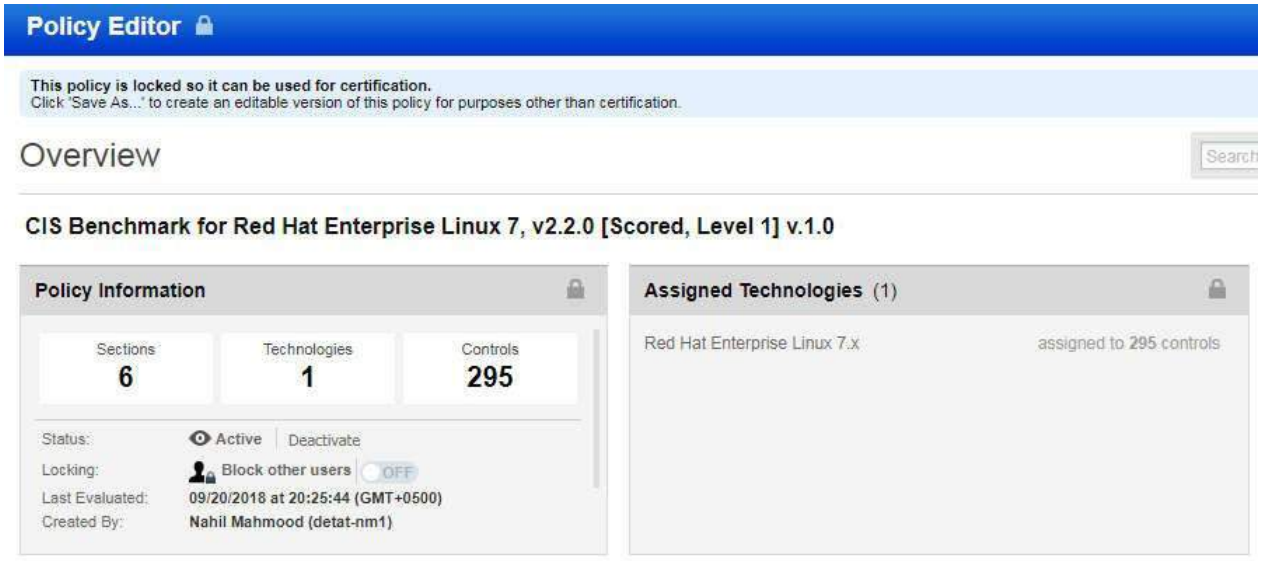



New Windows Record
Record Title
Login Credentials
IPs
Comments
Login Credentials
Windows Authentication
Local
Domain
Domain type:
NetBIOS, User-Selected IPs
Domain name: *
syntax: DOMAIN1
Login
For compliance scans, trusted scanning is required. Trusted scanning allows the service to condu
assessment.
Use the basic login credential or choose to use authentication vault for authenticated scanning.
Basic authentication
Authentication Vault
User Name: *
Password:

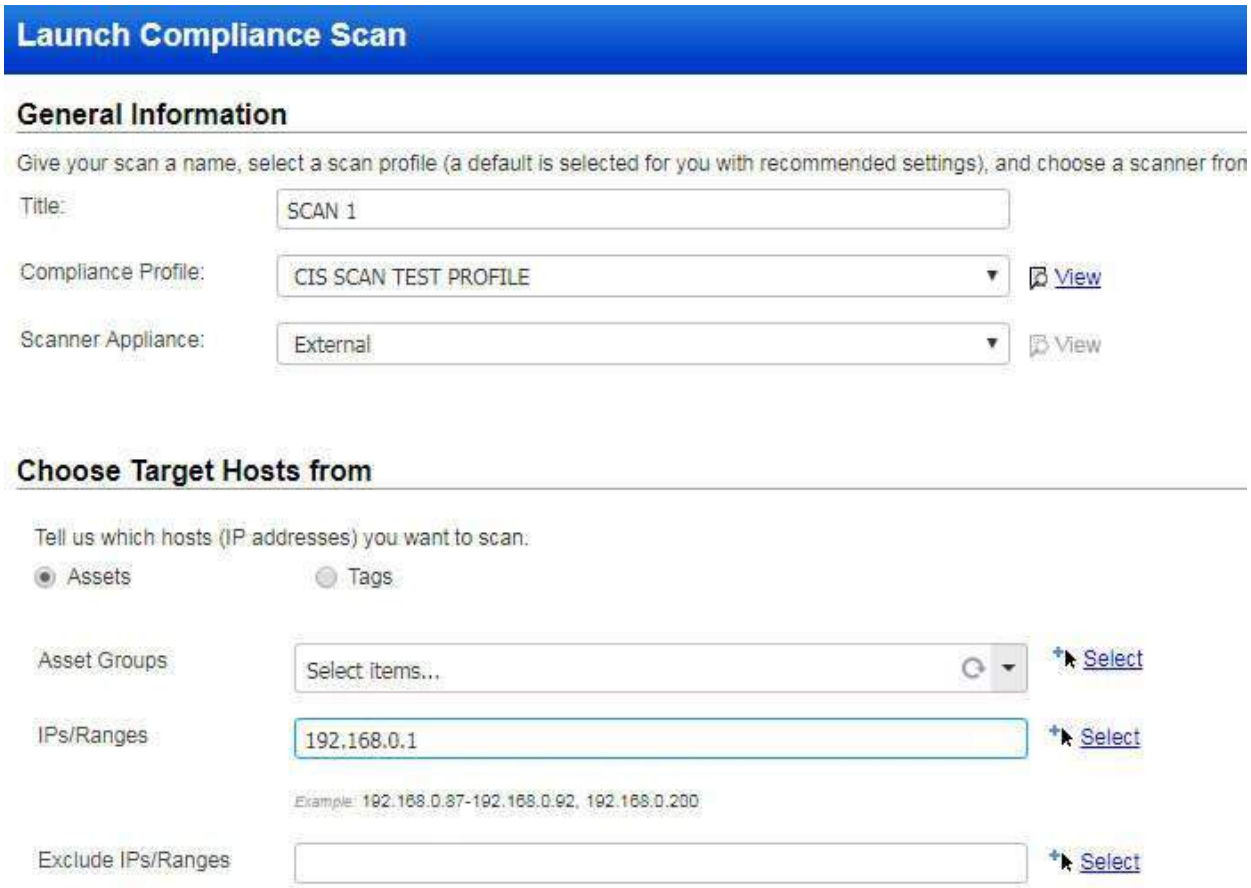

Welcome to Qualys® Policy Compliance
Thank you for signing up for our cloud based security service for policy compliance.
You'll find helpful information below to get started with your scans.
Steps for a successful scan
Skip to Dashboard
3 Configure authentication >
Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.
4 Start your scan >
You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.
5 Build a policy >
Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library.
Once you have a policy, go to the Policy Summary to check your compliance status and run reports.



COMPLIANCE LIBRARY: CIS RED HAT ENT. LINUX 7



POLICY EDITOR



LAUNCH COMPLIANCE SCAN

- The scan features may also be adjusted from the main Qualys dashboard

Topic no 113: SECURITY HARDENING – LIFECYCLE

- Security Hardening Lifecycle: Maintaining An Integrated & Current Program

1: Harden IT Asset

Pursue the 8 step hardening methodology

2: Periodic Validation

Check periodically (every quarter) for changes to the established standard or baseline

3: Seek Updated On Hardening Benchmarks

- Benchmarks are periodically updated
- Subscribe to feeds from CIS, DISA, NIST NCP (National Checklist Program) Repository

4: Implement Additional Controls

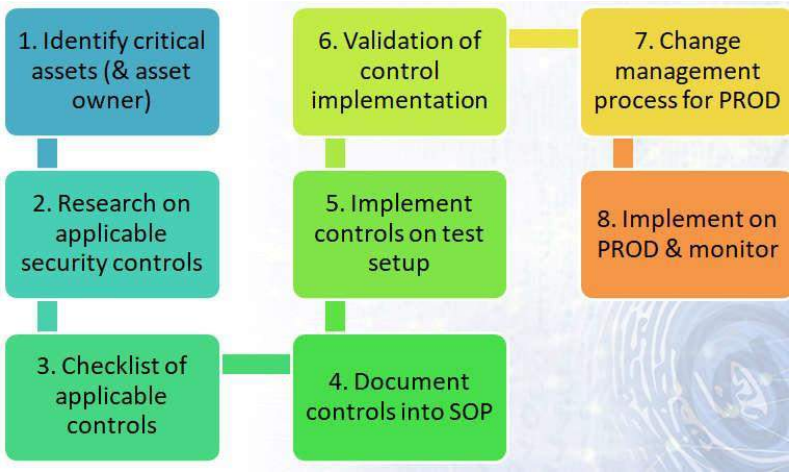
- Update the security controls by studying the changes

5: Pursue & Implement Controls That May Require Additional Working

- Some controls may have caused a crash or malfunction
- Some controls may have not been possible due to dependencies or missing utilities
- Enhance the % of implemented controls

Topic no 114: Hardening When CIS/DISA STIG Not Available

- What type of IT assets do not have a CIS/DISA STIG ?
  - Software applications (ASP.NET, PHP, Other)
  - Other applications such as asterisk deployments



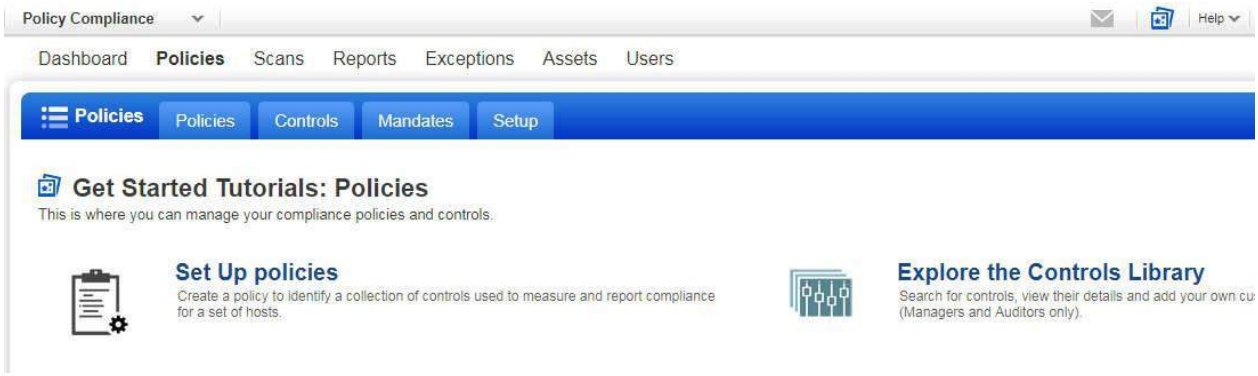
- **Step 2: Research:**

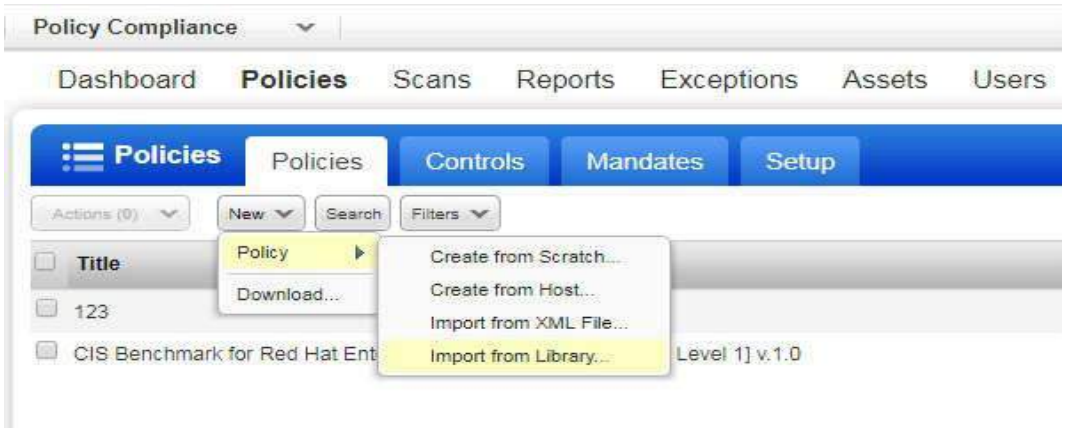
  - Look up google
  - Look for case studies and whitepapers

- **Other considerations:**
  - Implement on test setup
  - Test the controls
  - Security testing tools
  - Perform third-party security testing (penetration testing)
  - Vendor best-practices for application security hardening
- With efforts and by following the 8-step methodology, all types of assets can be hardened

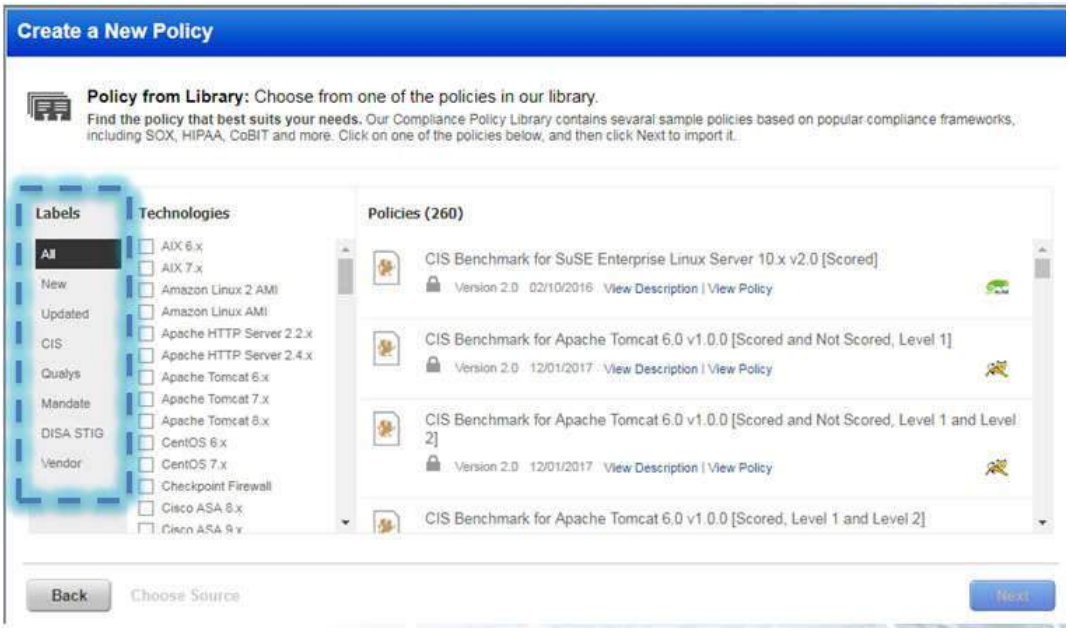
Topic no 115: QUALYS POLICY LIBRARIES

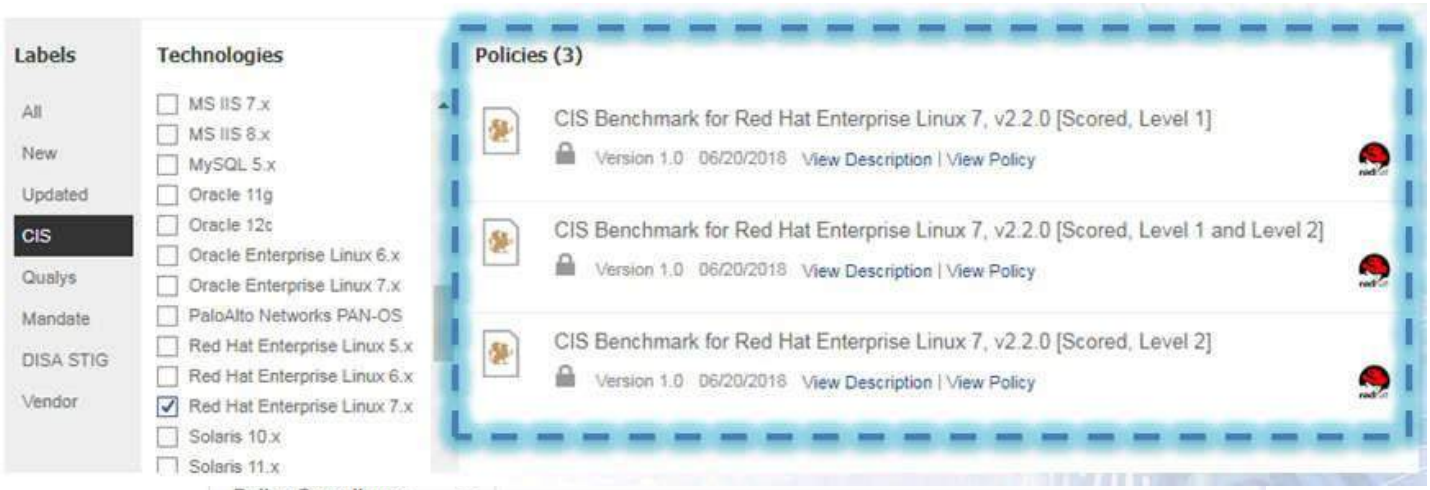
- Lets have a detailed look at Qualys built-in libraries for creating scanning policies
- CIS
- QUALYS
- MANDATE
- DISA
- VENDOR

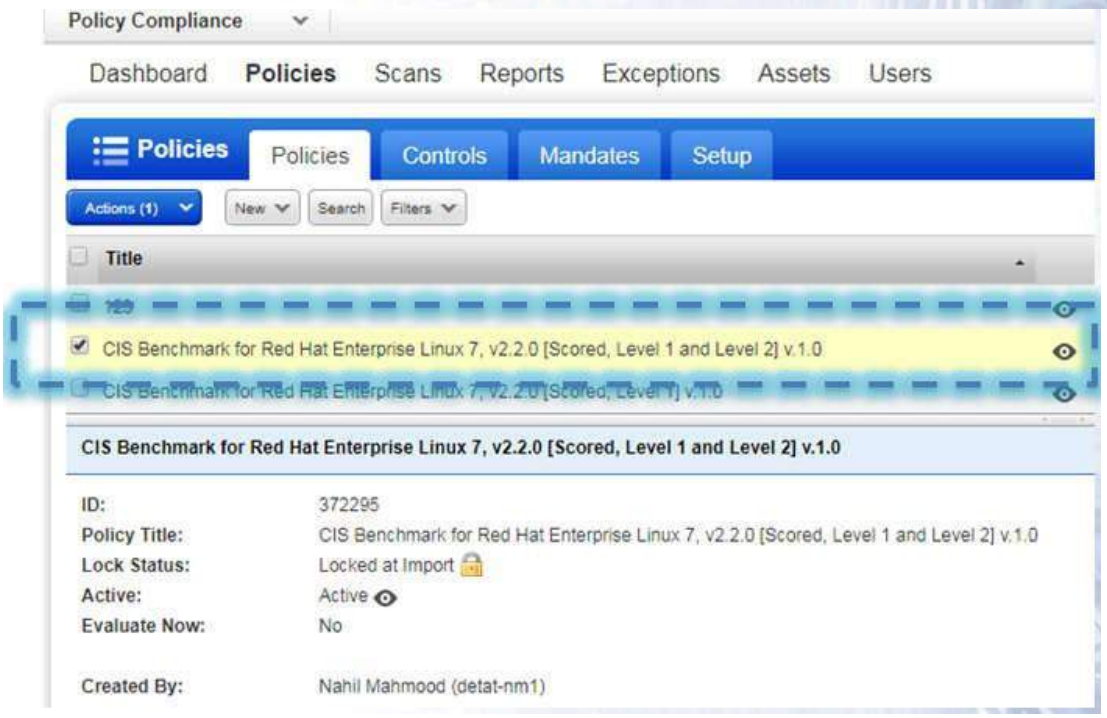




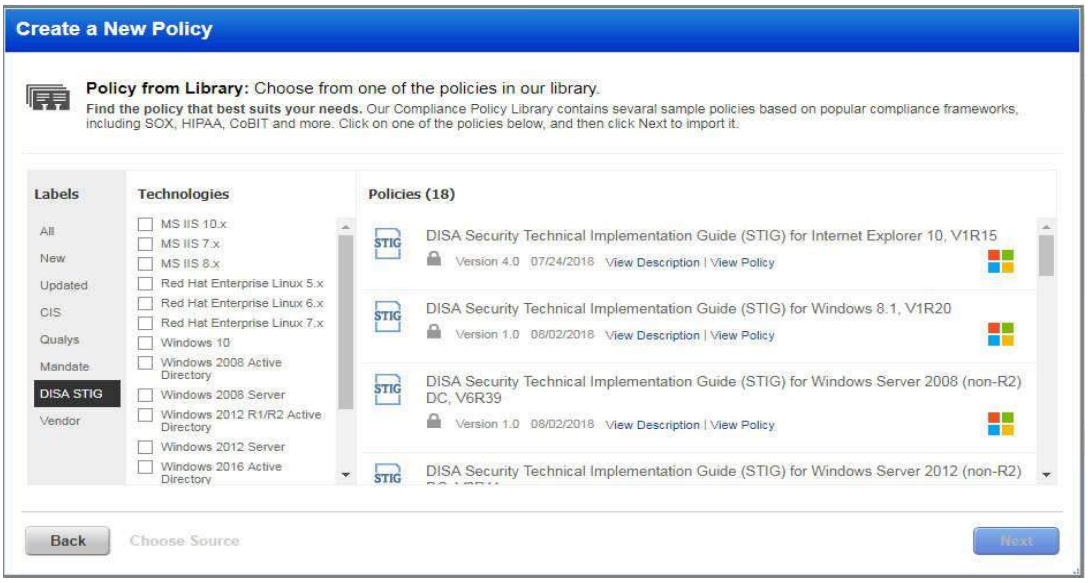
CREATE NEW POLICY > IMPORT FROM LIBRARY


Create a New Policy
Policy from Library: Choose from one of the policies in our library.
Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.
Labels
All
New
Updated
CIS
Qualys
Mandate
DISA STIG
Vendor
Technologies
AIX 6.x
AIX 7.x
Amazon Linux 2 AMI
Amazon Linux AMI
Apache HTTP Server 2.2.x
Apache HTTP Server 2.4.x
Apache Tomcat 6.x
Apache Tomcat 7.x
Apache Tomcat 8.x
CentOS 6.x
CentOS 7.x
Checkpoint Firewall
Cisco ASA 8.x
Policies (260)
CIS Benchmark for SuSE Enterprise Linux Server 10.x v2.0 [Scored]
Version 2.0 02/10/2016 View Description | View Policy
CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1]
Version 2.0 12/01/2017 View Description | View Policy
CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1 and Level 2]
Version 2.0 12/01/2017 View Description | View Policy
CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored, Level 1 and Level 2]
Back
Choose Source
Next

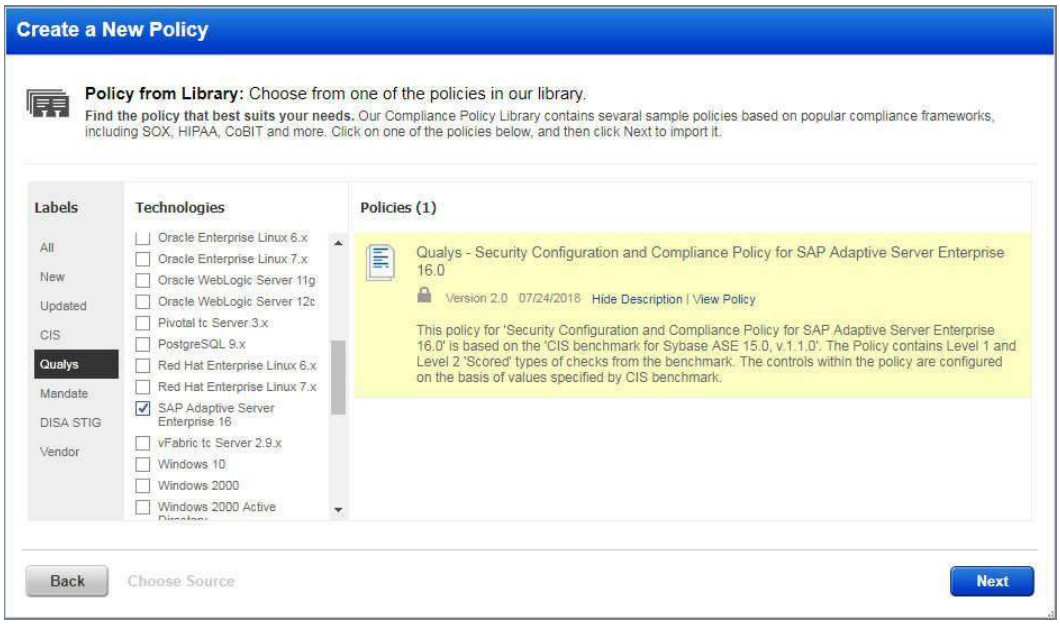

Labels
All
New
Updated
CIS
Qualys
Mandate
DISA STIG
Vendor
Technologies
MS IIS 7.x
MS IIS 8.x
MySQL 5.x
Oracle 11g
Oracle 12c
Oracle Enterprise Linux 6.x
Oracle Enterprise Linux 7.x
PaloAlto Networks PAN-OS
Red Hat Enterprise Linux 5.x
Red Hat Enterprise Linux 6.x
Red Hat Enterprise Linux 7.x
Solaris 10.x
Solaris 11.x
Policies (3)
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1]
Version 1.0 06/20/2018 View Description | View Policy
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2]
Version 1.0 06/20/2018 View Description | View Policy
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 2]
Version 1.0 06/20/2018 View Description | View Policy


Policy Compliance
Dashboard
Policies
Scans
Reports
Exceptions
Assets
Users
Policies
Policies
Controls
Mandates
Setup
Actions (1)
New
Search
Filters
Title
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] v.1.0
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0
ID: 372295
Policy Title: CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0
Lock Status: Locked at Import
Active: Active
Evaluate Now: No
Created By: Nahil Mahmood (detat-nm1)

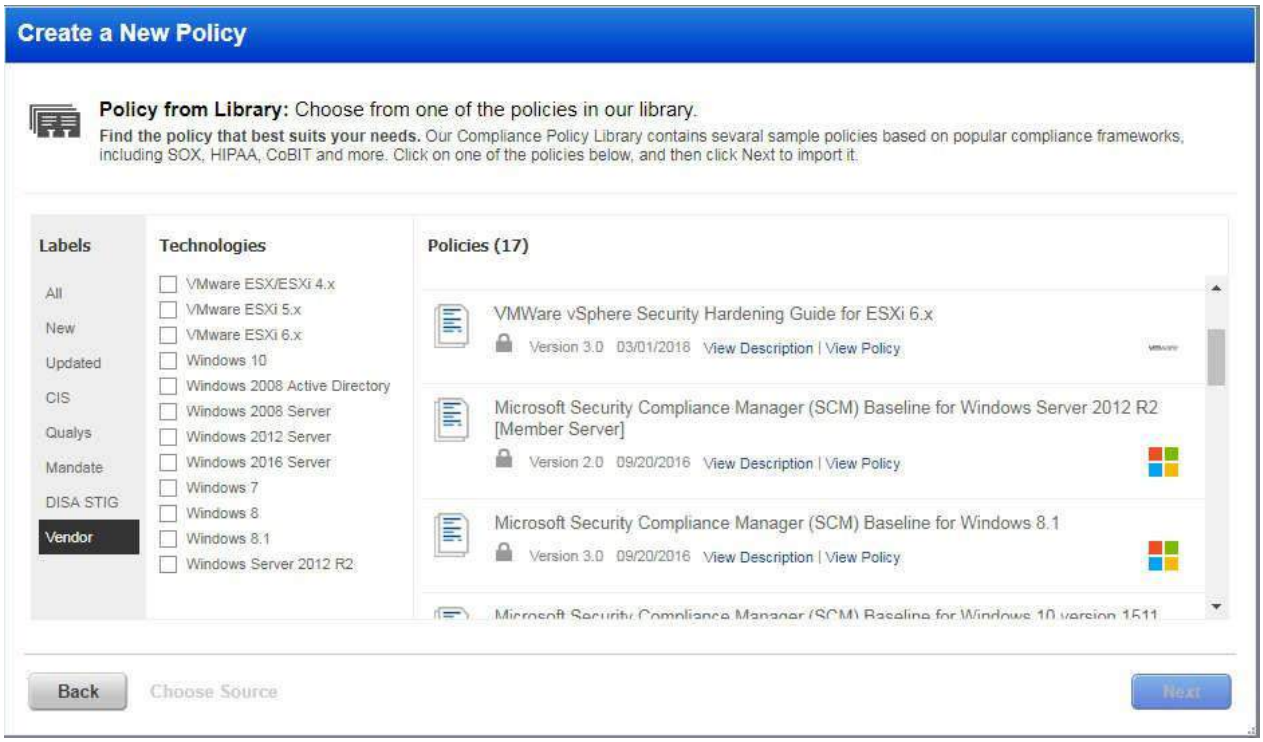
POLICIES DASHBOARD



DISA STIG



QUALYS SAP ADAPTIVE SERVER ENT 16



VENDOR POLICIES

- Qualys has a vast number of options for Compliance Scans, and these should be fully explored through the Qualys trial

Topic no 116: Security Hardening For Outsourced IT Assets

- IT Outsourcing
- Mechanism to harden outsourced IT assets
- Important considerations

- **IT Outsourcing examples:**
  - Call centers
  - Hosted servers
  - Software development
  - Workstation helpdesk functions
  - Network services
  - Any other arrangement
- **Mechanism:**
  - Information Security Policy
  - Vendor contract (right-to-audit clause)
  - Set up security project with security project manager
  - Periodic reviews
  - Penalties for non-compliance
- **Important considerations:**
  - Enter security requirements into RFP
  - Part of vendor evaluation
  - Proceed with contract including InfoSec clauses
  - Awareness training
- **Security evaluations:**
  - Include outsourced scope in periodic internal audit

- Ask for third-party security review
- Vulnerability assessment and penetration test (if applicable)
- Spot security checks

Topic no 117: What is Vulnerability Management?

- **What is vulnerability?**
  - Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures or in anything that leaves information security exposed to a threat.

- **How do you fix vulnerabilities?**
  - Computer users and network personnel can protect computer systems from vulnerabilities by keeping software security patches up to date. These patches can remedy flaws or security holes that were found in the initial release. Computer and network personnel should also stay informed about current vulnerabilities in the software they use and seek out ways to protect against them.

- **What is vulnerability management?**
  - Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities"

- **What is vulnerability assessment (VA)?**
  - A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

- **What are some of the common vulnerability scanners?**
  - OpenVAS
  - Nessus
  - Qualys
  - Rapid7

Topic no 118: What Are The Steps In VM Lifecycle?

VM Steps:

1. Analyze assets
2. Prepare scanner
3. Run vulnerability scan
4. Assess results
5. Patch systems
6. Verify (re-scan)

1. **Analyze Assets:**
    - Examine assets to scan
    - Gather details on IP subnet
    - Look at potential issues with network traffic
    - Inform asset owners and relevant department heads

2. **Prepare Scanner:**
   - Set scanner parameters
   - Select type of scan
   - Look at credentials-based scan
   - Explore and research plug-ins
   - Do a test run
   - Coordinate with asset owner

3. **Run Vulnerability Scanner:**
   - Run the automated scan
   - Monitor network performance degradation issues
   - Generate report

4. **Assess Results:**
   - Evaluate results
   - Prioritize according to the risk level
   - Collate results for asset owners
   - Communicate the results and remediation timelines

5. **Patch Systems:**
   - Research vulnerabilities
   - Evaluate fixes and remediation method
   - Test the patches and fixes
   - Apply patches/fixes
   - Monitor results

6. **Verify (Re-scan)**
   - Re-scan to confirm that the vulnerability scanner gives a positive report
   - Collate results of vulnerability scan
   - Report findings

Topic no 119: Why Is Software Insecure?

- Software is everywhere in IT
- Software is being developed in a manner which leaves many defects which may be exploited by attackers
- Race to meet software deadlines with little emphasis on security
- **Result:** insecure software
- Gary McGraw, "trinity of trouble" for software security:
  - **Connectivity;** ever-increasing computer connectivity & to the internet enhances exposure to attacks

- **Extensibility: "**Second, an extensible system is one that supports updates and extensions and thereby allows functionality to evolve incrementally. Web browsers, for example, support plug-ins that enable users to install extensions for new document types. Extensibility is attractive for purposes of increasing functionality, but also makes it difficult to keep the constantly-adapting system free of software vulnerabilities."

- **Complexity:** Software systems are growing exponentially in size and complexity, which makes vulnerabilities unavoidable.

- Carnegie Mellon University's CyLab Sustainable Computing Consortium estimates that commercial software contains 20 to 30 bugs for every 1,000 lines of code and Windows XP contains at least 40 million lines of code That's 1 million bugs in Windows XP

- **Monoculture: Dan Greer:** "The security situation is deteriorating, and that deterioration compounds when nearly all computers in the hands of end users rely on a single operating system subject to the same vulnerabilities the world over."

Topic no 120: Why Is A VM Program Required?

- **What is a patch?**
  - "A **patch** is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing **security** vulnerabilities and other bugs"

- **What is patch management?**
  - Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

- **Patch management tasks :**
  - Maintaining current knowledge of available patches, deciding what patches are

appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configs required.

- **Risk of not patching:**
  - By not applying a patch you might be leaving the door open for a malware attack

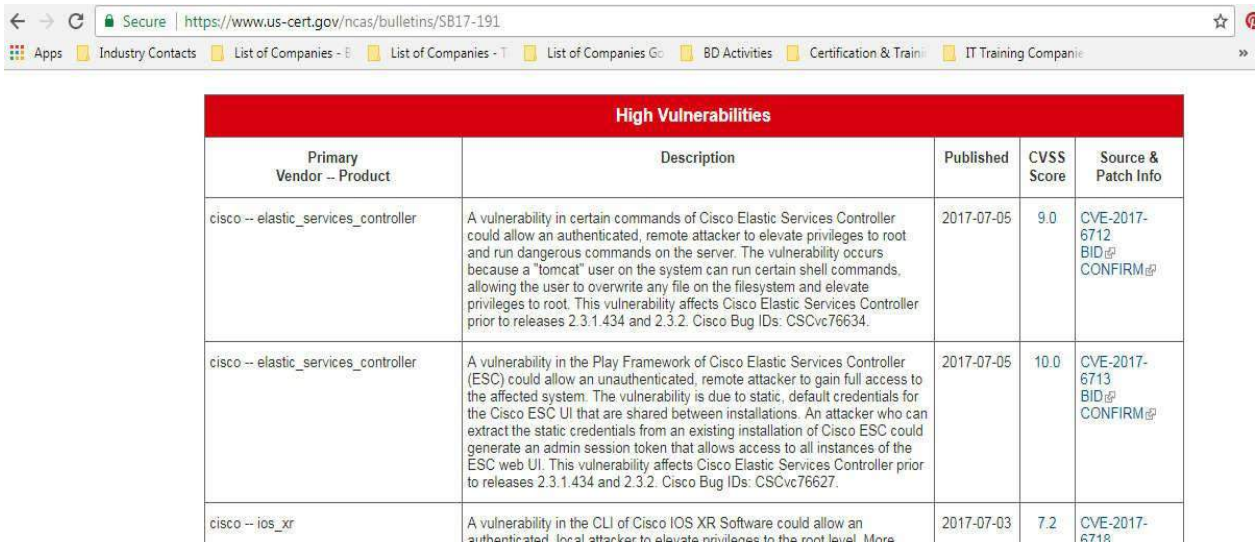
- Malware exploits flaws in a system in order to do its work. In addition, the timeframe between an exploit and when a patch is released is getting shorter
- Defects in clients like web browsers, email programs, image viewers, instant messaging software, and media players may allow malicious websites, etc. to infect or compromise your computer with no action on your part other than viewing or listening to the website, message, or media

A VM program addresses timely management of patching to ensure that vulnerabilities are not present for hackers to exploit

Topic no 121: What Is CVE & Vulnerability Database?

- **What is CVE?**
  - CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

SNAPSHOT OF US-CERT VULNERABILITY BULLETINS



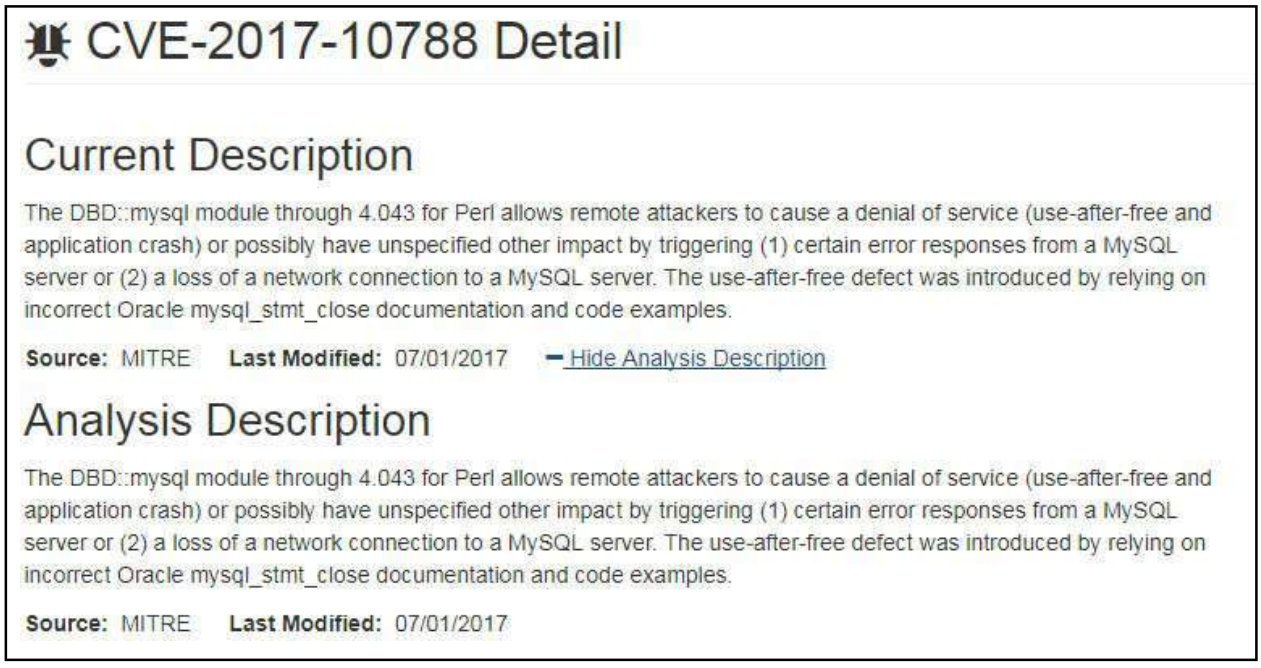
High Vulnerabilities

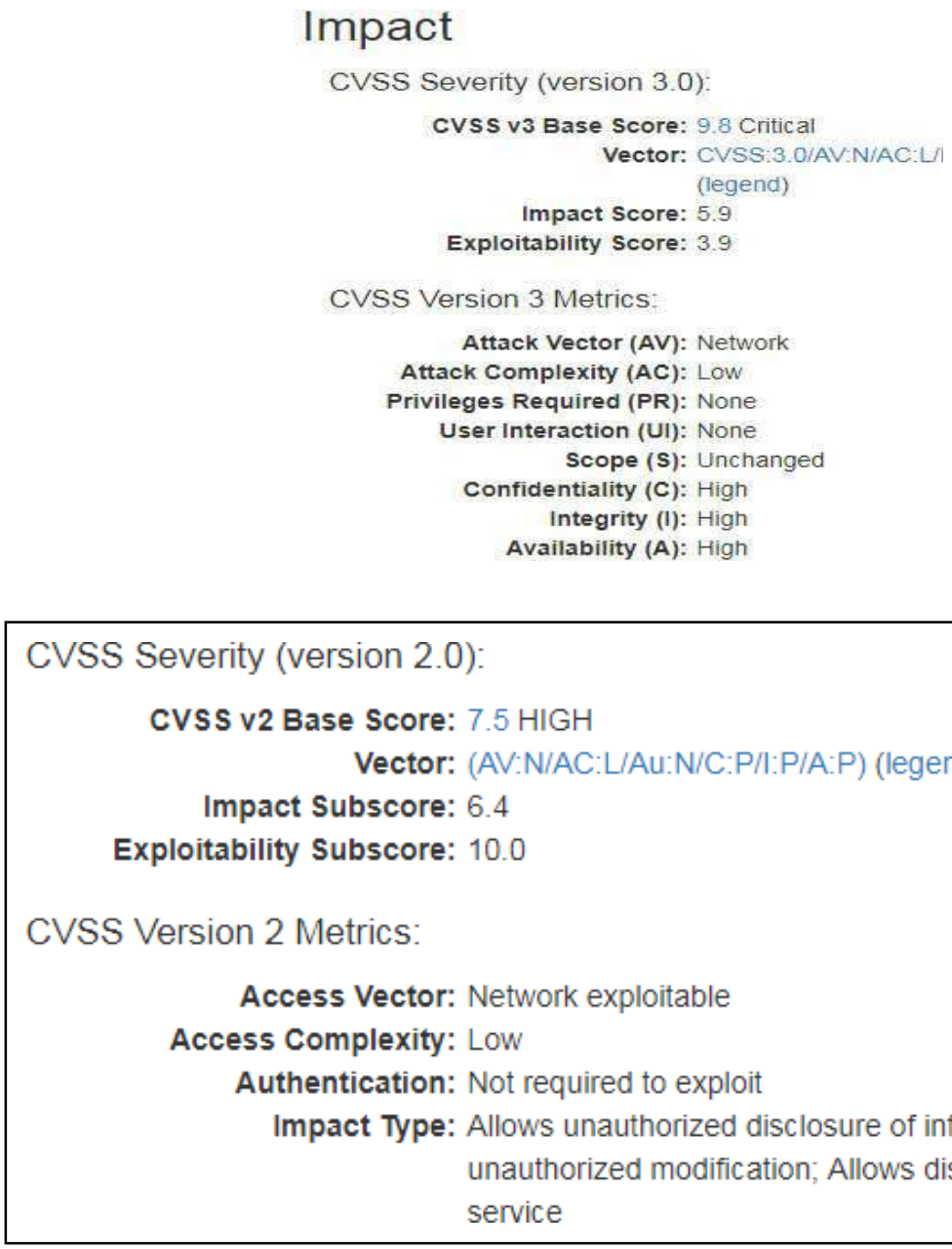
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- elastic_services_controller	A vulnerability in certain commands of Cisco Elastic Services Controller could allow an authenticated, remote attacker to elevate privileges to root and run dangerous commands on the server. The vulnerability occurs because a "tomcat" user on the system can run certain shell commands, allowing the user to overwrite any file on the filesystem and elevate privileges to root. This vulnerability affects Cisco Elastic Services Controller prior to releases 2.3.1.434 and 2.3.2. Cisco Bug IDs: CSCvc76634.	2017-07-05	9.0	CVE-2017-6712 BID CONFIRM
cisco -- elastic_services_controller	A vulnerability in the Play Framework of Cisco Elastic Services Controller (ESC) could allow an unauthenticated, remote attacker to gain full access to the affected system. The vulnerability is due to static, default credentials for the Cisco ESC UI that are shared between installations. An attacker who can extract the static credentials from an existing installation of Cisco ESC could generate an admin session token that allows access to all instances of the ESC web UI. This vulnerability affects Cisco Elastic Services Controller prior to releases 2.3.1.434 and 2.3.2. Cisco Bug IDs: CSCvc76627.	2017-07-05	10.0	CVE-2017-6713 BID CONFIRM
cisco -- ios_xr	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to elevate privileges to the root level. More	2017-07-03	7.2	CVE-2017-6718

- **What is NVD?**
  - The NVD is the CVE dictionary augmented with additional analysis, a database, and a fine- grained search engine. The NVD is a superset of CVE. The NVD is synchronized with CVE such that any updates to CVE appear immediately on the NVD.

- **What is the NVD severity score?**
  - The NVD uses the Common Vulnerability Scoring System (CVSS) Version 2, which is is an open standard for assigning vulnerability impacts that is used by a variety of organizations
  - NISTIR 7946 - CVSS Implementation Guidance describes methodologies developed by the NVD for using CVSS, and along with Appendix B describes the NVD's entire vulnerability assessment process.

SNAPSHOT OF CVE-2017-10788



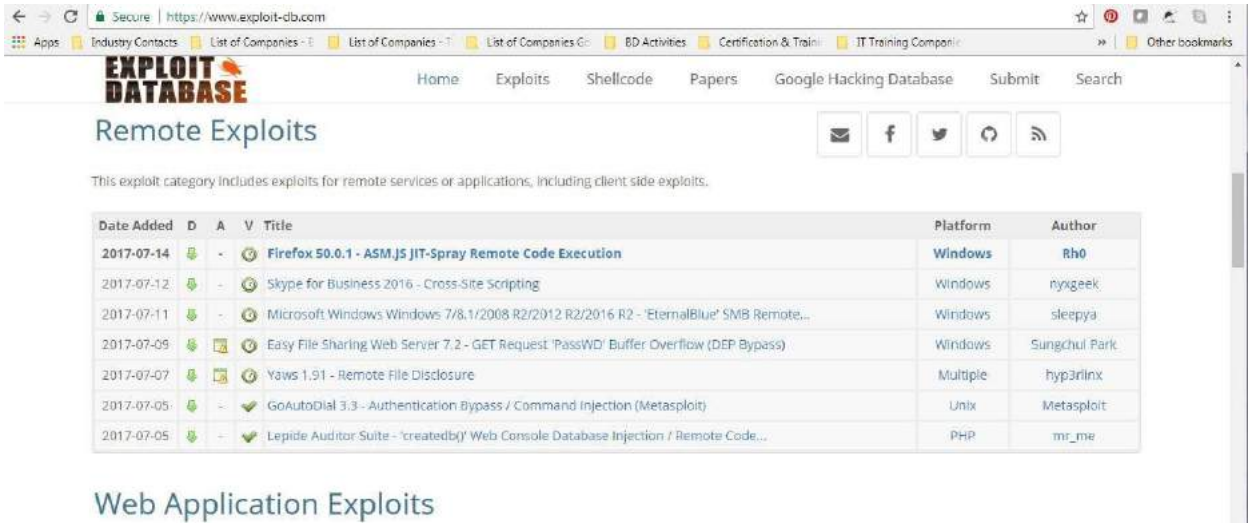


- Note that all the major vendors publish their security vulnerabilities online
  - Microsoft
  - Oracle
  - Cisco
  - Etc

Topic no 122: What Is An Exploit?

- **What is an exploit?**
  - Program or some code that takes advantage of a security hole (i.e. a vulnerability) in an application or system, so that an attacker can use it for their benefit.

- **Remote exploit:**
  - A *remote exploit* works over a network and exploits the security vulnerability without any prior access to the vulnerable system.
- **Local exploit:**
  - A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.
- **Exploit database:**
  - The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database.
  - The Exploit Database is a repository for *exploits and proof-of-concepts rather than advisories*, making it a valuable resource for those who need actionable data right away.



SNAPSHOT OF EXPLOIT CODE

EDB-ID: 42327	**Author**: Rh0	**Published**: 2017-07-14
CVE: CVE-2016-9079...	**Type**: Remote	**Platform**: Windows
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified:	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

```
<!DOCTYPE HTML>

<!--

    FULL ASLR AND DEP BYPASS USING ASM.JS JIT SPRAY (CVE-2017-5375)
    PoC Exploit against Firefox 50.0.1 (CVE-2016-9079 - Tor Browser 0day)

    Tested on:

    Release 50.0.1 32-bit - Windows 8.1 / Windows 10
    https://ftp.mozilla.org/pub/firefox/releases/50.0.1/win32/en-US/Firefox%20Setup%2050.0.1.exe

    Howto:

    1) serve PoC over network and open it in Firefox 50.0.1 32-bit
    2) if you don't see cmd.exe, open processexplorer and verify that cmd.exe was spawned by firefox.exe

    A successfull exploit attempt should pop cmd.exe
```

- **Zero-day exploit:**
  - A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it this **exploit** is called a zero day attack.

Topic no 123: Effective Vulnerability Management: Stage 2

Another look at the security transformation model

- Stage 1: Security hardening
  - Taking stock of your assets
  - Prioritizing the assets
  - Establishing an MSB
  - Implement security controls with CIS/DISA/Other benchmarks
  - Basic/broader security hardening
- Note that Stage 1 (Hardening) and Stage 2 (Patching) are shown sequentially to show priority
- In practical terms, the two efforts may be done slightly staggered depending upon resources available
- Establish one program and then the other
- Stage 1 (Hardening) is equivalent to tightening all the screws on machinery and will reduce impact of an attack (like a shield)

- Stage 2 (Patching) will seal all the entry points for an attacker to gain access or to penetrate a system
- Note that both Stage 1 and Stage 2 are equally important and necessary and assist in enhancing the security posture in their unique manner

Topic no 124: Security Breach Case Study 1: Home Dept 2014

- 56 million payment cards compromised
- Early September 2014
- Sequence of events:
  - The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials
  - Then they exploited a zero-day vulnerability in Windows, which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment.
  - Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014).
  - This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014).
  - The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.
- Home Depot didn't have secure configuration of the software or hardware on the POS terminals.
- There was no proof of regularly scheduled vulnerability scanning of the POS environment.
- They didn't have proper network segregation between the Home Depot corporate network and the POS network.
- Overall: several controls missing, vendor management of IDs and access management missing, and monitoring of the network was missing

Topic no 125: Security Breach Case Study 2: Anthem

- Health Insurer Anthem
- Affected 78.8 million individuals

- **Sequence of events:**
  - Data breach began on Feb. 18, 2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content

- Opening the email launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's data warehouse
- Starting with the initial remote access, the attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information and make changes in the environment
- The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse a system that stores a large amount of consumer personally identifiable information
- Queries to that data warehouse resulted in access to an ex filtration of approximately 78.8 m unique user records

- **Vulnerabilities:**
  - Exploitable vulnerabilities were found in anthem network
  - User security awareness training conducted to prevent phishing and social engineering
- **Remediation measures:**
  - Implemented two-factor authentication on all remote access tools, deployed a privileged account management solution and added enhanced logging resources to its security event and incident management solutions
  - Further, the company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication and created new Network Admin IDs

Topic no 126: Best Practices For Applying Security Patches

- "The risk of implementing the service pack, hotfix and security patch should ALWAYS be LESS than the risk of not implementing it."
- “You should never be worse off by implementing a service pack, hotfix and security patch. If you are unsure, then take steps to ensure that there is no doubt when moving them to production systems.”

1. Use a change control process

- A good change control procedure has an identified owner, a path for customer input, an audit trail for any changes, a clear announcement and review period, testing procedures, and a well- understood back-out plan.
- Change control will manage the process from start to finish

2. Read all related documentation:

- Before applying any service pack, hotfix or security patch, all relevant documentation should be read and peer reviewed. The peer review process is critical as it mitigates the risk of a single person missing critical and relevant points when evaluating the update
- Ensure the update is relevant, and will resolve an existing issue
- Ensure adoption won't cause other issues resulting in a compromise of the production system
- There are dependencies relating to the update, (i.e. certain features being enabled or disabled for the update to be effective.)
- Potential issues will arise from the sequencing of the update, as specific instructions may state or recommend a sequence of events or updates to occur before the service pack, hotfix or security patch is applied

3. Apply updates on a need-only basis
4. Testing
5. Plan to uninstall
6. Working backup and production downtime
7. Always have roll-back plan
8. Don’t get more than 2 service packs behind

Topic no 127: Who Conducts Vulnerability Management

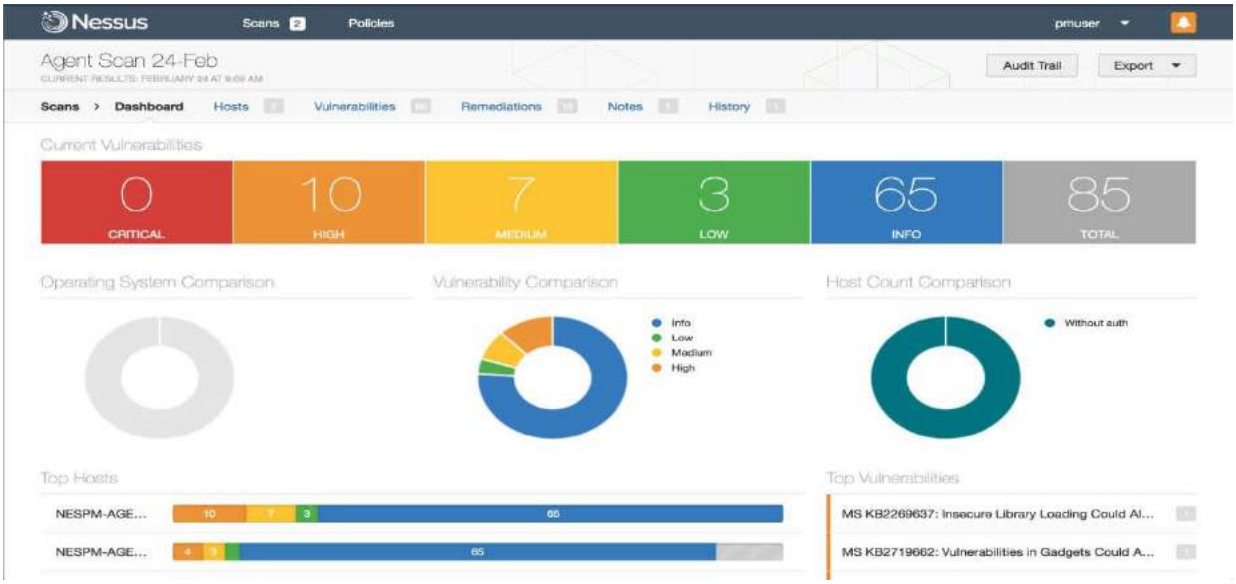
- A number of teams and resources may be involved in the VM lifecycle

SN	ACTIVITY	TEAM	SUPPORTED BY
1	ANALYZE ASSETS	INFOSEC	IT OPS TEAM
2	PREPARE SCANNER	INFOSEC	-
3	RUN VULNERABILITY SCAN	INFOSEC	-
4	ASSESS RESULTS	INFOSEC	IT OPS TEAM
5	TEST & PATCH SYSTEMS	IT OPS TEAM	INFOSEC
6	VERIFY (RE-SCAN)	INFOSEC	IT OPS TEAM
7	REPORT FINDINGS	INFOSEC	IT STEERING COMMITTEE

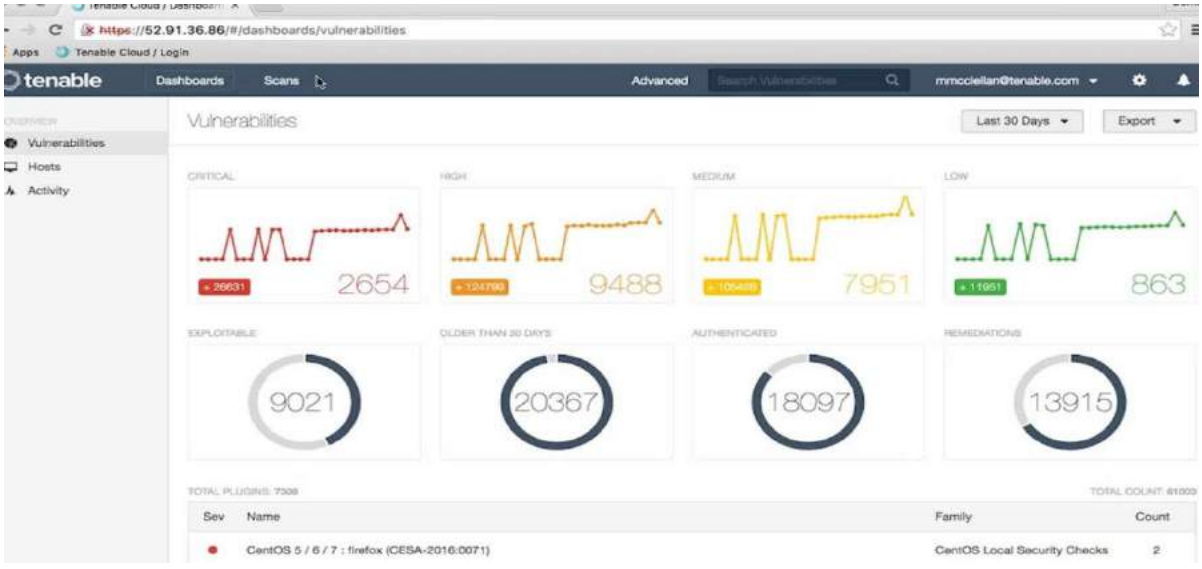
- **Role of Infosec team:**
  - Takes the primary ownership of the vulnerability management process
  - Runs scanning after coordinating with the relevant IT Ops team
  - Shares scanning reports with IT teams and management
  - Tracks remediation timelines
  - Understands criticality issues and helps to prioritize
  - Studies the security patch details as a backup resource
  - Assists with change management process
- **Role of IT Ops team:**
  - Owner of the IT asset
  - Receives the vulnerability scan report from Infosec team
  - Studies the vulnerability
  - Understands criticality, impact, & dependencies
  - Helps Infosec team develop a project plan (if required) and timelines for the patching
  - Tests the patches in test environment
  - Takes backups, develops roll-back plan
  - Takes downtime and takes ownership of the change management process
  - Implements the patches
  - Monitors the systems after patch implementation
  - Rolls-back if necessary
  - Creates the necessary documentation

Topic no 128: Nessus Features

- Lets take a look at Nessus features
- Nessus (Reports):
  - Customize reports to sort by vulnerability or host
  - Create an executive summary or compare scan results
  - Targeted email notifications of scan results
- Nessus (Scan Types):
  - Asset discovery
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening & missing patches
- Nessus (Compliance & Config Scans):
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA
- Nessus (Risk scores):
  - Vulnerability ranking based on CVE, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk
- Nessus is a cost-effective scanner that gets most of the job done for vulnerability scanning
- It has CIS and DISA compliance templates
- Has some flaws and bugs but overall useful tool

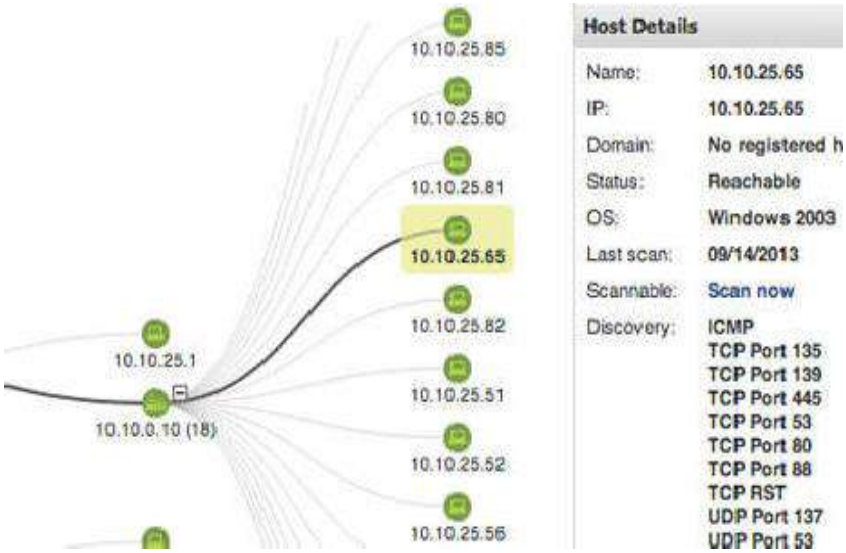

Nessus
Scans
Policies
pmuser
Agent Scan 24-Feb
Audit Trail
Export
Scans > Dashboard
Hosts
Vulnerabilities
Remediations
Notes
History
Current Vulnerabilities
0
CRITICAL
10
HIGH
7
MEDIUM
3
LOW
65
INFO
85
TOTAL
Operating System Comparison
Vulnerability Comparison
Info
Low
Medium
High
Host Count Comparison
Without auth
Top Hosts
NESPM-AGE...
NESPM-AGE...
Top Vulnerabilities
MS KB2269637: Insecure Library Loading Could Al...
MS KB2719662: Vulnerabilities in Gadgets Could A...

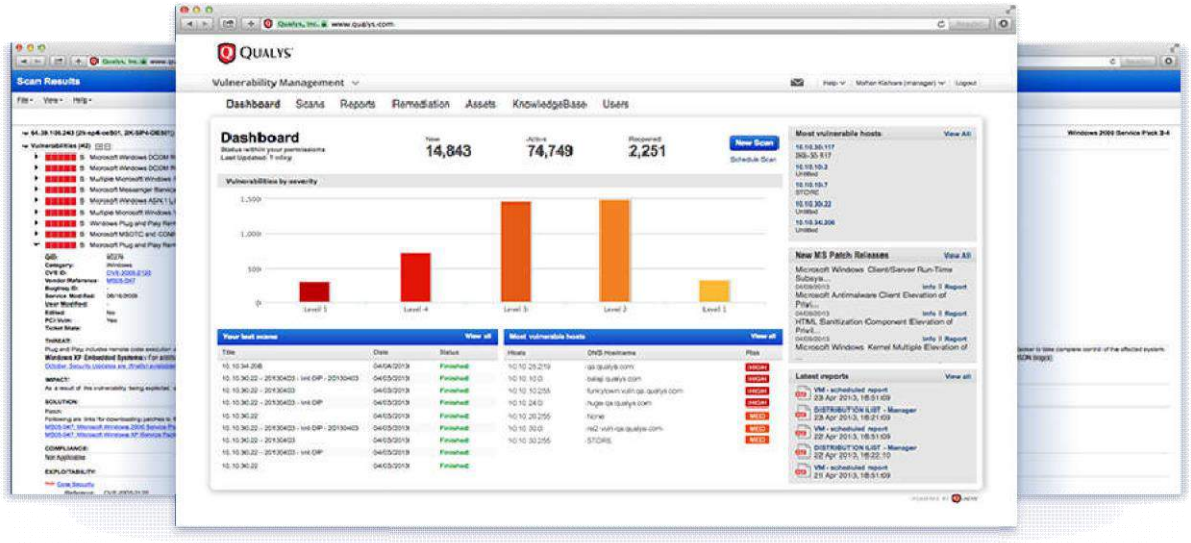

RI Office
Scans > Hosts
Vulnerabilities
Remediations
Hide Details
Host
Vulnerabilities
%
192.168.1.243
192.168.1.123
192.168.1.247
192.168.1.106
192.168.1.1
192.168.1.234
192.168.1.226
192.168.1.250
Scan Details
Name: RI Office
Folder: N/A
Status: Running
Policy: Internal Network Scan
Scanner: Scanner 2
Start time: Wed Dec 11 07:41:24 2013
Vulnerabilities
Info
Low
Medium
High
Critical

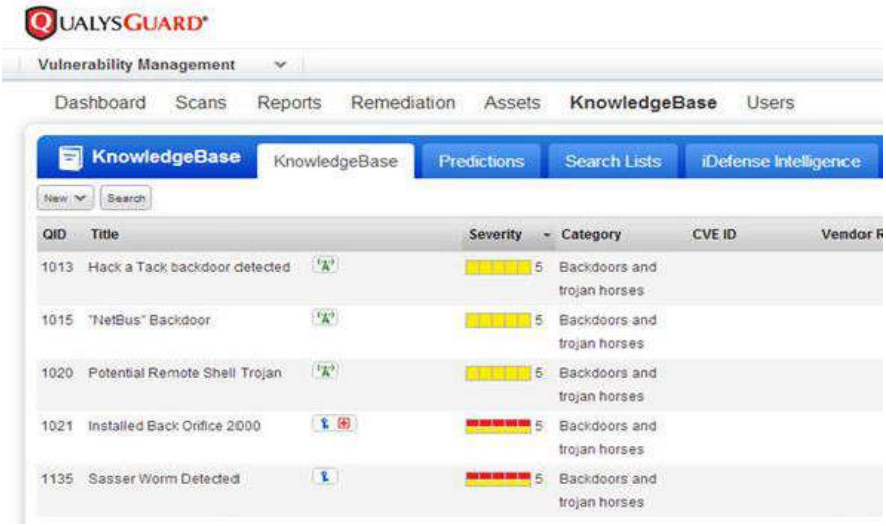

https://52.91.36.86/#/dashboards/vulnerabilities
Apps
Tenable Cloud / Login
tenable
Dashboards
Scans
Advanced
mmcclellan@tenable.com
Vulnerabilities
Hosts
Activity
Vulnerabilities
Last 30 Days
Export
CRITICAL
2654
HIGH
9488
MEDIUM
7951
LOW
863
EXPLOITABLE
9021
OLDER THAN 30 DAYS
20367
AUTHENTICATED
18097
REMEDIATIONS
13915
Sev
Name
Family
Count
CentOS 5 / 6 / 7 : firefox (CESA-2016:0071)
CentOS Local Security Checks
2

Topic no 129: Qualys Features

- Qualys:
  - Cloud-based service
  - On-premise device
  - Complete suite
  - Scalable and immediate deployment
  - Asset discovery; find and organize hosts
  - Prioritize & manage remediation tickets
  - Continuous monitoring service
  - Policy compliance scanning
  - Qualys Secure Seal for websites







- Qualys:
  - Website scanning

  - compliance
  - Annual subscription service model

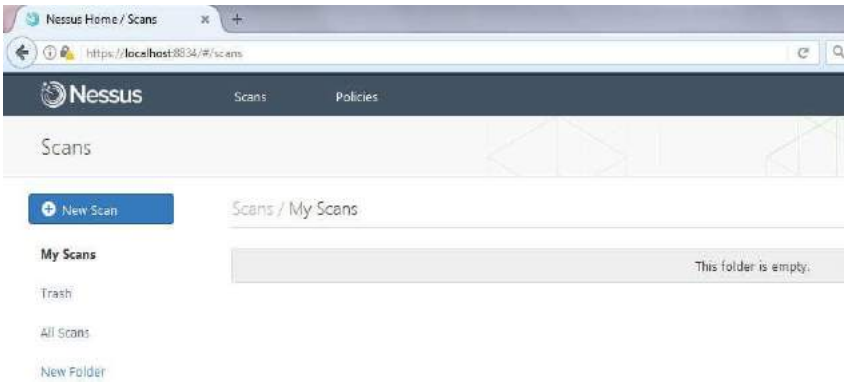
- Qualys is a convenient and scalable VM tool that comes with several modules
- Subscription-based pricing model which can be expensive
- Several advantages due to cloud-based service

Topic no 130: Nessus Demo – 1

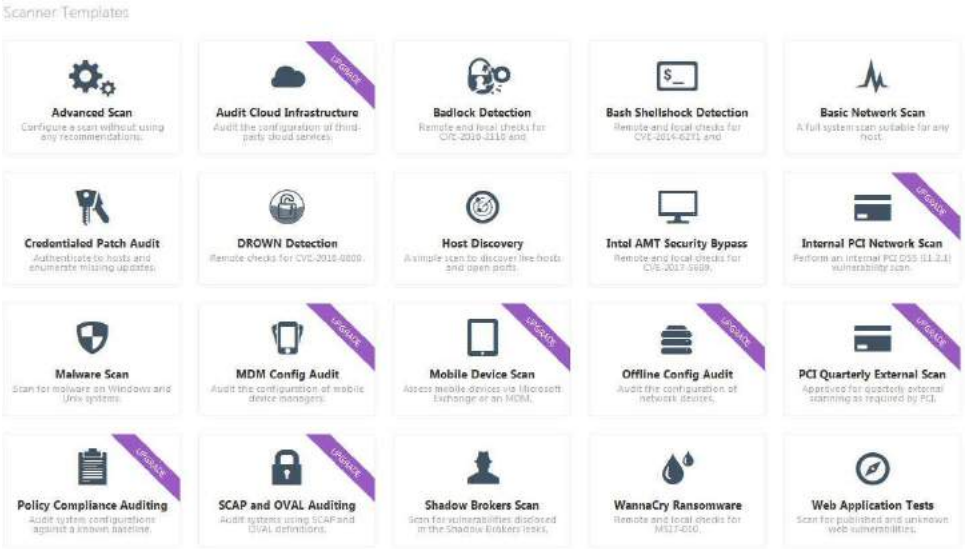
- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

LOGIN SCREEN

DASHBOARD

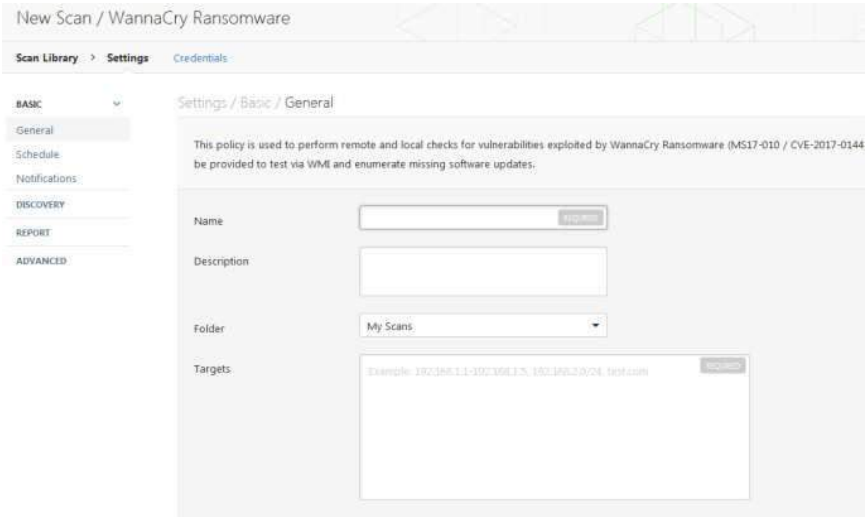


NEW SCAN



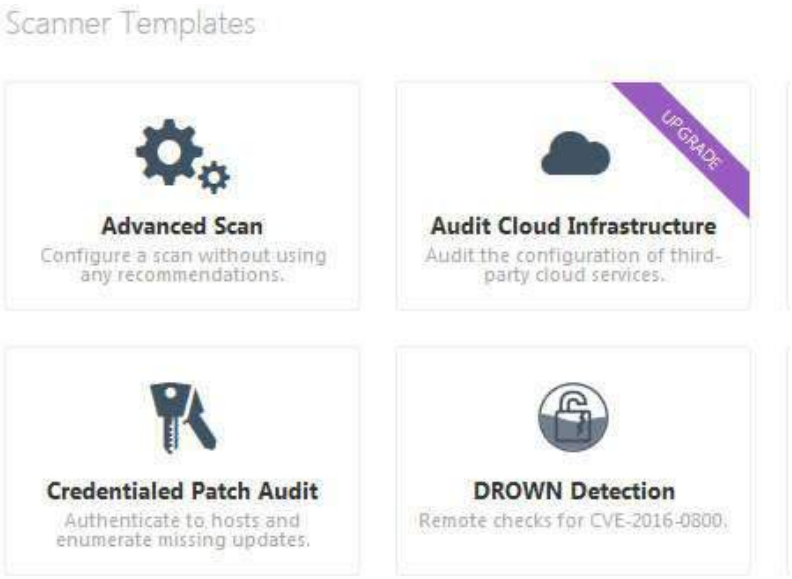
WANNACRY RANSOMWARE SCAN

NEW SCAN WINDOW

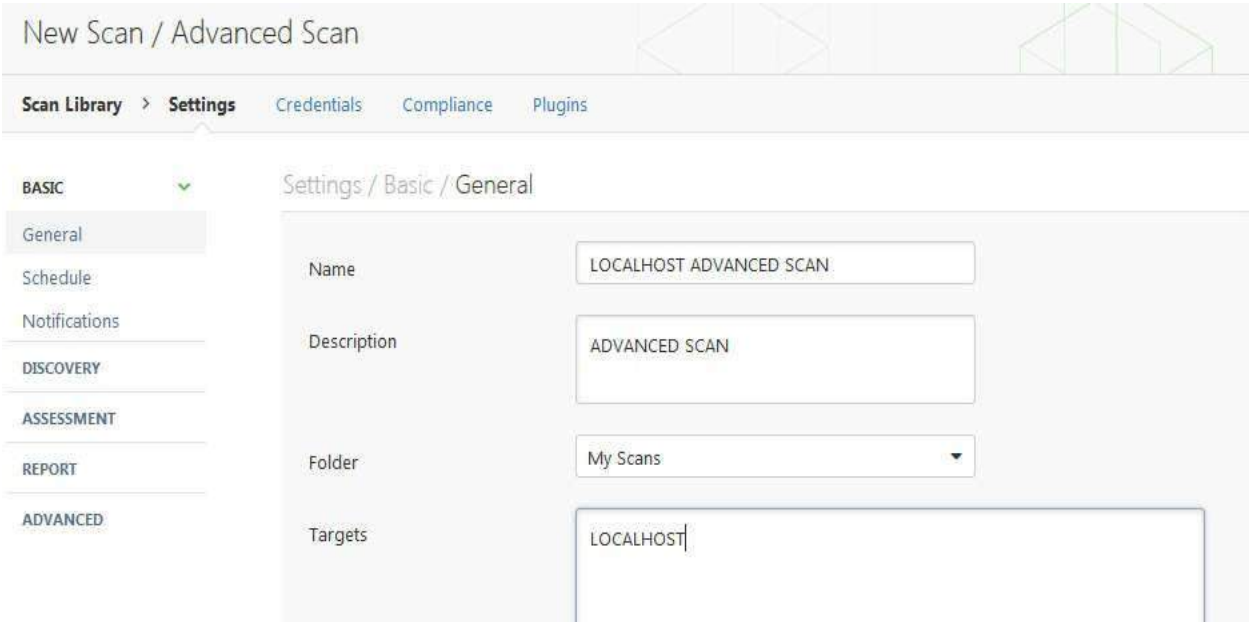


DASHBOARD VIEW WITH SCANS

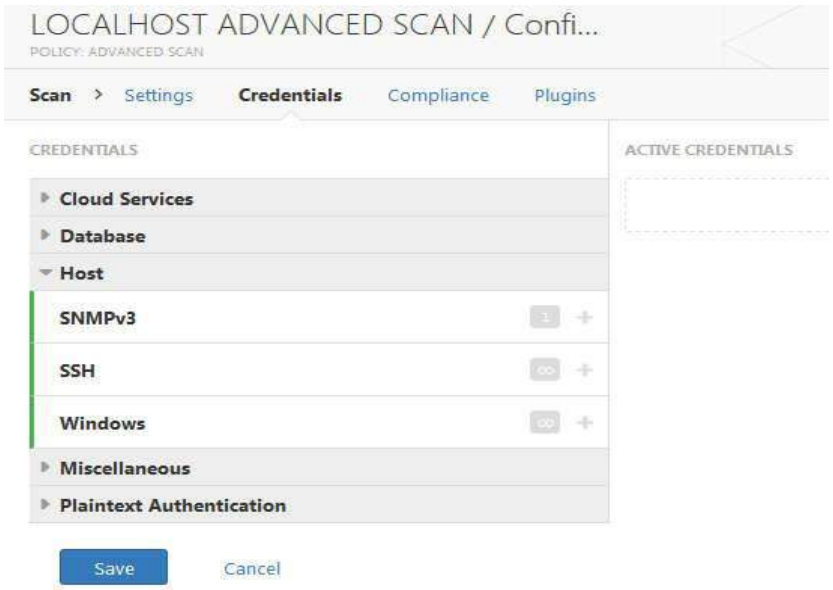
NEW SCAN…



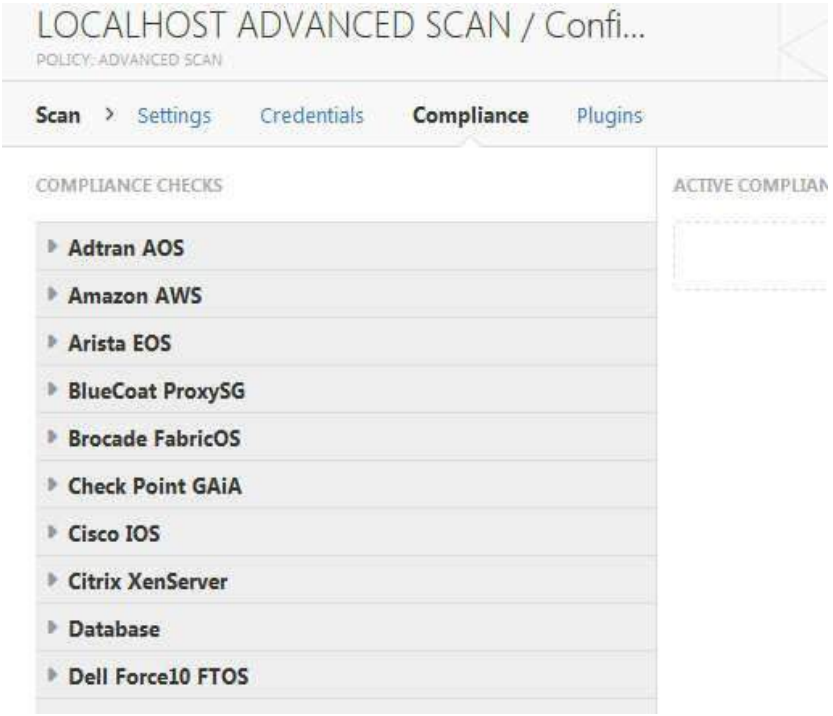
ENTER SCAN DETAILS



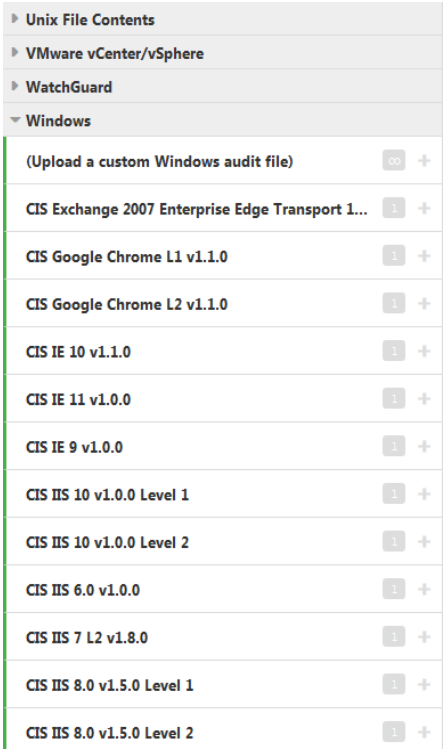
CREDENTIAL SCAN



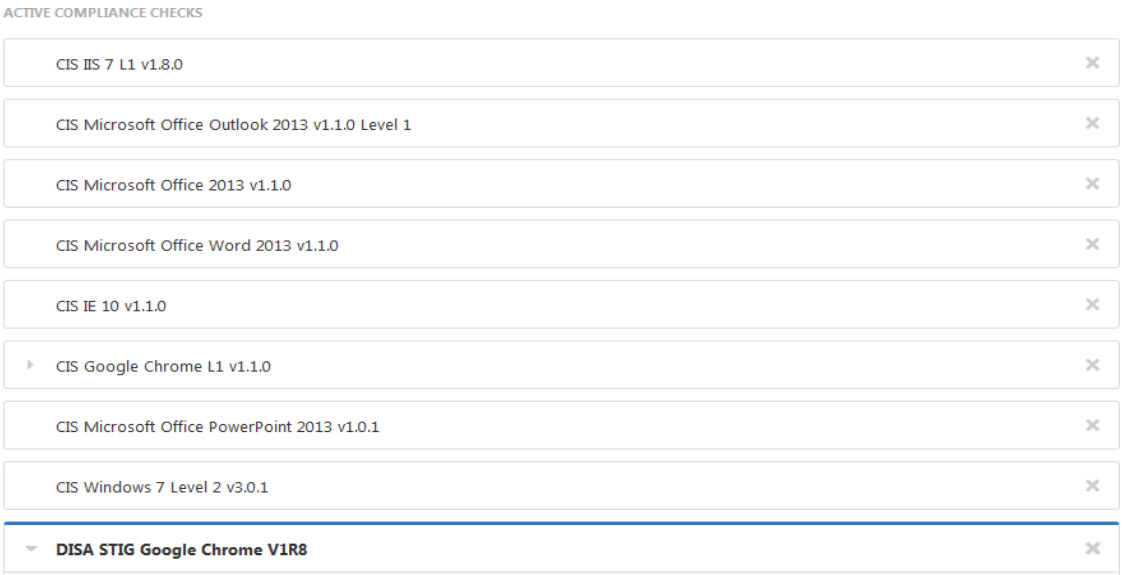
COMPLIANCE SCAN



WINDOWS COMPLIANCE MENU (CIS)



WINDOWS COMPLIANCE MENU (CIS)…

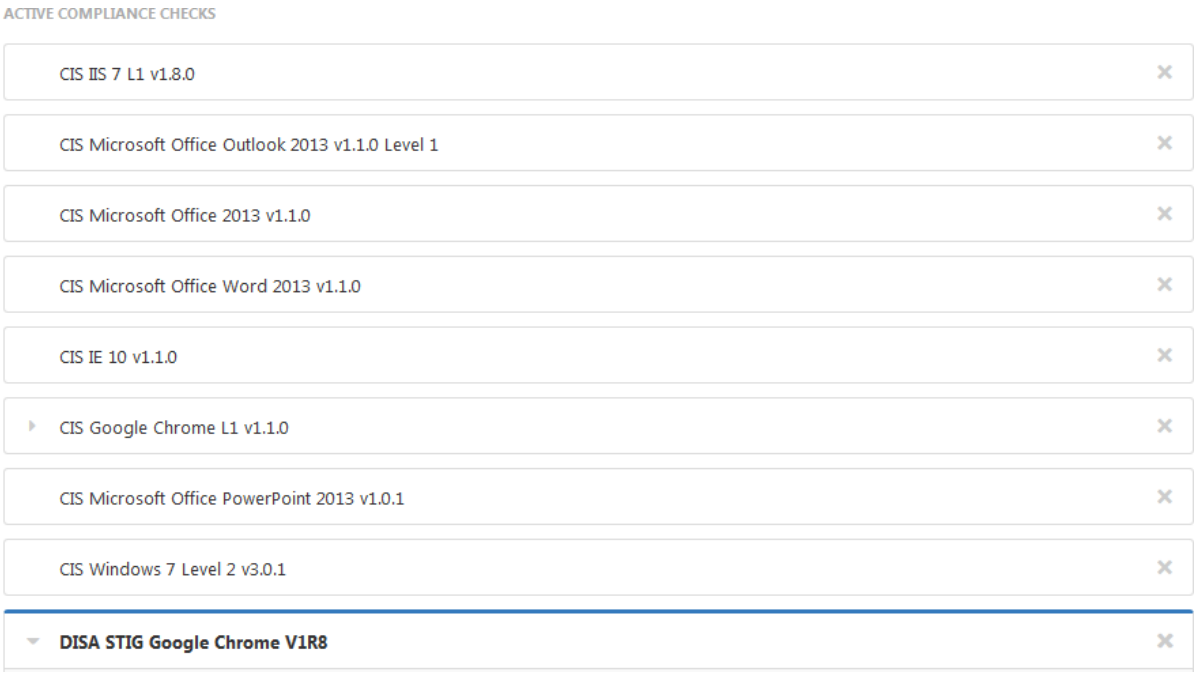


- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

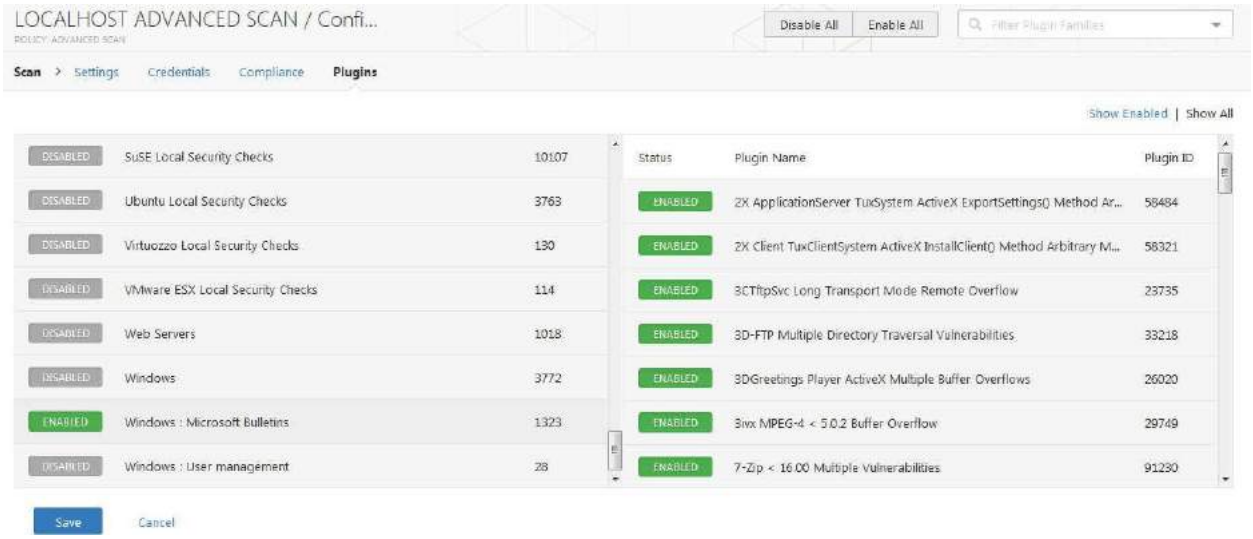
Topic no 131: Nessus Demo – 2

- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

- **ADVANCED SCAN / COMPLIANCE**

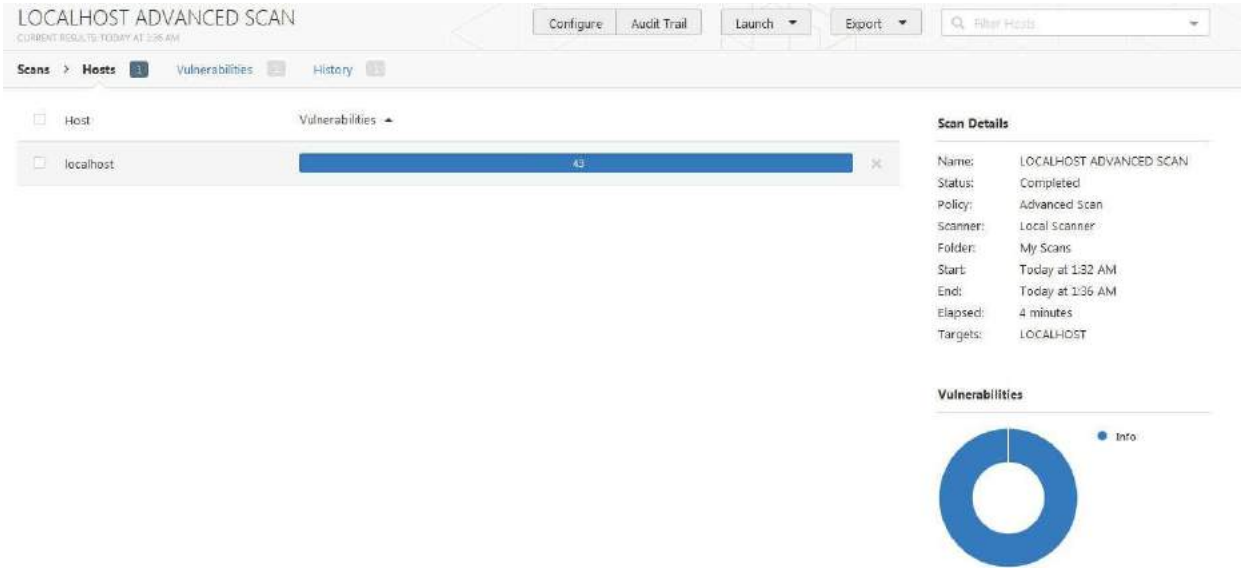


ADVANCED SCAN / PLUG-INS

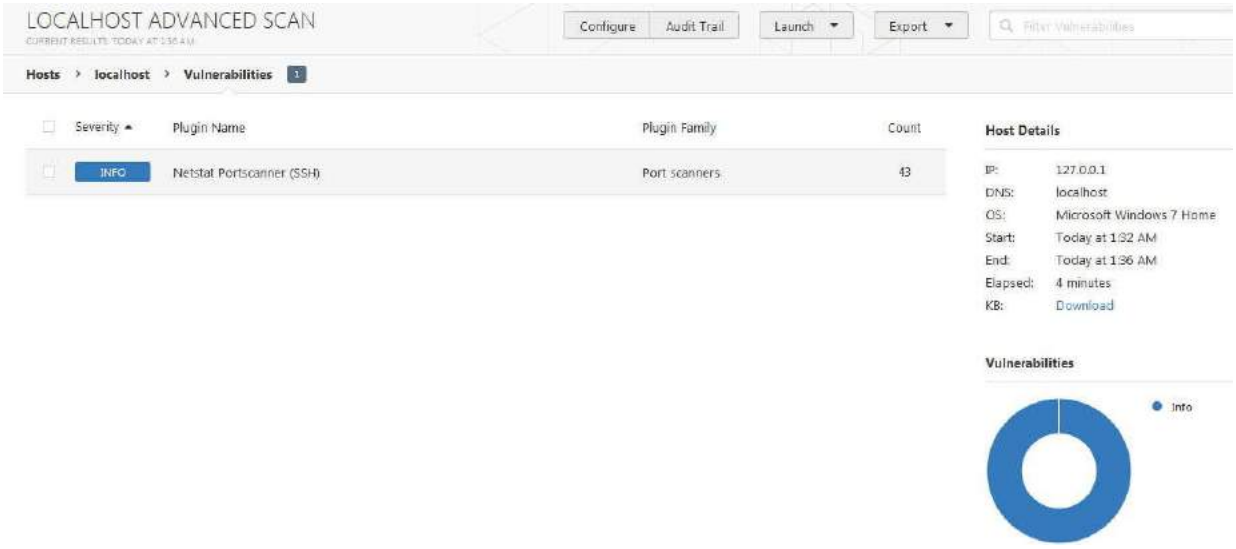


SCAN…IN PROGRESS

SCAN REPORT [43 INFO]



SCAN REPORT [DETAILS]



SCAN REPORT [DETAILS…]

https://en.wikipedia.org/wiki/Netstat

Output

```
Port 68/udp was found to be open
```

Port	Hosts
68 / udp	localhost

```
Port 123/udp was found to be open
```

Port	Hosts
123 / udp	localhost

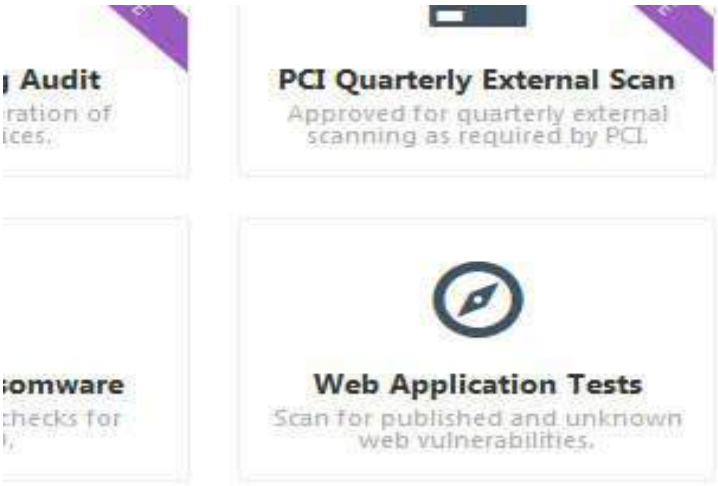
```
Port 135/tcp was found to be open
```

Port	Hosts
135 / tcp / epmap	localhost

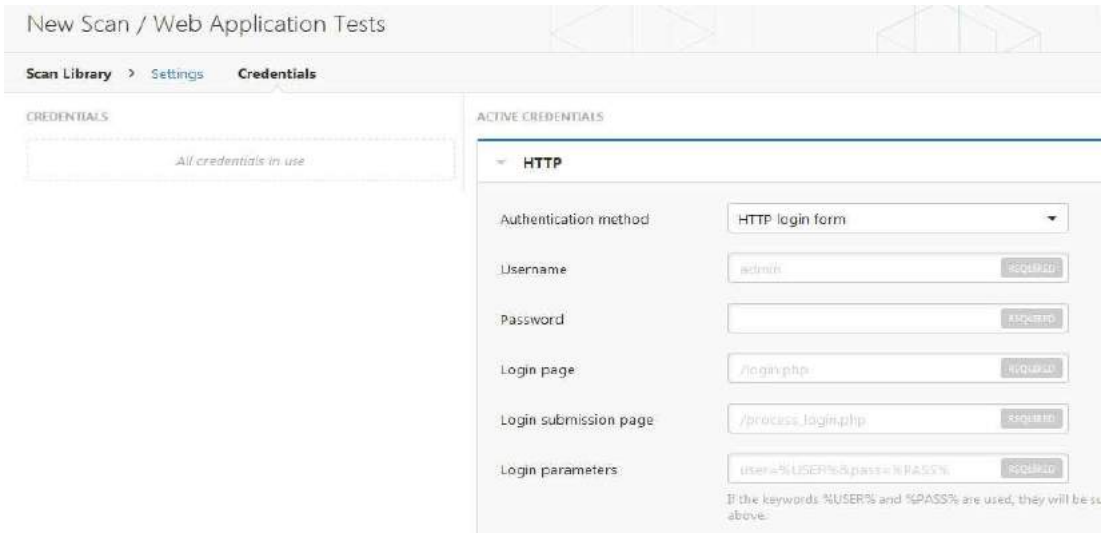
```
Port 137/udp was found to be open
```

Port	Hosts
137 / udp	localhost

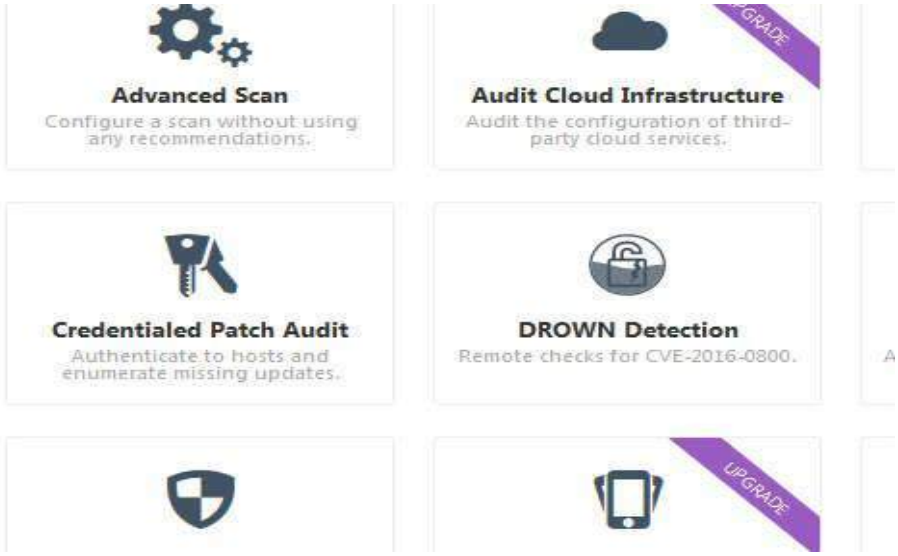
WEB APPLICATION TEST



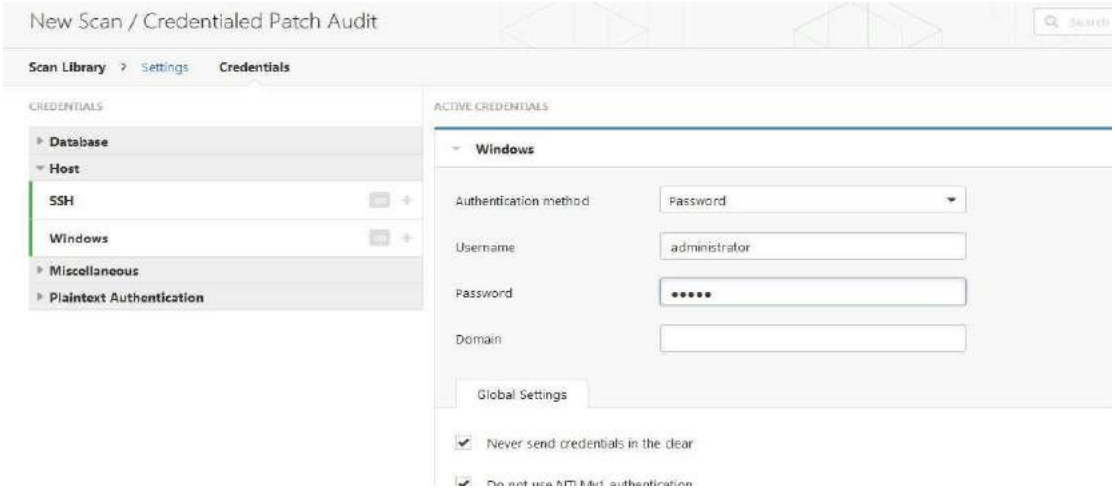
WEB APPLICATION TEST - CREDENTIALS



CREDENTIALED PATCH AUDIT

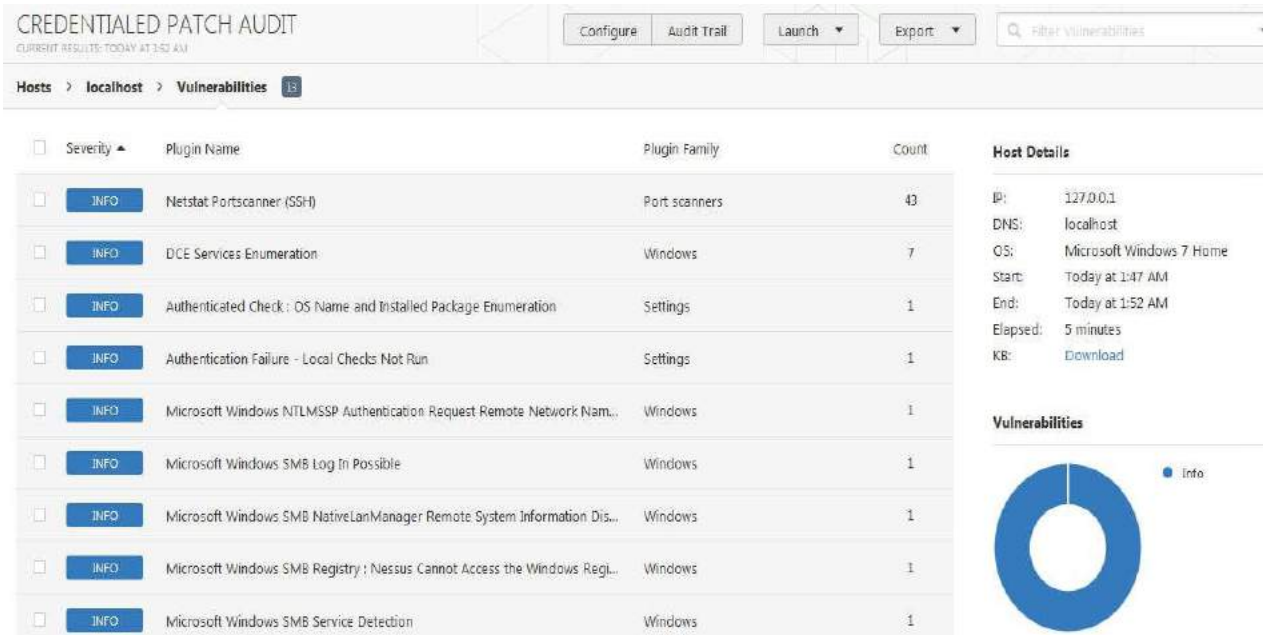


CREDENTIALED PATCH AUDIT

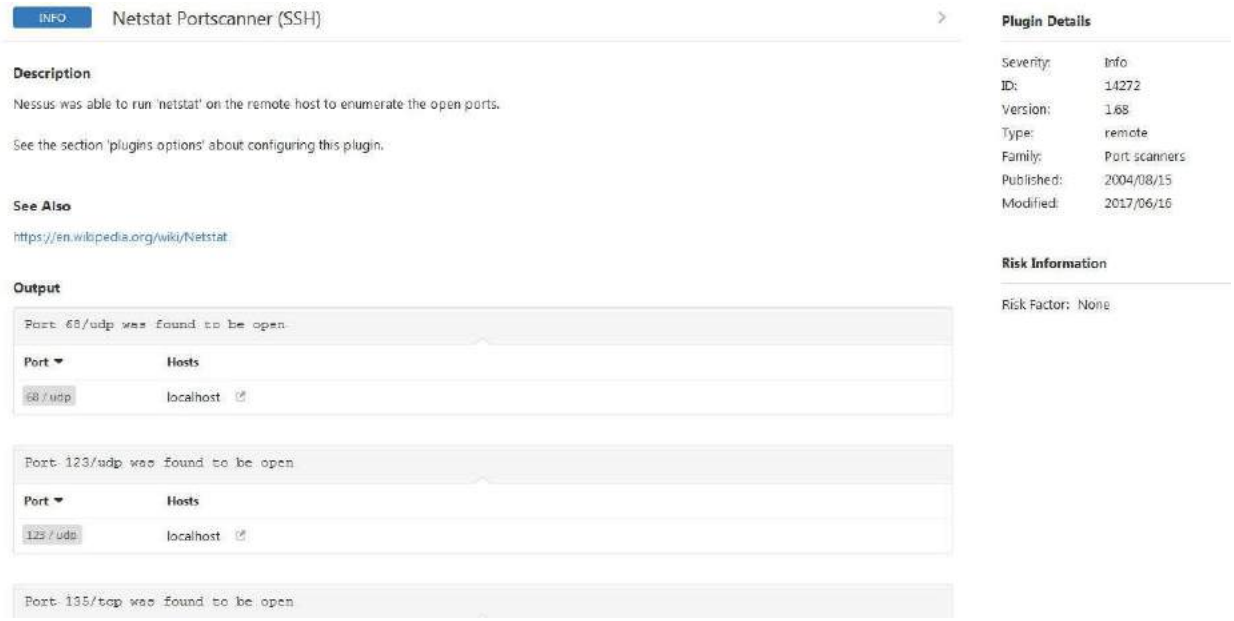


SCANS DASHBOARD

- **CREDENTIALED AUDIT SCAN RESULTS [61 INFO]**



CREDENTIALED AUDIT SCAN RESULTS [DETAILS]



Topic no 136: How Do VM Scanners Work?

- Lets take a look at Qualys scanning technique:
- QualysGuard scanning methodology mainly focuses on the different steps that an attacker might follow in order to perform an attack.
- It tries to use exactly the same discovery and information gathering techniques that will be used by an attacker.

  - **Checking if the remote host is alive**
  - The first step is to check if the host to be scanned is up and running in order to avoid wasting time on scanning a dead or unreachable host
  - This detection is done by probing some well-known TCP and UDP ports. If the scanner receives at least one reply from the remote host, it continues the scan
  - **Firewall detection**
  - The second test is to check if the host is behind any firewalling/filtering device. This test enables the scanner to gather more information about the network infrastructure and will help during the scan of TCP and UDP ports.
  - **TCP / UDP Port scanning**
  - The third step is to detect all open TCP and UDP ports to determine which services are running on this host. The number of ports is configurable, but the default scan

is approximately 1900 TCP ports and 180 UDP ports.

- **OS Detection**
- Once the TCP port scanning has been performed, the scanner tries to identify the operating system running on the host.
- This detection is based on sending specific TCP packets to open and closed ports.

- **TCP / UDP Service Discovery**
- Once TCP/UDP ports have been found open, the scanner tries to identify which service runs on each open port by using active discovery tests

- **Vulnerability assessment based on the services detected**
- Once the scanner has identified the specific services running on each open TCP and UDP port, it performs the actual vulnerability assessment.
- The scanner first tries to check the version of the service in order to detect only vulnerabilities applicable to this specific service version. Every vulnerability detection is non-intrusive, meaning that the scanner never exploits vulnerability if it could negatively affect the host in any way.

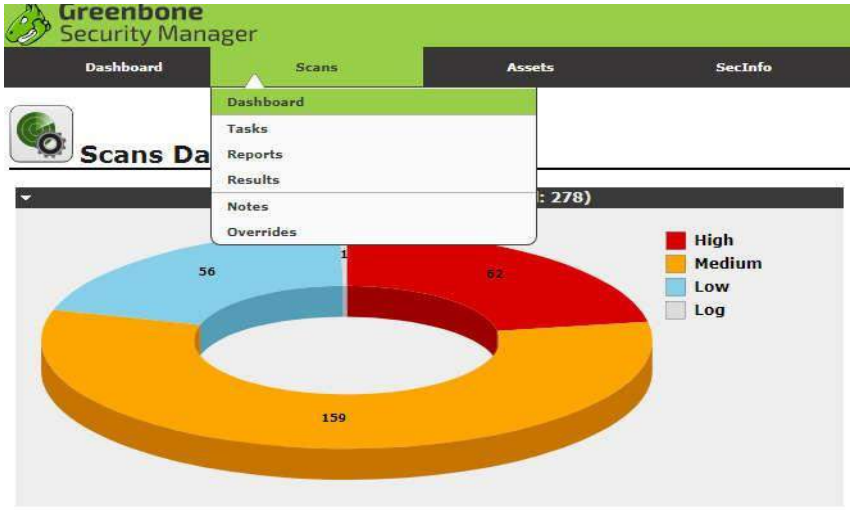
- **Limitations:**

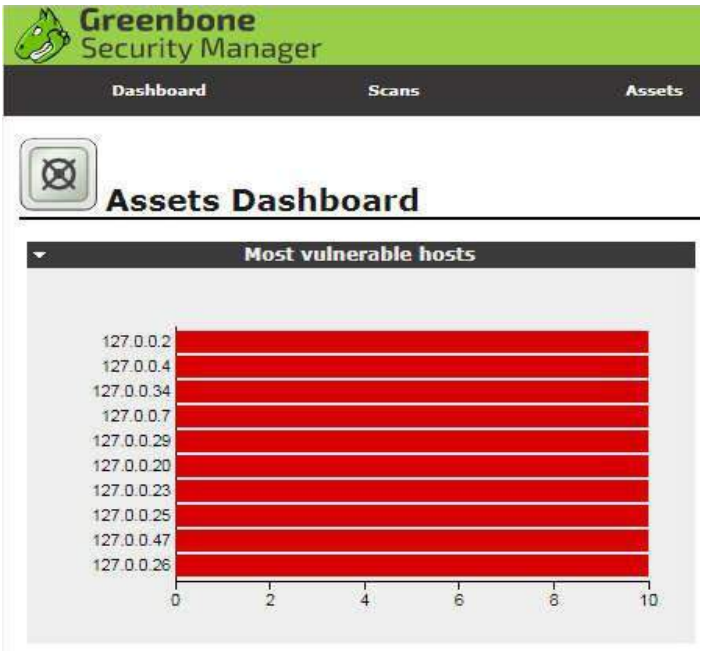
a. Vulnerability scanners work in the same manner as antivirus programs do by using databases that store descriptions of different types of vulnerabilities

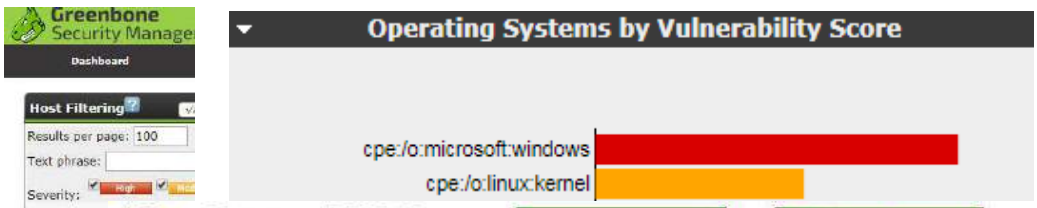
b. False positive or false negative rate

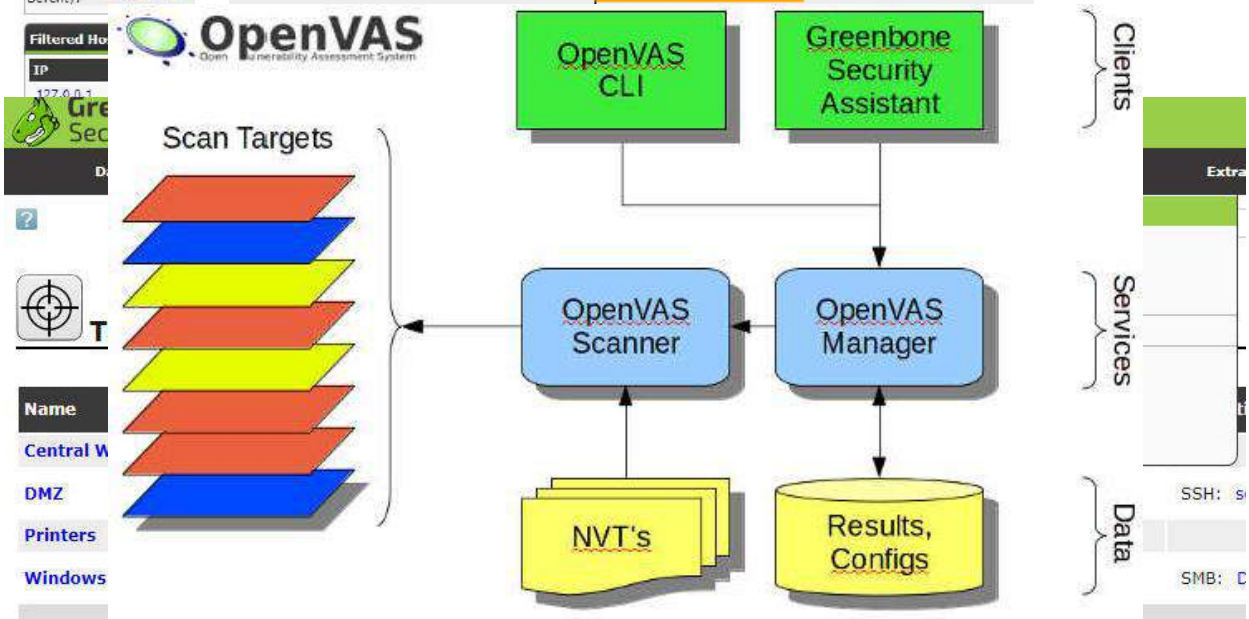
Topic no 139: Open Source Vulnerability Scanners

- Lets take a look at OpenVAS
- http://www.openvas.org/livedemo.html
- Login and password: livedemo


Greenbone
Security Manager
Dashboard
Scans
Assets
SecInfo
Dashboard
Tasks
Reports
Results
Notes
Overrides
Scans Da
: 278)
56
62
159
High
Medium
Low
Log


Greenbone
Security Manager
Dashboard
Scans
Assets
Assets Dashboard
Most vulnerable hosts
127.0.0.2
127.0.0.4
127.0.0.34
127.0.0.7
127.0.0.29
127.0.0.20
127.0.0.23
127.0.0.25
127.0.0.47
127.0.0.26
0
2
4
6
8
10


Operating Systems by Vulnerability Score
cpe:/o:microsoft:windows
cpe:/o:linux:kernel


OpenVAS
Scan Targets
OpenVAS CLI
Greenbone Security Assistant
OpenVAS Scanner
OpenVAS Manager
NVT's
Results, Configs
Clients
Services
Data

Topic no 140: Suggested Frequency For VM Scanning

APPROXIMATELY 50k NETWORK VULNERABILITY TESTS

- OpenVAS is a simple, free (opensource) VA scanner
- It has source code documentation, virtual images for download, and mailing lists on its website

- **Pre-requisites**
  - Information security team
  - Vulnerability management policy
  - Inhouse scanner or openvas tool
  - Trained staff
- **At the start:**
  - Organizations scanning once a year or not at all
  - Vulnerabilities identified by internal scanning or external VA report
  - Not remediated

- Lack of discipline and management support

- **As organizations get more mature in scanning discipline:**
  - Quarterly scan
  - Quarterly remediation by IT teams
  - Quarterly report to IT Steering Committee
- **Mature organizations:**
  - Monthly scan
  - Monthly remediation
  - Quarterly or bi-annual external VA/PT
  - Monthly reports to IT Steering Committee
- **Most mature organizations:**
  - Fortnightly scan
  - Fortnightly remediation
  - Monthly reporting

Topic no 141: VM Challenges & Pitfalls

- **Challenges:**
  - Internal expertise on VM tool
  - Not enough support from IT teams
  - Vulnerability patching causing application failure
  - Management support

- **Internal expertise on VM tool**
  - Not too much expertise required
  - Create testbed
  - Monitor traffic pattern
  - Train staff if possible
  - Patch small portions of the network first
- **Not enough support from IT teams:**
  - Create reports and share among IT management
  - Highlight and educate risks to IT management and board
  - Create departmental competition and relationship-building
- **Patching causing application failure:**
  - In test environment create work around or compensating controls
  - Test the compensating controls
  - Document the compensating controls
- **Not enough management support:**
  - Share reports with management highlighting recent incidents
  - Share industry-specific or geographically relevant breach reports
  - Create awareness

Topic no 142: IT Asset Management Challenges

- The typical enterprise has hundreds or thousands of IT assets with a fast-paced business environment
- Tough challenge to keep all IT assets tracked and updated with all the right software patches and updates
- **Challenges:**
  - Asset discovery & tracking
  - Antivirus status
  - Windows & OS updates
  - Patch management
  - Change management
- **Asset discovery & tracking**

- New assets added & old assets removed
- Temporary or replacement machines
- Travelling staff
- Test beds
- Vendor environments

- **Antivirus status:**
  - Working and updated antivirus critical to a security managed network
  - Geographically dispersed network
  - Some stations not responding or updating
- **Windows & OS updates:**
  - Windows, Linux, Unix, AIX and database systems
  - Vendor patches from multiple sources
  - Testing the patches
  - Acquiring downtime windows
  - Monitoring the performance
- **Patch management:**
  - Scanning for vulnerabilities
  - Passing on reports to IT teams
  - Tracking the remediation
  - Re-scanning for verification
  - Reporting to management
- **Change management:**
  - Change management inherent to all change processes
  - Change management requires reviews and approvals
  - Configuration management database or repository

Topic No 144: ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- Asset management helps with the following security functions:

1. Patch management
2. Software whitelisting
3. Software assets discovery and management
4. Enterprise tracking and reporting

- Gartner refers to this area as Unified endpoint management (UEM):

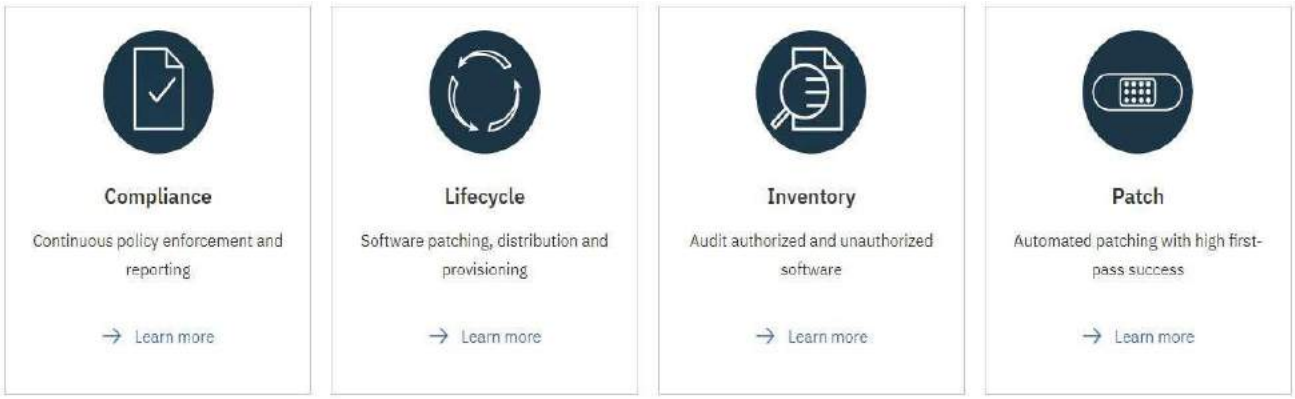
GARTNER MAGIC QUADRANT FOR

UNIFIED ENDPOINT MANAGEMENT 2018

- Unified endpoint management (UEM) tools combine the management of multiple endpoint types in a single console. :

GARTNER UEM 2018 REPORT

1. Configure, manage and monitor iOS, Android, Windows 10 and macOS, and manage some Internet of Things (IoT) and wearable endpoints.
2. Unify the application of configurations, management profiles, device compliance and data protection.
3. Provide a single view of multi device users, enhancing efficacy of end-user support and gathering detailed workplace analytics.
4. Act as a coordination point to orchestrate the activities of related endpoint technologies such as identity services and security infrastructure.



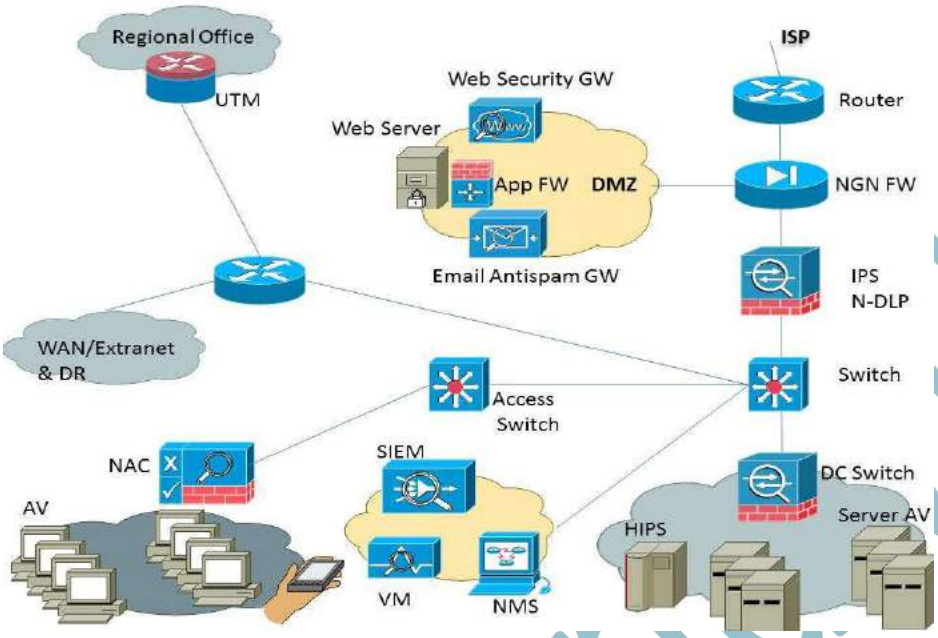
MICROSOFT SOFTWARE RESTRICTION POLICIES (SRP) FOR WHITELISTING

- Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs
- Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.
- You can also use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. Software restriction policies are integrated with Microsoft Active Directory and Group Policy.
- You can also create software restriction policies on stand-alone computers. Software restriction policies are trust policies, which are regulations set by an administrator to restrict scripts and other code that is not fully trusted from running.

Topic No 145: WHAT IS SECURITY ENGINEERING?

- Security Engineering is the third layer of the Security Transformation Model
- Consists of more in-depth and complicated security activities which take more time and effort
- Many times related to security architecture
- **Types of activities for security engineering:**
    - FW granular access lists
    - Building an effective DMZ architecture
    - Segregating the network with VLANs
    - Adding a security tool such as SIEM, FW, DLP, NAC, etc
    - App-DB encryption
- **DMZ Architecture Case Study:**
    - DMZ is an important zone in the overall security architecture
    - Devices which need to communicate to outside world placed in DMZ

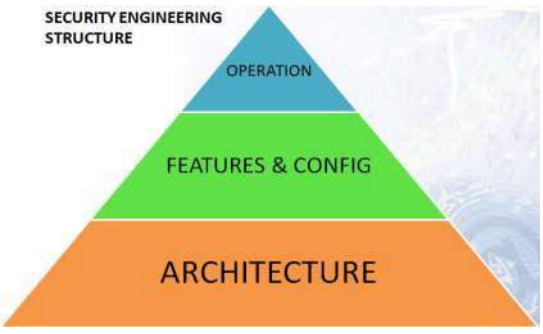
- Web servers, email gateways, web gateways



- **FW Access List Case Study:**
  - Most of the industry has not worked on building granular access lists
  - Most FWs have "allow all" for traffic
  - Granular access lists need to be built based on servers, or traffic flows
- **Why at Layer 3 of Security Transformation Model?**
  - These take time, effort, and often budget approval

Topic No 146: WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING?

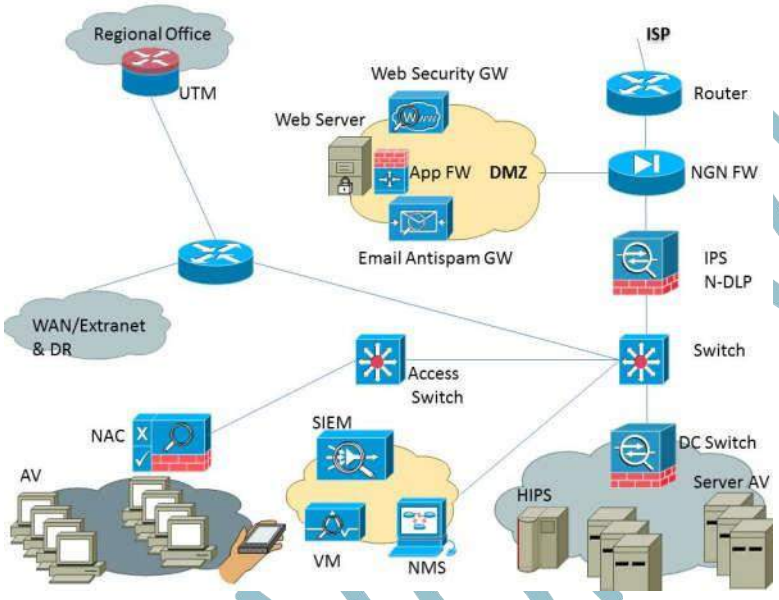
- Security architecture as per best-practices
- The right security devices in the right places
- Effective security configuration of security devices (features)
- Optimum operation of security devices
- Aggregate controls



Examples:

- FW first and then IPS

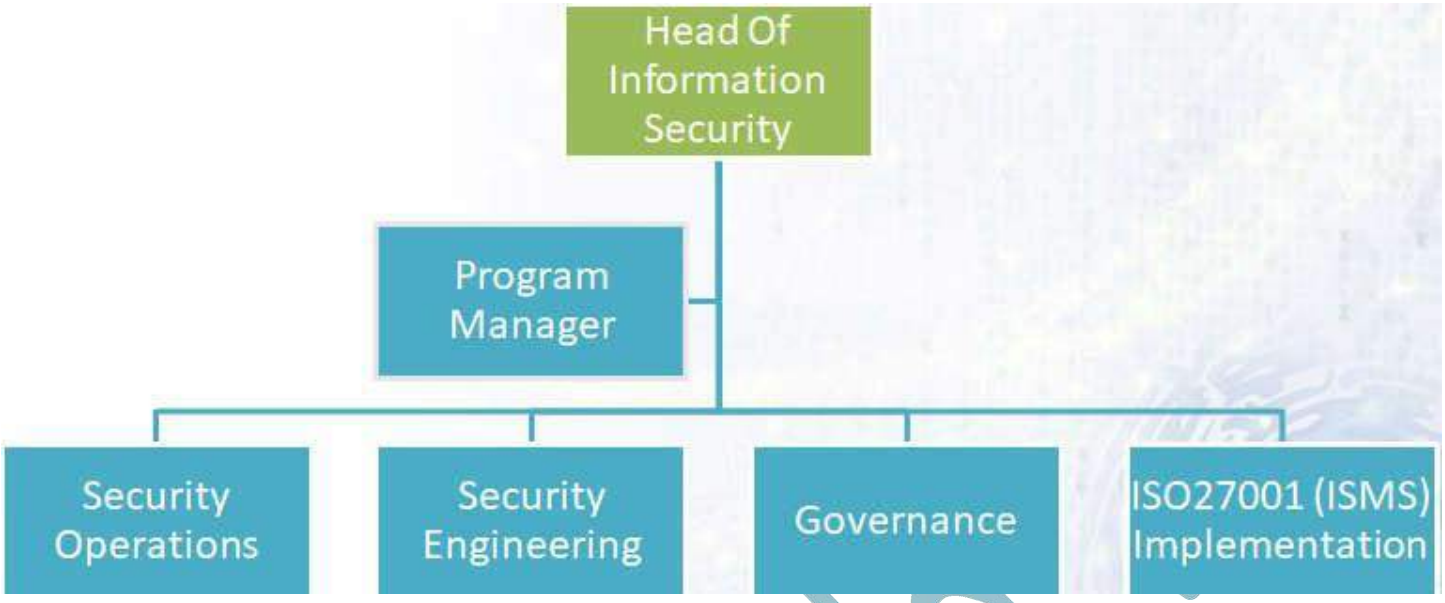
- Edge FW, data center FW
- Malware protection at the network edge
- VPN termination on remote access VPN device
- VPN tunnels for extranet connectivity



implemented

Topic No 147: WHOSE RESPONSIBILITY IS SECURITY ENGINEERING?

TYPICAL STRUCTURE OF AN INFORMATION SECURITY TEAM

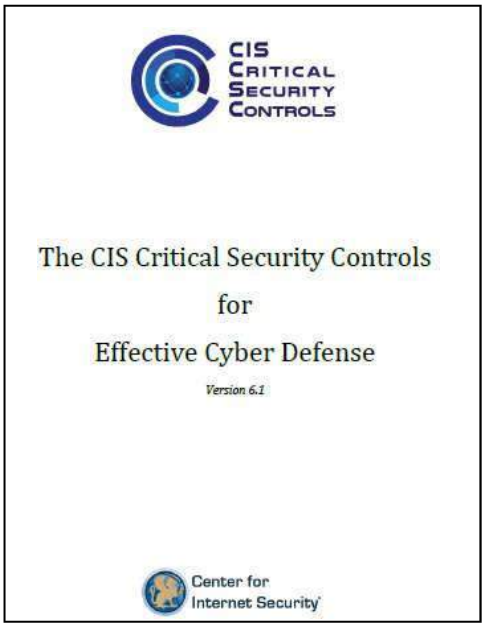


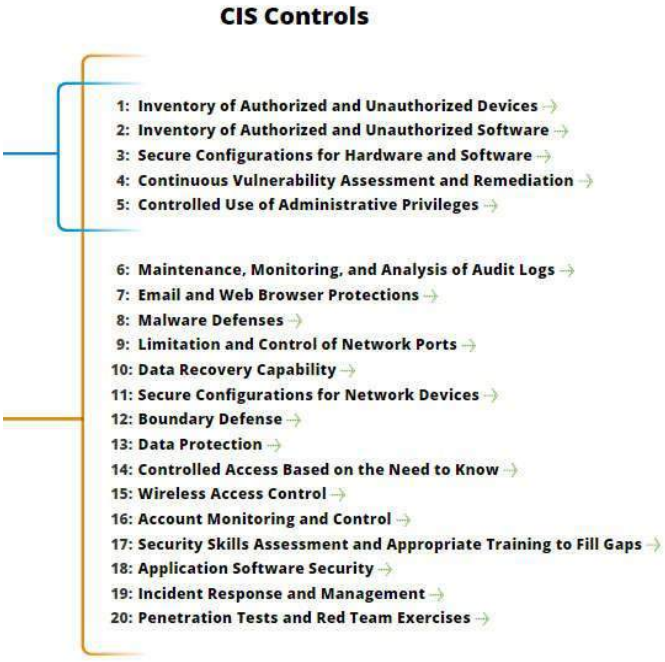
ACTIVITY	TEAM
SECURITY REQUIREMENTS	INFORMATION SECURITY WITH IT CONSULTATION
SECURITY DESIGN	NETWORK/IT SECURITY ASSISTED BY VENDOR
VALIDATING SECURITY DESIGN	INFORMATION SECURITY
SECURITY IMPLEMENTATION	NETWORK/IT SECURITY ASSISTED BY VENDOR
VALIDATING SECURITY REQMTS MET	INFORMATION SECURITY TEAM

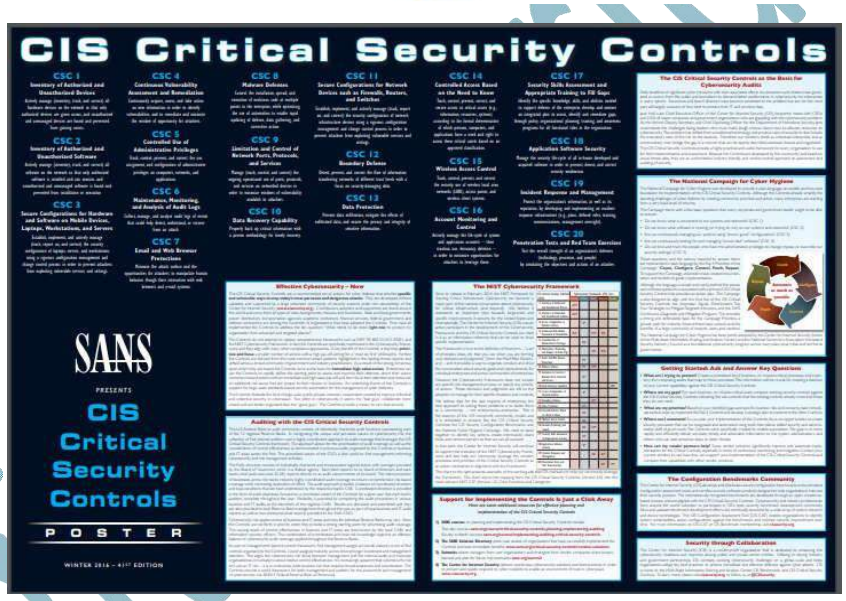
- As Security Engineering involves in-depth knowledge of IT & Security, the necessary resources, knowledge, skills, and people need to be pooled to achieve the objectives effectively

Topic No 148: CIS 20 CRITICAL SECURITY CONTROLS

- What are the CIS 20 Critical Security Controls?







- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services

- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

s

: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systemsconnected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6

employed.

: If configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.

: Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices .

: Maintain an asset inventory of all systems connected to the network and the network devices themselves,recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible

- The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc.
- The asset inventory created must also include data on whether the device is a portable and/or personal device.
- Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

1

network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.

1.6: Use client certificates to validate and authenticate systems prior to connecting to the private network.

Topic No 150: CSC2: Inventory Of Authorized & Unauthorized Software

: Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

: Deploy application whitelisting technology that allows systems to run software only if it is included on the

- The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software.
- Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

: Deploy software inventory tools throughout the organization covering each of the operating system types in

- The software inventory system should track the version of the underlying operating system as well as the applications installed on it.
- The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

: Virtual machines and/or air-gapped systems should be used to isolate and run applications that are requiredfor business operations but based on higher risk should not be installed within a networked environment.

Topic No 151: CSC3-I: Secure Configurations For HW & SW

Establish standard secure configurations of your operating systems and software applications.

- Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system.
- These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

: Follow strict configuration management, building a secure image that is used to build all new systems thatare deployed in the enterprise.

- Any existing system that becomes compromised should be re-imaged with the secure build.
- Regular updates or exceptions to this image should be integrated into the organization's change management processes.
- Images should be created for workstations, servers, and other system types used by the organization.

: Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.

- Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

: Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels.

- Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Topic No 152: CSC3-II: Secure Configurations For HW & SW

: Use file integrity checking tools to ensure that critical system files (including sensitive system and

- The reporting system should have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command).
- These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

: Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur.

- This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system.
- Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

: Deploy system configuration management tools, such as **Active Directory Group Policy Objects** for Microsoft Windows systems or **Puppet for UNIX systems** that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

- They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

Topic No 153 & 154: CSC4-I: Continuous Vuln. Assessment & Remediation

: Run automated vulnerability scanning tools against all systems on the network on a weekly or morefrequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system

administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

- Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common
- Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

: Correlate event logs with information from vulnerability scans to fulfill two goals.

- First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged.
- Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

: Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

- Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
- Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user

: Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at

- Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.

: Deploy automated patch management tools and software update tools for operating system andsoftware/applications on all systems for which such tools are available and safe.

- Patches should be applied to all systems, even systems that are properly air gapped.

: Monitor logs associated with any scanning activity and associated administrator accounts to ensure that thisactivity is limited to the timeframes of legitimate scans

: Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable businessrisk.

- Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.

: Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers,desktops, laptops).

- Apply patches for the riskiest vulnerabilities first.
- A phased rollout can be used to minimize the impact to the organization.
- Establish expected patching timelines based on the risk rating level.

Topic No 155 & 156: CSC5-I: Controlled Use of Administrative Privileges

: Minimize administrative privileges and only use administrative accounts when they are

monitor for anomalous behavior.

: Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

: Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

: Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system

: Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account

: Use multifactor authentication for all administrative access, including domain administrative access Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

: Where multi-factor authentication is not supported, user accounts shall be required to use

: Administrators should be required to access a system using a fully logged and non-administrative account Then, once logged on to the machine without administrative privileges,

the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

: Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Topic No 157 & 158: CSC6-I: MAINTENANCE, MONITORING, ANALYSIS OF AUDIT LOGS

: Utilize Three Synchronized Time Sources: Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent

: Activate audit logging: Ensure that local logging has been enabled on all systems and networking devices.

: Enable detailed logging: Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

: Ensure adequate storage for logs: Ensure that all systems that store logs haveadequate storage space for the logs generated.

: Central Log Management: Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

: Deploy SIEM or Log Analytic Tool: Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

: Regularly Review Logs: On a regular basis, review logs to identify anomalies or abnormal events.

: Regularly Tune SIEM: On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

Topic No 159 & 160: CSC7-I: EMAIL AND WEB BROWSER PROTECTIONS

: Ensure Use of Only Fully Supported Browser & Email Clients: Ensure that only fully supported web browsers & email clients are allowed to execute in the org, ideally only using thelatest version of the browsers & email clients provided by the vendor.

: Disable Unnecessary or Unauthorized Browser or Email Client Plugins: Uninstall or disable any unauthorized browser or email client plugins or add-on applications.

: Limit Use of Scripting Languages in Web Browsers and Email Clients: Ensure that only authorized scripting languages are able to run in all web browsers and email clients.

: Maintain and enforce Network based URL Filters: Enforce network based URL filters that limit a systems ability to connect to websites not approved by the org. This filtering shall beenforced for each of the orgs systems (whether at org facility or not).

: Subscribe to URL-categorization service: Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized websites shall be blocked by default.

: Log all URL requests: Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

: Use of DNS Filtering Services: Use DNS filtering services to help block access to known malicious domains.

: Implement DMARC and Enable Receiver-Side Verification: To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail(DKIM) standards.

7.1o: Sandbox All Email Attachments: Use sandboxing to analyze and block inbound email attachments with malicious behavior.

Topic No 161 & 162: CSC8-I: MALWARE DEFENSES

8.1: Utilize Centrally Managed Anti-malware Software: Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

: Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

: Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available In an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

: Configure Anti-Malware Scanning of Removable Devices: Configure devices so that they automatically conduct an anti-maiware scan of removable media when inserted or connected.

: Configure Devices Not To Auto-run Content: Configure devices to not auto-run content from removable media.

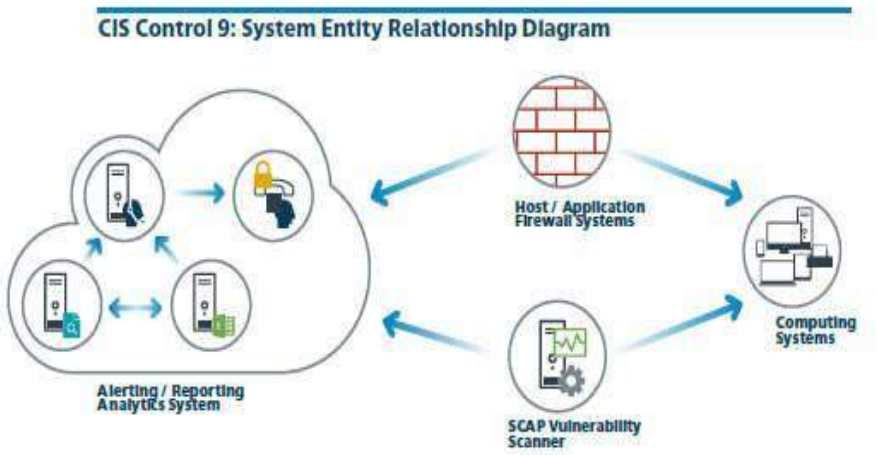
: Centralize Anti-malware Logging: Send all malware detection events to enterprise anti- malware administration tools and event log servers for analysis and alerting.

: Enable DNS Query Logging: Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.

: Enable Command-line Audit Logging: Enable command-line audit logging for commandshells, such as Microsoft Power shell and Bash.

Topic No 163: CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

CIS 20 Critical Security Controls



: Associate Active Ports, Services and Protocols to Asset Inventory

- Associate active ports, services and protocols to the hardware assets in the asset inventory.

: Ensure Only Approved Ports, Protocols and Services Are Running

- Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

: Perform Regular Automated Port Scans

- Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

: Apply Host-based Firewalls or Port Filtering

- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

: Implement Application Firewalls

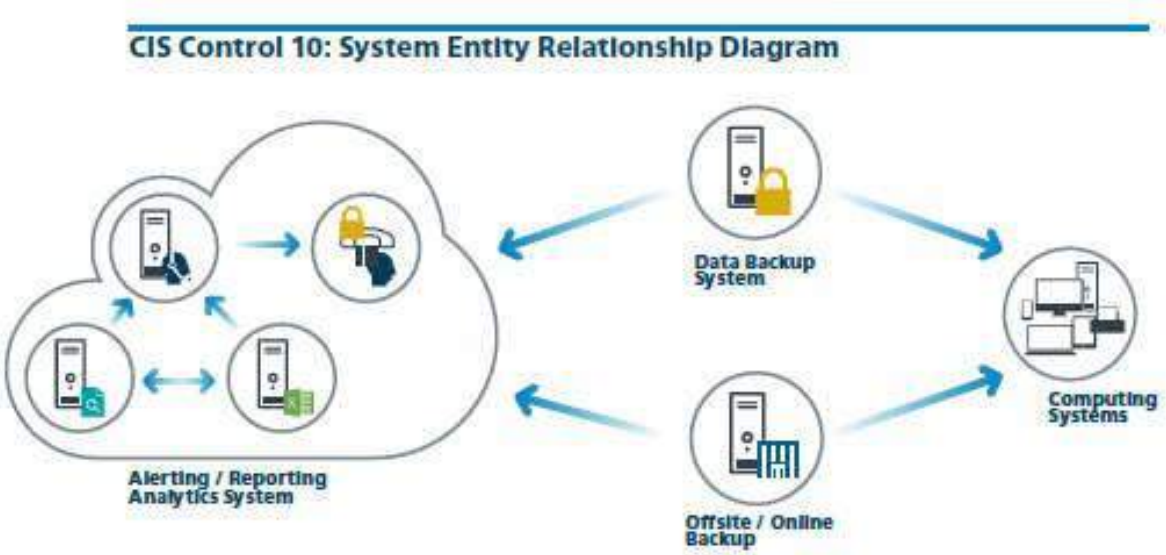
- Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

PROCEDURES & TOOLS:

- Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system.
- Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

Topic No 164: CIS CONTROL 10: DATA RECOVERY CAPABILITIES

CIS 20 Critical Security Controls



: Ensure Regular Automated Back Ups

- Ensure that all system data is automatically backed up on regular basis.

: Perform Complete System Backups

- Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

: Test Data on Backup Media

- Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

: Ensure Protection of Backups

- Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

: Ensure Backups Have At least One Non-Continuously Addressable Destination

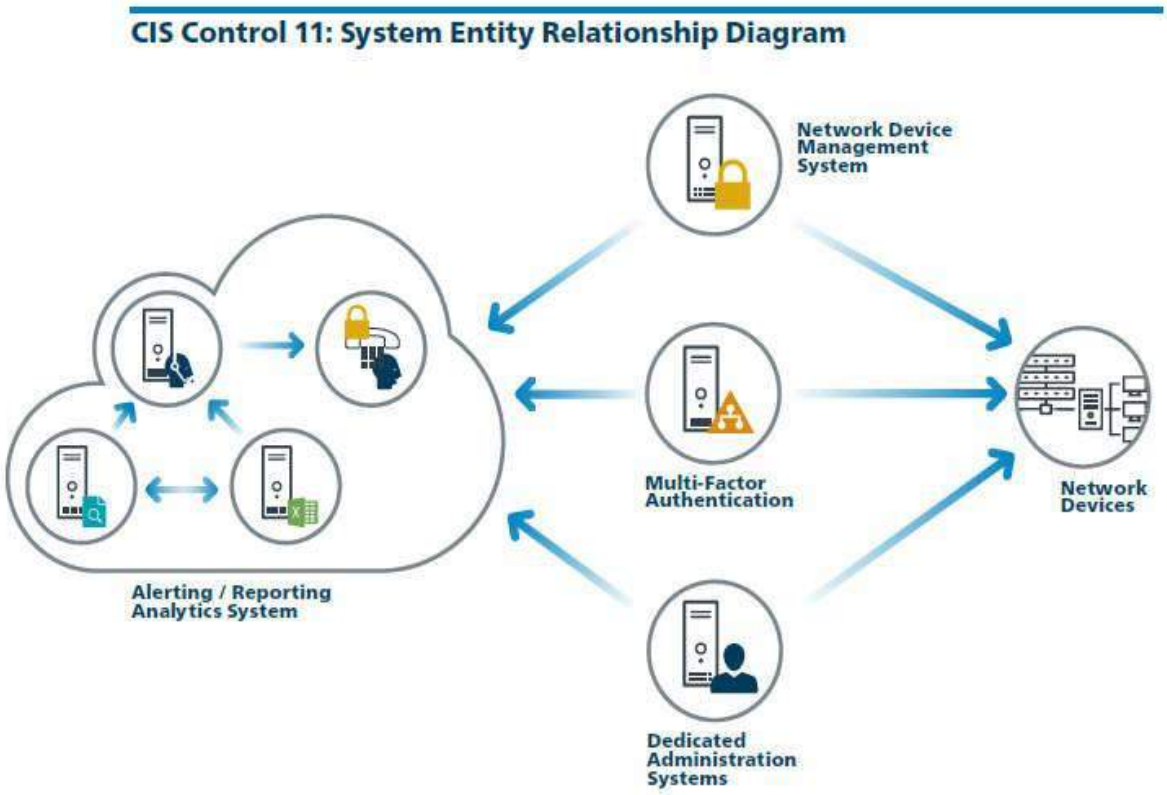
- Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

Procedures & Tools:

- Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.
- In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

Topic No165 & 166: CIS CONTROL 11: SECURE CONFIG FOR NETWORK DEVICES

- Secure Configuration For Network Devices Such As Firewalls, Routers, And Switches



: Maintain Standard Security Configurations for Network Devices

- Maintain standard, documented security configuration standards for all authorized network devices.

: Document Traffic Configuration Rules

- All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

: Use Automated Tools to Verify Standard Device Configurations and Detect Changes

- Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviation is discovered

: Install the Latest Stable Version of Any Security-related Updates on All Network Devices

- Install the latest stable version of any security-related updates on all network devices.

: Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions

- Manage all network devices using multi-factor authentication and encrypted sessions.

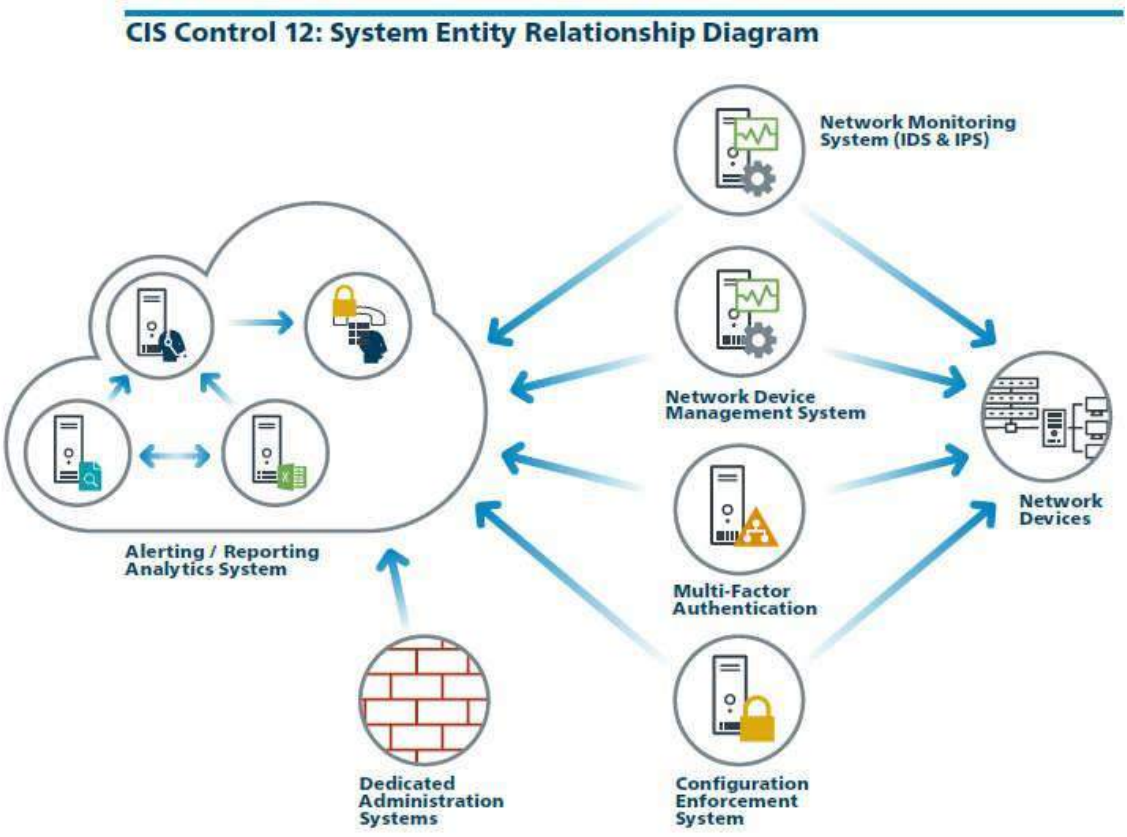
: Use Dedicated Machines For All Network Administrative Tasks

- Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

: Manage Network Infrastructure Through a Dedicated Network

- Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Topic No 167, 168 & 169: CIS CONTROL 12: BOUNDARY DEFENSE – I



BOUNDARY DEFENSE

: Maintain an Inventory of Network Boundaries

- Maintain an up-to-date inventory of all of the organization's network boundaries.

: Scan for Unauthorized Connections across Trusted Network Boundaries

- Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

: Deny Communications with Known Malicious IP Addresses

- Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.

: Deny Communication over Unauthorized Ports

- Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

: Configure Monitoring Systems to Record Network Packets

- Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

: Deploy Network-based IDS Sensor

- Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.

: Deploy Network-Based Intrusion Prevention Systems

- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.

: Deploy NetFlow Collection on Networking Boundary Devices

- Enable the collection of NetFlow and logging data on all network boundary devices.

: Deploy Application Layer Filtering Proxy Server

- Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.

: Decrypt Network Traffic at Proxy

- Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.

: Require All Remote Login to Use Multi-factor Authentication

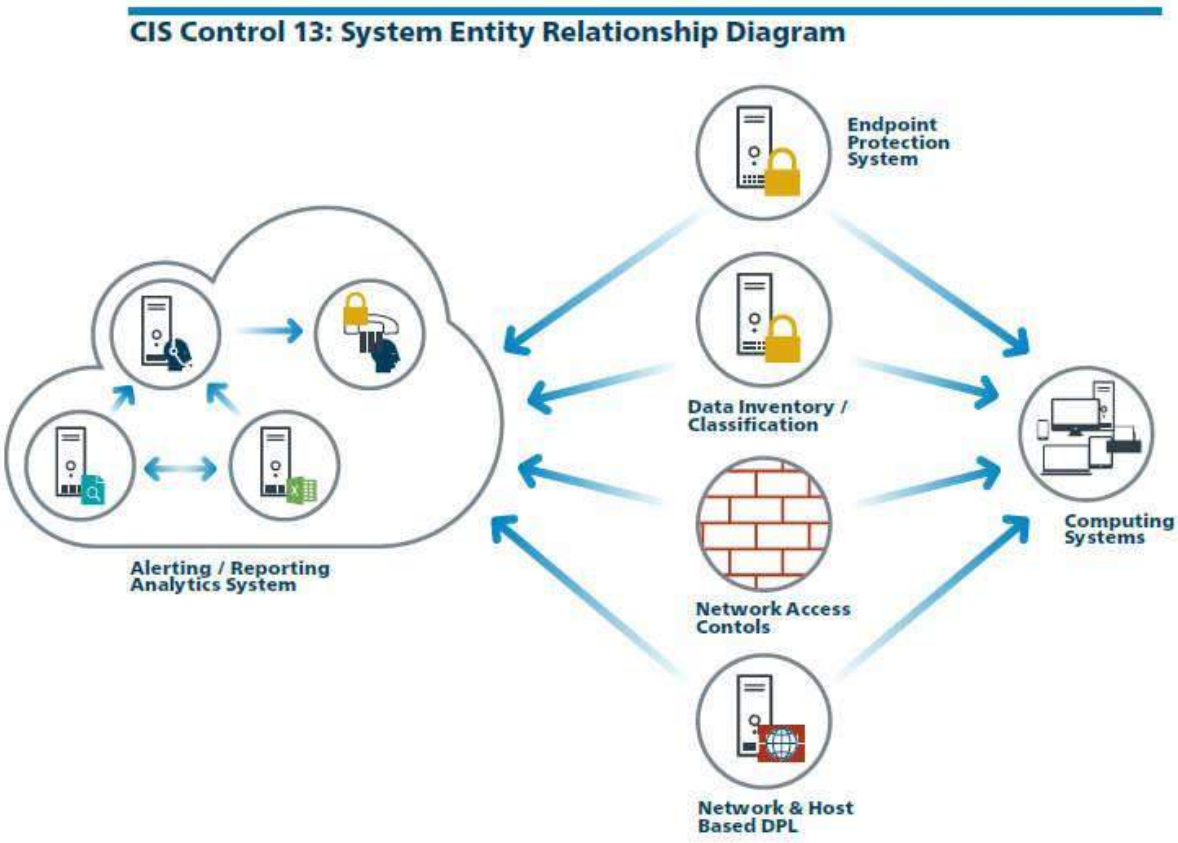
- Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication

: Manage All Devices Remotely Logging into Internal Network

- Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

Topic No 170, 171 & 172: CIS CONTROL 13: DATA PROTECTION-I

Data Protection



: Maintain an Inventory of Sensitive Information

- Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.

: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

- Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

: Monitor and Block Unauthorized Network Traffic

- Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

: Only Allow Access to Authorized Cloud Storage or Email Providers

- Only allow access to authorized cloud storage or email providers.

: Monitor and Detect Any Unauthorized Use of Encryption

- Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

: Encrypt the Hard Drive of All Mobile Devices.

- Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.

: Manage USB Devices

- If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

: Manage System's External Removable Media's Read/write Configurations

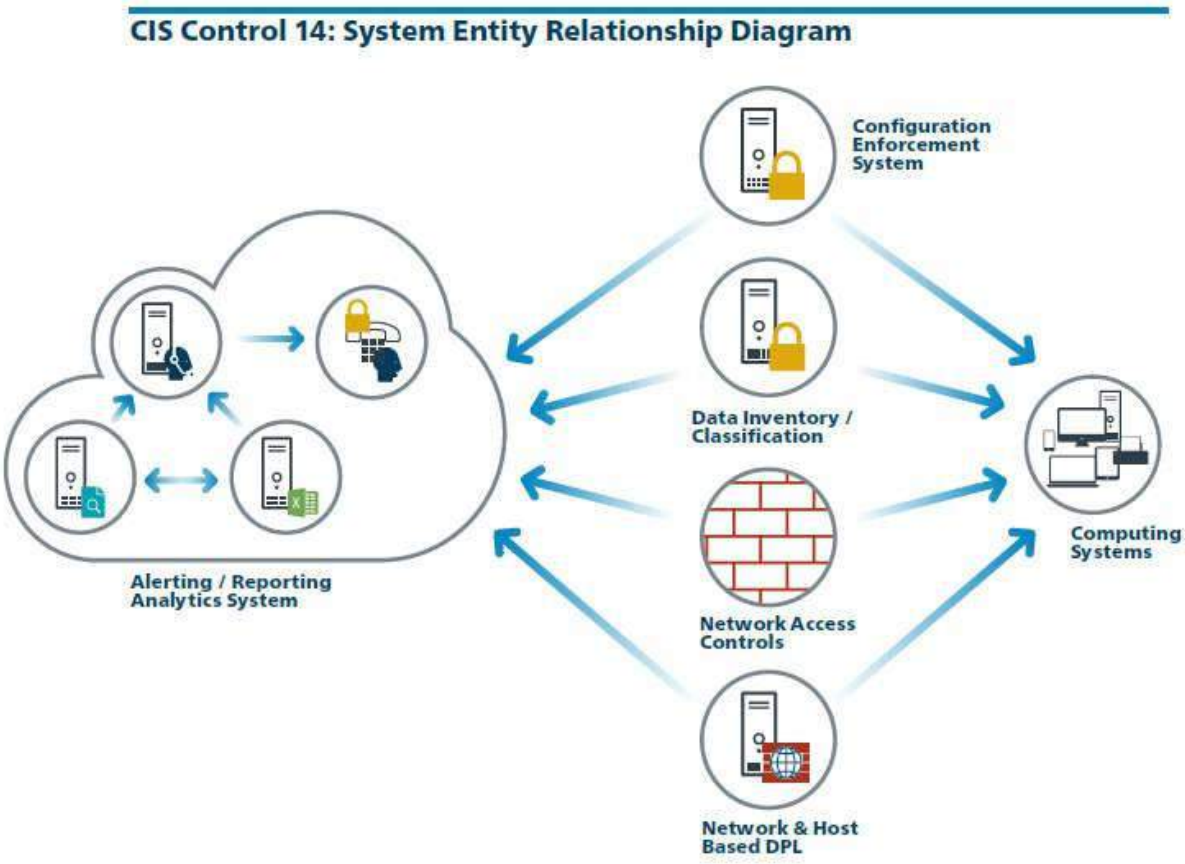
- Configure systems not to write data to external removable media, if there is no business need for supporting such devices.

: Encrypt Data on USB Storage Devices

- If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

Topic No 173 & 174: CIS CONTROL 14: CONTROLLED ACCESS-NEED TO KNOW-I

Controlled Access Based On The Need To Know



: Segment the Network Based on Sensitivity

- Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

: Enable Firewall Filtering Between VLANs

- Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

: Disable Workstation to Workstation Communication

- Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.

: Encrypt All Sensitive Information in Transit

- Encrypt all sensitive information in transit.

: Utilize an Active Discovery Tool to Identify Sensitive Data

- Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.

: Protect Information through Access Control Lists

- Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

: Enforce Access Control to Data through Automated Tools

- Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.

: Encrypt Sensitive Information at Rest

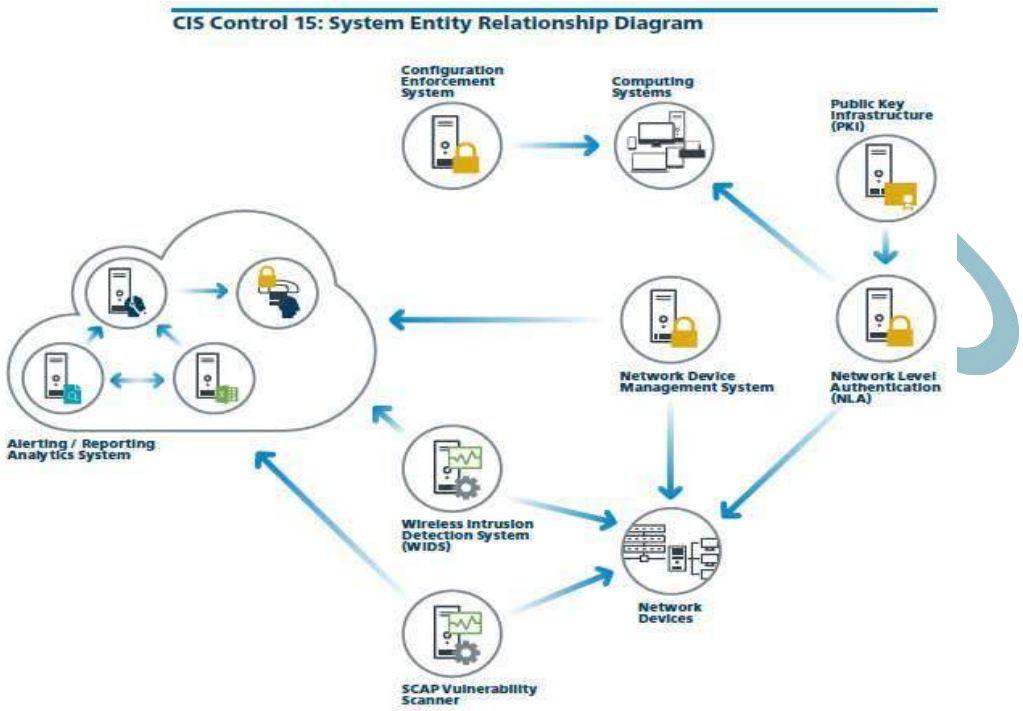
- Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

: Enforce Detail Logging for Access or Changes to Sensitive Data

- Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

Topic No 175,176 & 177: CIS CONTROL 15: WIRELESS ACCESS CONTROL-I

Wireless Access Control



: Maintain an Inventory of Authorized Wireless Access Points

- Maintain an inventory of authorized wireless access points connected to the wired network.

: Detect Wireless Access Points Connected to the Wired Network

- Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.

: Use a Wireless Intrusion Detection System

- Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.

: Disable Wireless Access on Devices if Not Required

- Disable wireless access on devices that do not have a business purpose for wireless access.

: Limit Wireless Access on Client Devices

- Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

: Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients

- Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.

: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

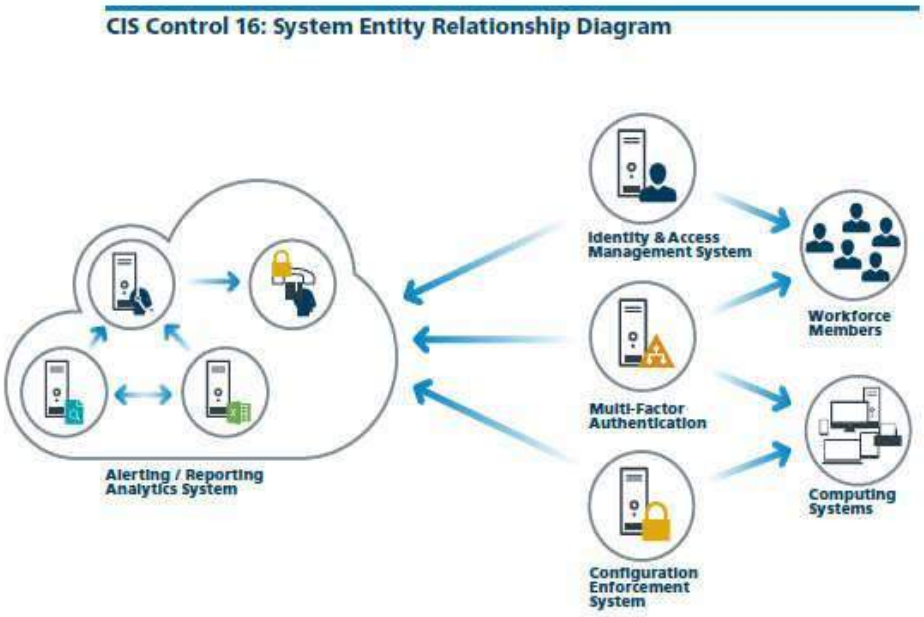
- Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

: Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication

- Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.

Topic No 178, 179 & 180: CIS CONTROL 16: ACCOUNT MONITORING & CONTROL-I

Account Monitoring & Control



: Maintain an Inventory of Authentication Systems

- Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.

: Configure Centralized Point of Authentication

- Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

: Require Multi-factor Authentication

- Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

: Encrypt or Hash all Authentication Credentials

- Encrypt or hash with a salt all authentication credentials when stored.

: Encrypt Transmittal of Username and Authentication Credentials

- Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

: Maintain an Inventory of Accounts

- Maintain an inventory of all accounts organized by authentication system.

: Establish Process for Revoking Access

- Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

: Disable Any Unassociated Accounts

- Disable any account that cannot be associated with a business process or business owner.

: Disable Dormant Accounts

- Automatically disable dormant accounts after a set period of inactivity.

: Ensure All Accounts Have An Expiration Date

- Ensure that all accounts have an expiration date that is monitored and enforced.

: Lock Workstation Sessions After Inactivity

- Automatically lock workstation sessions after a standard period of inactivity.

: Monitor Attempts to Access Deactivated Accounts

- Monitor attempts to access deactivated accounts through audit logging.

: Alert on Account Login Behavior Deviation

- Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

: Encrypt Transmittal of Username and Authentication Credentials

- Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

: Maintain an Inventory of Accounts

- Maintain an inventory of all accounts organized by authentication system**.**

16.7: Establish Process for Revoking Access

- Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

: Disable Any Unassociated Accounts

- Disable any account that cannot be associated with a business process or business owner.

: Disable Dormant Accounts

- Automatically disable dormant accounts after a set period of inactivity.

: Ensure All Accounts Have An Expiration Date

- Ensure that all accounts have an expiration date that is monitored and enforced.

: Lock Workstation Sessions After Inactivity

- Automatically lock workstation sessions after a standard period of inactivity.

: Monitor Attempts to Access Deactivated Accounts

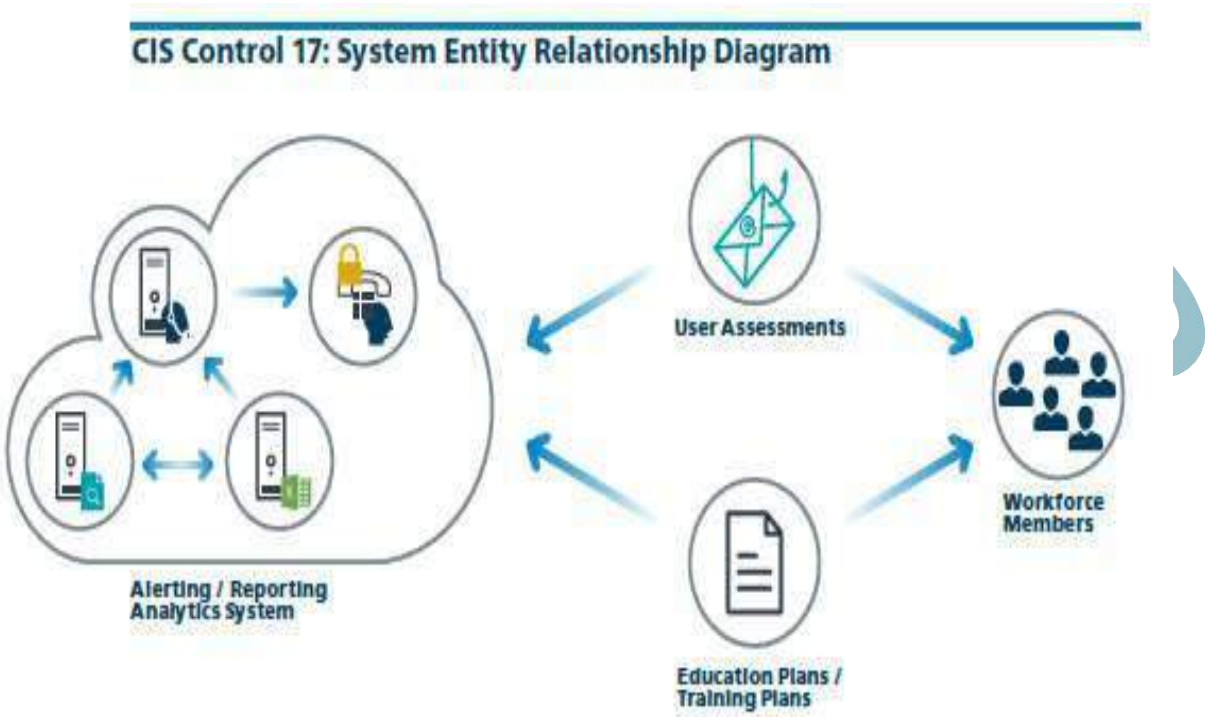
- Monitor attempts to access deactivated accounts through audit logging.

: Alert on Account Login Behavior Deviation

- Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

Topic No 181, 182: CIS CONTROL 17: SECURITY AWARENESS & TRAINING-I

- IMPLEMENT A SECURITY AWARENESS & TRAINING PROGRAM



: Perform a Skills Gap Analysis

- Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.

: Deliver Training to Fill the Skills Gap

- Deliver training to address the skills gap identified to positively impact workforce members' security behavior.

: Implement a Security Awareness Program

- Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner

: Update Awareness Content Frequently

- Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.

: Train Workforce on Secure Authentication

- Train workforce members on the importance of enabling and utilizing secure authentication.

: Train Workforce on Identifying Social Engineering Attacks

- Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.

: Train Workforce on Sensitive Data Handling

- Train workforce on how to identify and properly store, transfer, archive and destroy .

: Train Workforce on Causes of Unintentional Data Exposure

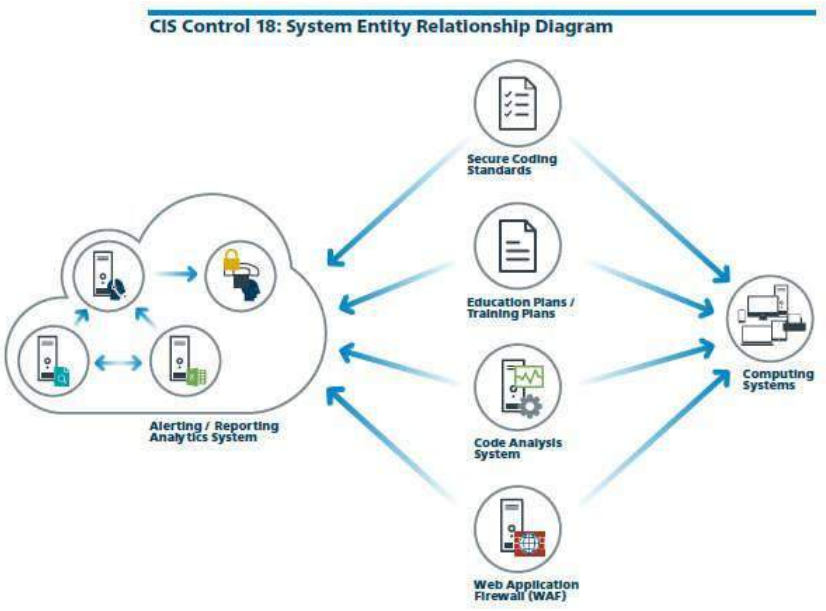
- Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

: Train Workforce Members on Identifying and Reporting Incidents

- Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

Topic No 183,184,185: CIS CONTROL 18: APPLICATION SOFTWARE SECURITY-I

Application Software Security



: Establish Secure Coding Practices

- Establish secure coding practices appropriate to the programming language and development environment being used.

: Ensure Explicit Error Checking is Performed for All In-house Developed Software

- For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, & acceptable ranges or formats.

: Verify That Acquired Software is Still Supported

- Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security [illegible].

: Only Use Up-to-date And Trusted Third-Party Components

- Only use up-to-date and trusted third-party components for the software developed by the organization.

: Use Only Standardized and Extensively Reviewed Encryption Algorithms

- Use only standardized and extensively reviewed encryption algorithms.

: Ensure Software Development Personnel are Trained in Secure Coding

- Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

: Apply Static and Dynamic Code Analysis Tools

- Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.

: Establish a Process to Accept and Address Reports of Software Vulnerabilities

- Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.

: Separate Production and Non-Production Systems

- Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.

: Deploy Web Application Firewalls (WAFs)

- Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks.

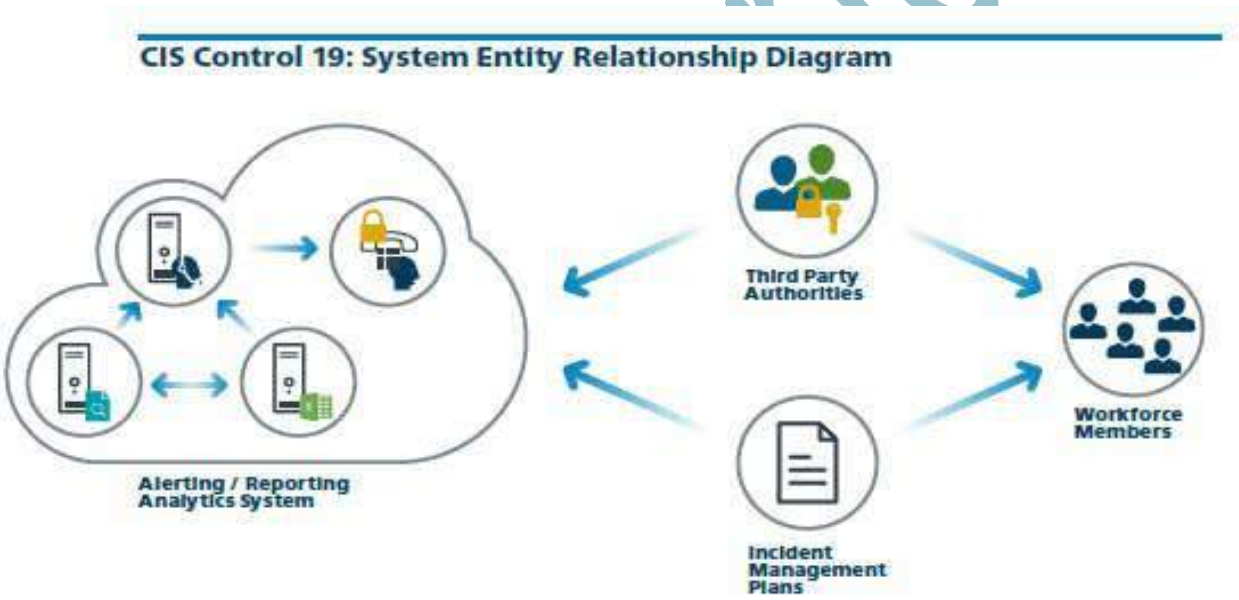
- For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

: Use Standard Hardening Configuration Templates for Databases

- For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Topic No 186, 187: CIS CONTROL 19: INCIDENT RESPONSE & MANAGEMENT-I

- Incident Response & Management



: Document Incident Response Procedures

- Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.

: Assign Job Titles and Duties for Incident Response

- Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.

: Designate Management Personnel to Support Incident Handling

- Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

: Devise Organization-wide Standards for Reporting Incidents

- Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the .

: Maintain Contact Information For Reporting Security Incidents

- Assemble & maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant govt departments, vendors, etc

: Publish Information Regarding Reporting Computer Anomalies and Incidents

- Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.

: Conduct Periodic Incident Scenario Sessions for Personnel

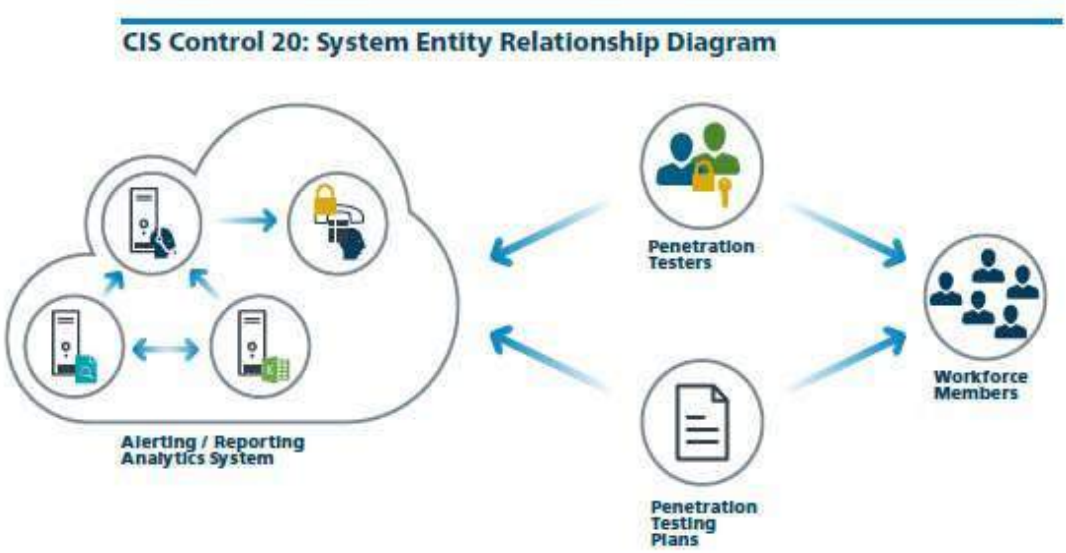
- Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats.
- Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.

: Create Incident Scoring and Prioritization Schema

- Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.

Topic No 188, 189: CIS CONTROL 20: PEN TESTS & RED TEAM EXERCISES-I

Penetration Tests & Red Team Exercises



: Establish a Penetration Testing Program

- Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.

: Conduct Regular External and Internal Penetration Tests

- Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

: Perform Periodic Red Team Exercises

- Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

: Include Tests for Presence of Unprotected System Information and Artifacts

- Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.

: Create Test Bed for Elements Not Typically Tested in Production

- Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

: Use Vulnerability Scanning and Penetration Testing Tools in Concert

- Use vulnerability scanning & penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide & focus pen testing efforts.

: Ensure Results from Penetration Test are Documented Using Open, Machine- readable Standards

- Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.

: Control and Monitor Accounts Associated with Penetration Testing

- Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for and are removed or restored to normal function after testing is over.

Topic No 190: What Is IT Governance?

- **What is IT Governance?**
  - The primary goals of IT Governance are to assure that the investments in IT generate business value, and to mitigate the risks that are associated with IT
  - Simply put, it's putting structure around how organizations align IT strategy with business strategy, ensuring that companies stay on track to achieve their strategies and goals, and implementing good ways to measure IT's performance.
  - It makes sure that all stakeholders' interests are taken into account and that processes provide measurable results.
  - An IT governance framework should answer key questions such as how the IT dept is functioning overall, what key metrics management needs and what return IT is giving back to the business from investments
- Frameworks which cover IT Governance:
  - ISO27001: 2013 (Information Security Management System - ISMS)
  - ITIL (IT Infrastructure Library)

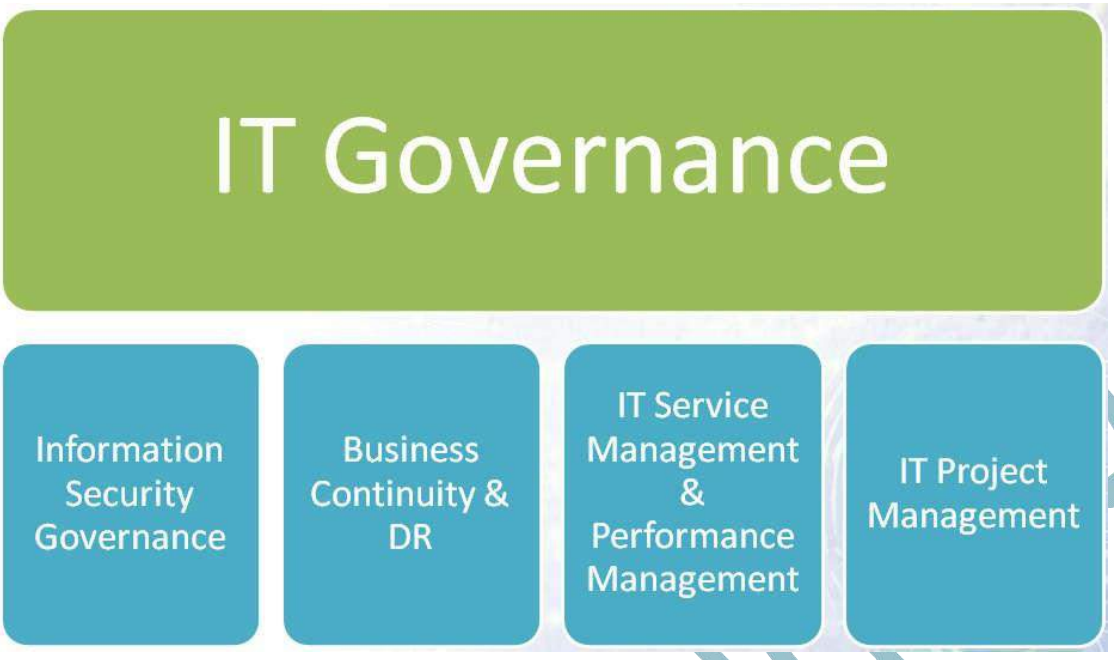
- COBIT (Control Objectives for Information & Related Technology)

- **What is COBIT?**
  - Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and .

ISACA®
Trust in, and value from, information systems

Topic No 191: What Is Information Security Governance?

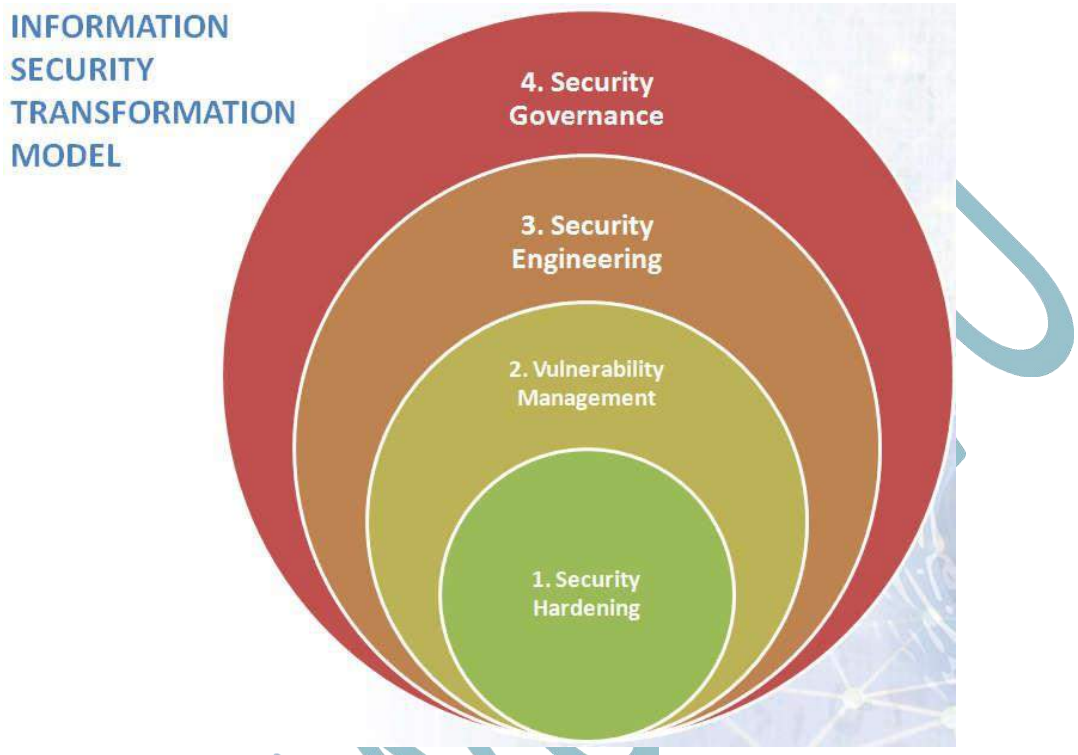
- **What is Information Security governance ?**
  - *"Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."*
- Information Security governance is the mechanism how the information security function is managed by the organization



- The leading framework for Information Security governance is ISO27001:2013 (ISMS)
  - Considered gold standard
  - Most widely deployed Information Security governance framework
- "Provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."
- Clauses 4 to 10 of ISO27001:2013
  - 4: Organization & context, scope
  - 5: Leadership & commitment, policy, organizational roles & responsibilities
  - 6: Planning; Infosec objectives and planning to achieve them
  - 7: Support; resources, competence, awareness
  - 8: Operations; risk assessment and risk management
  - 9: Performance evaluation; monitoring, measurement & analysis; internal audit
  - 10: Non-conformities & corrective actions, continual improvement

Topic No 192: Why Is InfoSec Governance At Stage 4?

- Lets have a look at the Security Transformation Model



- **Why is security governance at stage 4?**
  - First build a building and then manage it
  - First 2 stages build up the essential foundation
  - 3rd stage implements advanced security measures
  - Then (4th stage) it is time to manage
- **Limited organizational bandwidth?**
  -
  - May get lost in governance if implement at the wrong time
  - Spend limited resources where they count most (in security hardening)
- **Pakistan's InfoSec paradigm**
  - Governance overkill
  - Reactive
  - Superficial
  - Complete absence of underlying security controls

  - that is why security transformation is required
- Once the basic foundations of security hardening, vulnerability management, and security engineering are in place it is time to manage the "system"
- If we try to establish governance first, our entire energies will be consumed in managing a system that has not yet been built.
- Organizational security maturity…when does governance make sense?
- Governance is important but only after security hardening & controls (stage 1, 2, and 3) are in place

Topic No 193: Can InfoSec Governance Be Before Stage 4?

- Lets have a look at the Security Transformation Model
- Implications of implementing Stage 4 before first 3 stages:
  - Expending project energy, resources, and time in governance whereas they should have been spent on building fundamental security foundation (which later requires management)
  - Getting caught up in intangible "governance" activity
  - Getting caught up in policy & management without essential and fundamental underlying security controls
  - Setting unrealistic expectations
  - Note that governance consists of documentation and process which tends to bog

Security controls (Stage 1-3) once they are implemented by following security hardening & vulnerability management international best-practices can be better documented and regulated through governance (policy, SOP)

- **Why?**
  - We know what works and is implementable in terms of security controls
  - Controls are implemented incrementally (practical)
  - Minimal policy in place at initial stages as a starting point

- However:
  - Certain projects may have governance stipulations by the regulator/customers
  - Deadline to achieve certain governance or security milestones
  - In such cases tailor security transformation project
- The sequence of the security transformation model (stages 1 through 4) should be followed wherever possible as it is a tried and tested model
- The security transformation model may be tailored as per your unique requirements

Topic No 194: Pakistan's InfoSecurity Posture & Challenges

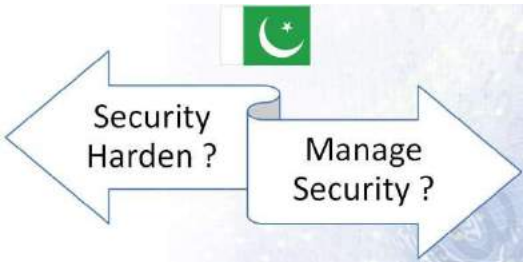
- Lets have a look at the typical IT & Information Security challenges

IT CHALLENGES SUMMARY

INFORMATION SECURITY CHALLENGES

PAKISTAN INDUSTRY CHARACTERISTICS

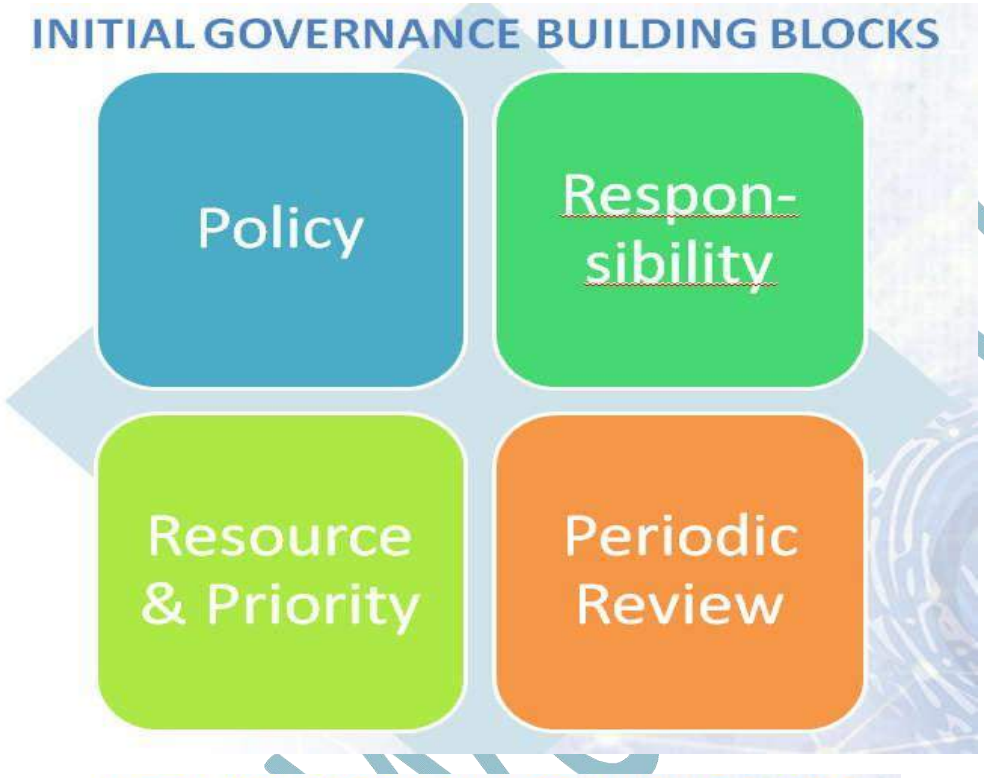
PAKISTAN INDUSTRY CHARACTERISTICS

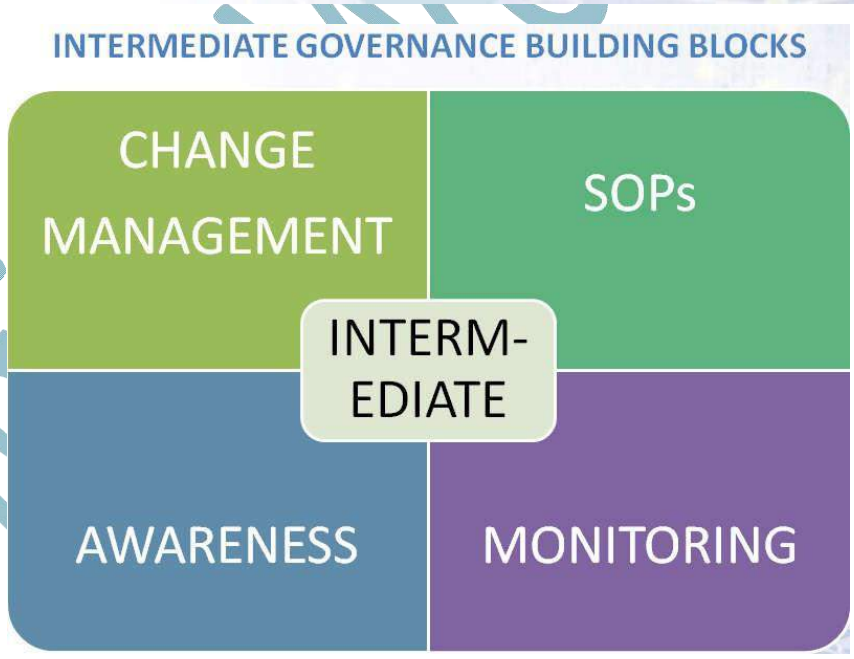


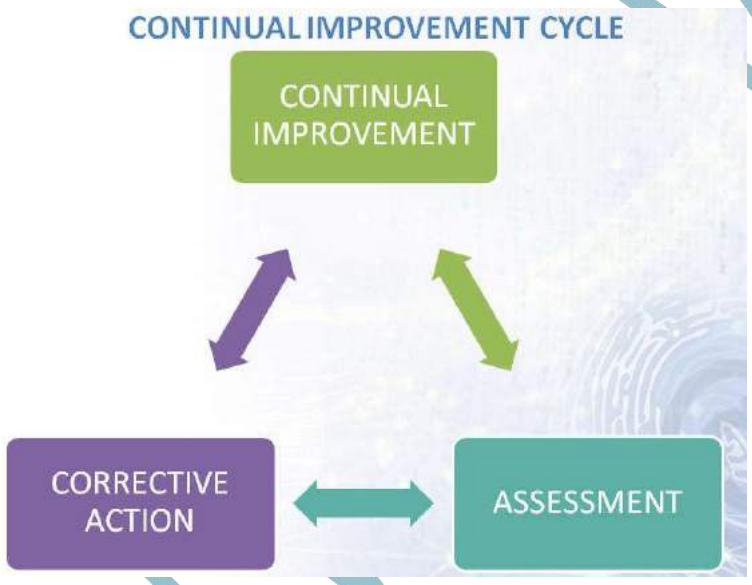
- Pakistan is now almost one entire technology generation behind in Information Security
- IT progressed during the last 10-12 years but InfoSec was ignored
- Information Security Transformation Model is the only way to catch up

Topic No 195: InfoSec Governance Building Blocks

- Lets have a look at the Information Security governance building blocks







- **Governance implementation should be broken up into phases**
  - Essential (initial) activities first
  - Gradually progress with activities that match organizational readiness & maturity

Topic No 196: Whose Responsibility Is InfoSec Governance?

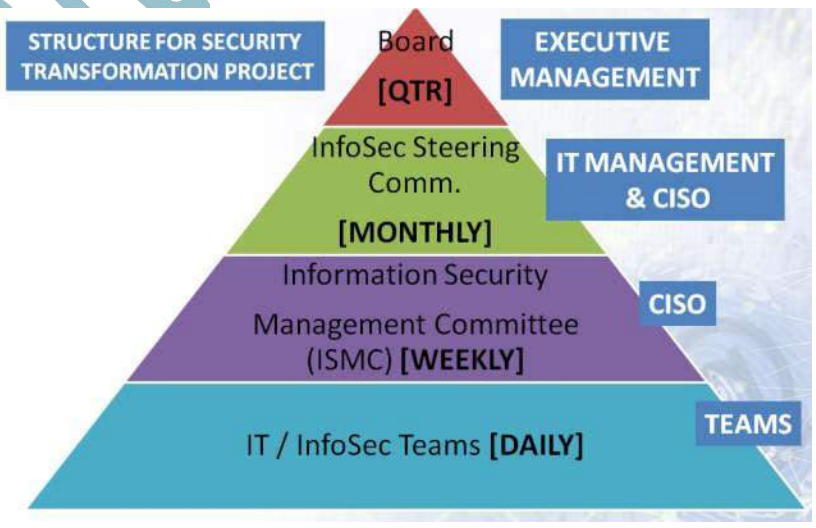
- Information security governance has responsibilities at different layers of the organization
- In Pakistan, the governance functions are slightly different than practice in more mature markets

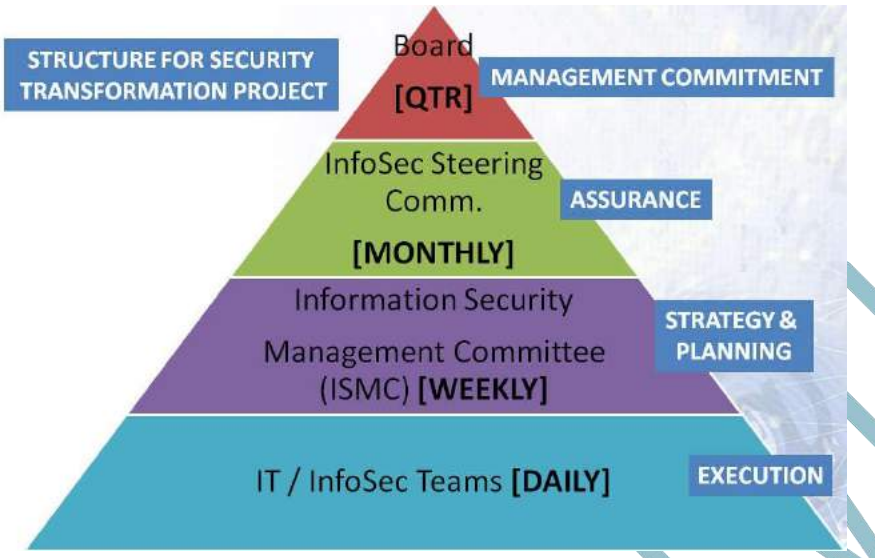
TYPICAL ORGANIZATIONAL TIERS AND MEMBERS

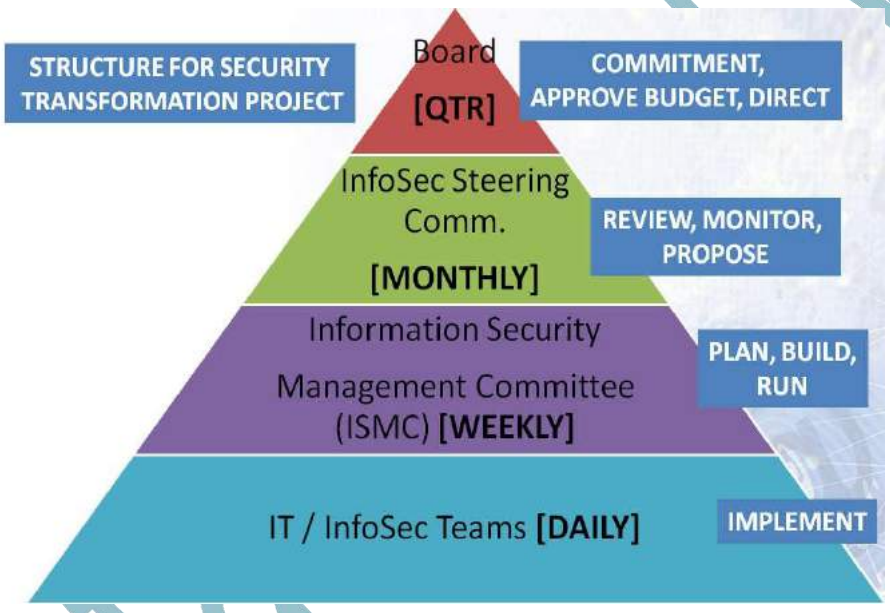
TIER	MEMBERS
BOARD (STEERING COMMITTEE)	BOARD MEMBER, CIO, CISO, IT MANAGEMENT, (SOME KEY BUSINESS MEMBERS)
IT MANAGEMENT (CIO)	GMs BELONGING TO IT MANAGEMENT, CISO
CISO/SECURITY HEAD	CISO AND ISMC
IT & SECURITY TEAMS	IT TEAMS AND PROJECT TEAMS

BOARD (STEERING COMMITTEE)	ORGANIZATIONAL COMMITMENT, APPROVE BUDGET, DIRECT
IT MANAGEMENT (CIO)	REVIEW, MONITOR, PROPOSE
CISO/SECURITY HEAD	PLAN, BUILD, RUN
IT & SECURITY TEAMS	IMPLEMENT/EXECUTE

- Based on experience with real Information Security Transformation projects in the Pakistan industry, we have set a more practical structure as shown in the following slides
- Well-suited to drive the Security Transformation project successfully





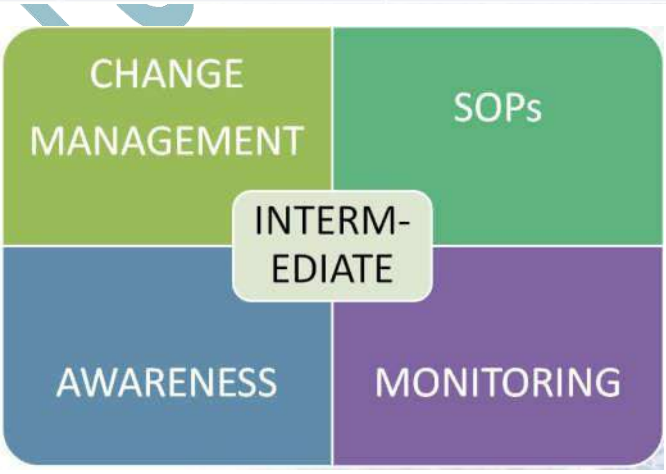


- When working in the practical industry in a market where the security posture is sub-par, we should be open to adopt structures and strategies relevant for such a level of market
- ISACA and other frameworks propose mechanisms that do not always make sense in an unprepared market

Topic No 197: How Is InfoSec Governance Implemented?

- Lets have a look at the Information Security governance building blocks

ACTIVITY	RESPONSIBLE	DETAIL
POLICY	DEVELOPED BY CISO SIGNED OFF BY BOARD/EXECUTIVE	SETS THE SCOPE, OBJECTIVES, FRAMEWORK, REQUIREMENTS
RESPONSIBILITY & AUTHORITY	BOARD/EXECUTIVE	ASSIGNS ROLES, RESPONSIBILITIES, AND AUTHORITY FOR INFOSEC PROGRAM
RESOURCE ASSIGNMENT & PRIORITY SETTING	BOARD/EXECUTIVE	ALLOCATION OF RESOURCES AND BUDGET FOR THE INFOSEC FUNCTIONS
PERIODIC REVIEW	BOARD/EXECUTIVE	MONITOR AND REVIEW THAT THE GOALS OF THE INFOSEC PROGRAM ARE BEING MET

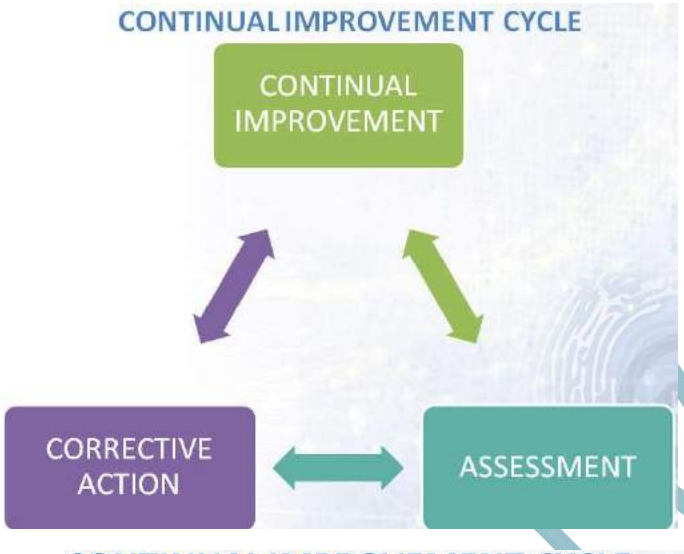


INTERMEDIATE GOVERNANCE BUILDING BLOCKS

ACTIVITY	RESPONSIBLE	DETAIL
CHANGE MANAGEMENT	IT MANAGEMENT	ESTABLISHING AND ENFORCING A CHANGE MANAGEMENT PROCESS
SOPs	IT MANAGEMENT	DEVELOPING STANDARD OPERATING PROCEDURES BASED ON ACTUAL PRACTICE
AWARENESS	CISO/ SECURITY TEAMS	CONDUCTING SECURITY AWARENESS TRAINING
MONITORING/ REVIEW	IT MANAGEMENT	GAUGING THE PERFORMANCE AND PROGRESS OF THE INFOSEC PROGRAM AGAINST AGREED PROJECT PLAN/MILESTONES

MATURE GOVERNANCE BUILDING BLOCKS

ACTIVITY	RESPONSIBLE	DETAIL
RISK MANAGEMENT	DRIVEN BY INFOSEC SUPPORTED BY IT MANAGEMENT	RISK ASSESSMENT, RISK TREATMENT & RISK MANAGEMENT LIFECYCLE
INTERNAL AUDIT	INTERNAL AUDIT DEPT, OR INFOSEC	IMPLEMENT PERIODIC AUDIT PROGRAM
INCIDENT MANAGEMENT	IT MANAGEMENT & INFOSEC	INCIDENT MANAGEMENT LIFECYCLE



CONTINUAL IMPROVEMENT CYCLE

ACTIVITY	RESPONSIBLE	DETAIL
CONTINUAL IMPROVEMENT	BOARD/ EXECUTIVE	CONTINUAL STEPS FOR THE EFFECTIVENESS OF INFOSEC PROGRAM
CORRECTIVE ACTIONS	IT MANAGEMENT / INFOSEC	CORRECTIVE ACTIONS FOR NON-CONFORMITIES AND GAPS
THIRD-PARTY ASSESSMENTS	BOARD/INFOSEC	CONDUCT THIRD-PARTY ASSESSMENTS SUCH AS VA/PT, GAP ANALYSIS

- Information Security governance can quickly become a challenge as governance is considered an intangible
  - How do you achieve governance ?
  - When do you know you have achieved it ?
  - How you drive process and documentation in IT ?
- The key is to align Information Security governance as closely as possible with ISO27001:2013 (ISMS), and to go for crisp clear actions which are always measurable
- Certify against ISO27001:2013 (ISMS) for best-practices implementation

Topic No 198: How To Build Effective InfoSec Governance?

- Key success factors:
  - Leadership
  - Strategy
  -
  - Reporting
  - Project management
  - Culture

- **Leadership:**
  - Executive management role
  - Tone at the top
  - Drive pressing priority
  - Approves budgets and resources
  - Periodic review of progress
- **Strategy:**
  - How the objectives will be practically achieved while achieving the technical, governance, and performance goals
  - How the organization will gear up and focus for the security transformation
- **Structure:**

  - What hierarchies, team structures, reporting lines, and resources will come together
- How will different teams work together to achieve the common goals?

- **Reporting:**
  - What will be reported?
  - What will be the frequency of reports?
  - Who will perform review and assurance?
  - Who will monitor and track progress?
- **Project Management:**
  - How will an exceptional execution discipline be built?
  - How will milestones and performance be tracked?
  - How will project management best-practices be utilized?
- **Culture:**
  - How will an open, cooperative, authentic, and committed culture be built?
  - How will [illegible]?
  - How will a performance driven culture be promoted?
- Building effective information security governance or an effective information security transformation project are based on good management, execution and project management skills

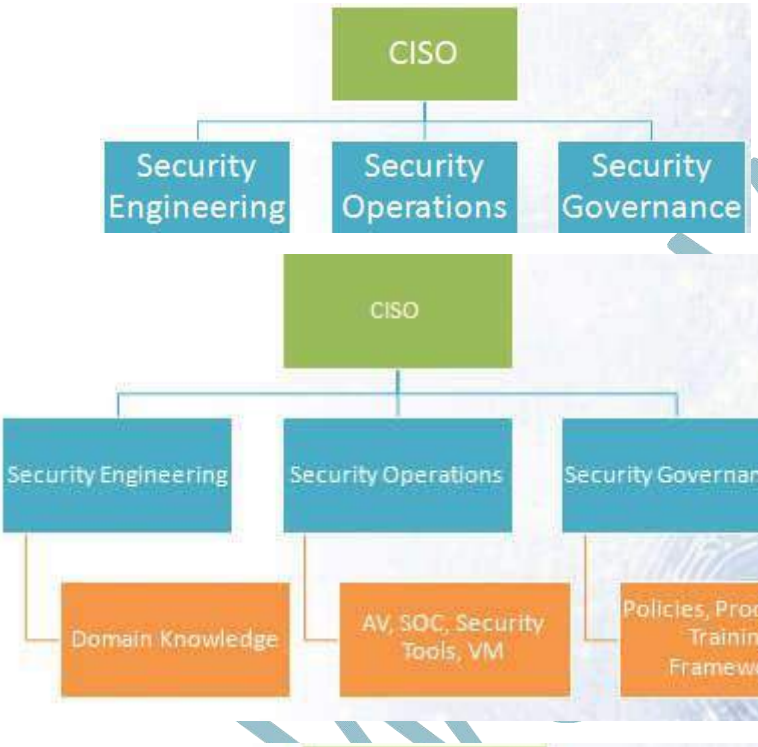
Topic No 199: InfoSec Dept Structure (Large-Sized Org)

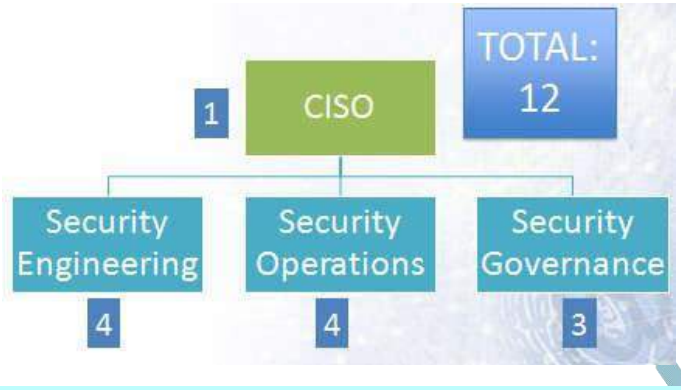
- Lets look at the recommended structure for a large organization

- A large organization can have an Infosec team ranging between 25-30 staff
- 10% of IT (250 to 300 IT staff)

Topic No 200: InfoSec Dept Structure (Mid-Sized Org)

- Lets look at the recommended structure for a mid-sized organization





- A mid-sized organization can have an Infosec team ranging between 10-15 staff
- 10% of IT (100 to 150 IT staff)

Topic No 201: InfoSec Dept Structure (Small Org)

- Lets look at the recommended structure for a small organization

- A small-sized organization can have an Infosec team ranging between 2-4 staff
- 10% of IT (15 to 50 IT staff)

Topic No 202: Role Of CISO In Driving Infosec Program

- The CISO plays a crucial role in successfully driving the Information Security program
-
  -
  - Placement in organizational hierarchy

- **Leadership & strategy:**
  - Good understanding of IT & Information security challenges
  - Experience of driving critical projects in organizations
  - Ability to build program strategy, structure, reporting mechanism , and execution discipline to achieve results
  - Ability to work with Board and senior executive management to drive program
  - Ability to motivate and communicate security vision to team
  - Ability to infuse credibility & authenticity in IT environment
  - Ability to build team work & cooperation culture
- **Technology Domain Knowledge:**
  - CISOs or security heads usually have 5-10 years experience in IT followed by 3-5 years in Information Security
  - CISOs are typically strong in 2-3 domain areas such as networking + infrastructure OR software + databases OR software QA & process engineering
  - A good CISO is able to build a good team to cover all major domain areas and all functional reqmts
  - Having a solid technical base, good CISOs are able to easily build a security competence layer on top of it
- **Governance domain knowledge:**
  - Working with regulators & compliance

- Policies & SOPs
- Frameworks & standards
- A passion for training & awareness
- A process oriented mindset to successfully build a strong InfoSec program
- Ability to balance people, process, and technology

- **Good people skills:**
  - A CISO requires good people management skills as the security transformation project is all about motivating, directing, and organizing people to achieve a focused goal
  - Personal discipline & commitment
- **Placement:**
  - Within
  - Within risk
  - Reporting to board committee

Topic No 203: Key Inhibitors For Security Program Failure

- There may be several inhibitors to achieving a successful security transformation project

- **Executive management:**
  - Allocates budget and approves resources

- Sets organizational priority & "tone at the top"
- Even if you start a program without executive management support, it may not last long
- Periodic reviews by executive management drive the execution in the IT organization
- Organizational priorities may change quickly if executive management does not sustain its commitment

- **Strategy & structure:**
  - A good or poor strategy & structure will make or break any project, in any discipline, in any organization
  - Addressing the needs and inter-linkages to make the entire machinery work in a streamlined manner

- Understanding roles of various stakeholders and taking them all along
  - Having sufficient experience to work at various levels of the organization

- **Execution:**
  - All information security projects boil down to strong execution & project management once leadership commitment and strategy/structure issues are addressed
  - Allocating tasks to run different phases in parallel & sequentially
  - Prioritizing tasks
  - Tracking progress
  - Reporting dashboards
  - Team/Steering Committee/Board presentations
- Failure of the Information Security program will be imminent if any one of these three elements (leadership, strategy/structure, execution) is not adequately addressed

Topic No 204: InfoSec Strategy For Smaller Organizations

- Smaller & newer organizations face unique challenges which may require a creative approach to implement a successful security transformation program

- **Limited budget:**
  - Limited priority with limited resources
  - Break up project into phases matching resource allocation & organizational bandwidth available
  - Limit scope to 1 location, department, team, or even to 1 application
  - Consider hiring one competent security or IT member in the team
  - Provide management support and periodic review
  - 12 to 15 months for security transformation

- **Untrained staff:**
  - Consider hiring a consultant
  - Train, incentivize, and motivate team
  - Give time to the team to adopt the security culture & processes
  - Periodic management reviews & corrective actions
- **Adhoc culture:**
  - Smaller & newer organizations may have a chaotic and adhoc culture
  - Lack of process approach

- Resources not disciplined for consistent delivery
- Rapidly changing focus and attention span
- May be resolved with a good project leader or competent consultant
- Training & setting organizational vision

- The leaders of small organizations are usually aware of their organizational capacity and limitations with experience
- Work with the organziational leadership to deploy competent project lead and team members

Topic No 205: Common Challenges: Security Documentation

- Common challenges with security governance documentation
- As we have seen in the previous modules, **policies, SOPs, checklists, guidelines, and records** are all important parts of the Information Security Management System (ISMS) and are based on documentation usually with an associated process

- **Process culture absent:**
  - Adhoc culture a corporate culture based on the ability to adapt quickly to changing conditions.
  - Rapidly changing priorities
  - Inhibits time & concentration required for documentation
  - Requires executive support to build process oriented culture
  - Requires business transformation as well as security transformation as the style in which the organization works needs to be addressed
  - New focus on quality, process, and assurance for results

long and detailed

- **Defective & voluminous documentation:**
  - Effective writing & documentation is a rare skill
  - No one likes to read long, winding, poorly structured documentation
  - No one likes to read
  -
  - Gradually build organizational appetite for documentation with extremely concise documents
  - Documentation has a close relationship with process culture and quality – is your organizational going after the right goals with balance?
- **Training & awareness:**
  - There may be a fear for documentation, and staff may be unaware or not possessing the skills or experience of documentation
  - Train and raise awareness in a friendly environment
  - Incentivize
  - Create working templates which are easily accessible on organizational portal
  - Create how-to videos & FAQs, etc
  - Invest in raising competence & skills of staff
- **Roles & responsibilities:**
  - Is right person working at the right place?
  - Do key people tasked with security governance & documentation has the right skills and experience to build documentation?
  - Are staffs aware of their responsibilities related to security governance documentation …policies, SOPs, checklists, etc?
  - Is documentation and process approach part of staff JDs & appraisal?

Topic No 206: Security Documentation: Policies

- **Policies**
- Standards
- Procedures

- Guidelines

Policies:

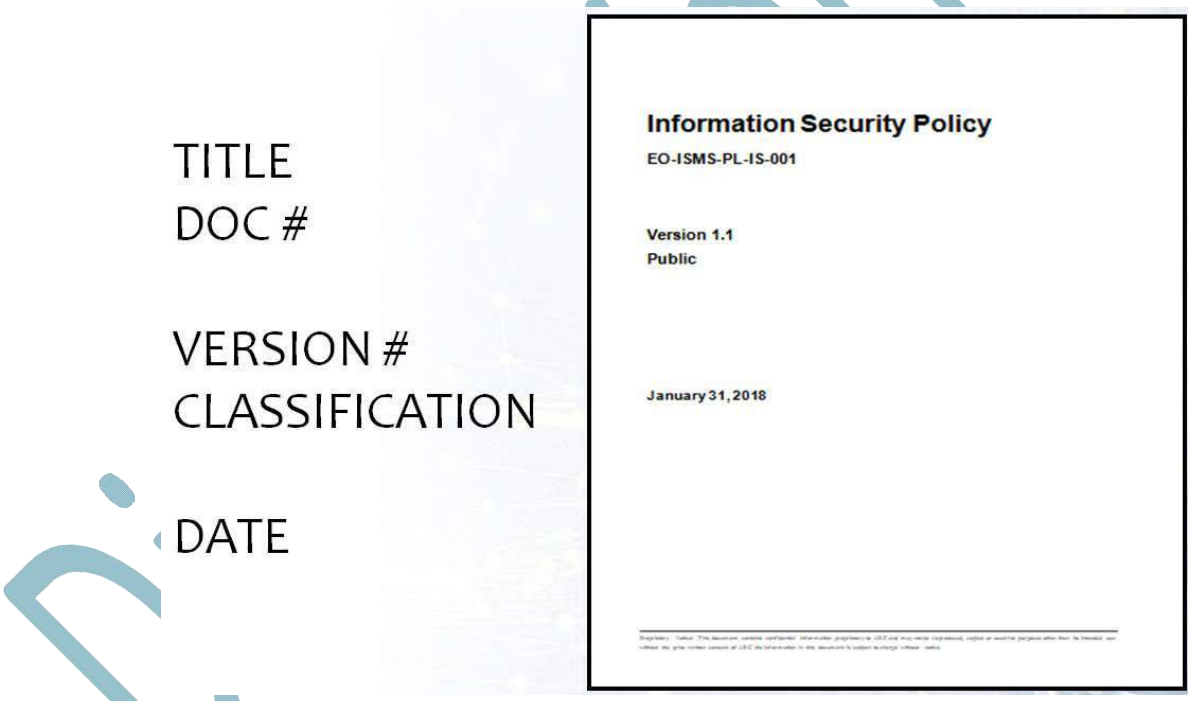
Policies are **formal statements produced and supported by senior management**. They can be organization-wide, issue-specific or system specific. Your organization's policies should reflect your objectives for your information security program.

Your policies should be like a building foundation; **built to last and resistant to change or .**

1. **Driven by business objectives** and convey the amount of risk senior management is willing

2. Easily accessible and understood by the intended reader

3. Created with the intent to be **in place for several years and regularly reviewed with approved changes** made as needed.



HEADER

	Information Security Policy	I S M S	
		Classification: Public	Doc. Version: 1.1
		Doc. No: EO-ISMS-PL-IS-001	Dated: January 31, 2018

REVISION HISTORY

Revision History

Ver #	Rev Date	Author	Distr Date	Brief Description
1.0	August 18, 2017	Nahil Mahmood	November 10th, 2017	Initial Version
1.1	December 30, 2017		January 31, 2018	Section 1.3, clause number 4 has been completed. Clause xxvii has been added for secure software development principles adoption.

REVIEW HISTORY

Review History

Ver #	Review Date	Reviewed By	Identified Changes
1.0	November 7th, 2017	CTO	No
1.0	November 9th, 2017	CEO	No
1.1	January 5, 2018	CTO	No
1.1	January 22, 2018	CEO	No

APPROVED BY

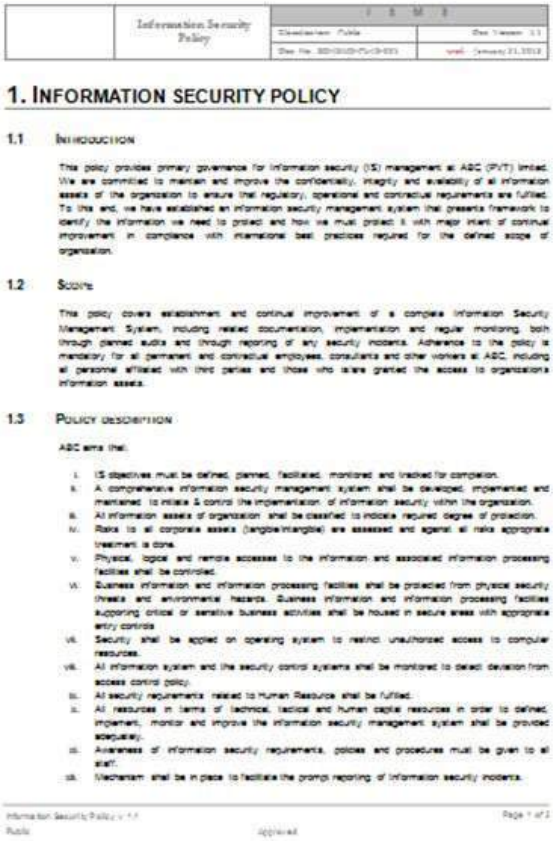
Approved By

Name	Role	Version
	CTO	1.0 (Initial base line)
	CEO	1.0 (Initial base line)
	CTO	1.1
	CEO	1.1

INTRODUCTION

SCOPE

POLICY DESCRIPTION



	Information Security Policy	I S M S	
		Classification: Public	Doc. Version: 1.1
		Doc. No: EO-ISMS-PL-IS-001	Dated: January 31, 2018

1. INFORMATION SECURITY POLICY

1.1 INTRODUCTION

This policy provides primary governance for information security (IS) management at ABC (PVT) limited. We are committed to maintain and improve the confidentiality, integrity and availability of all information assets of the organization to ensure that regulatory, operational and contractual requirements are fulfilled. To this end, we have established an information security management system that presents framework to identify the information we need to protect and how we must protect it with major intent of continual improvement in compliance with international best practices required for the defined scope of organization.

1.2 SCOPE

This policy covers establishment and continual improvement of a complete Information Security Management System, including related documentation, implementation and regular monitoring, both through planned audits and through reporting of any security incidents. Adherence to the policy is mandatory for all permanent and contractual employees, consultants and other workers at ABC, including all personnel affiliated with third parties and those who is/are granted the access to organization's information assets.

1.3 POLICY DESCRIPTION

ABC aims that:

i. IS objectives must be defined, planned, facilitated, monitored and tracked for completion.
ii. A comprehensive information security management system shall be developed, implemented and maintained to initiate & control the implementation of information security within the organization.
iii. All information assets of organization shall be classified to indicate required degree of protection.
iv. Risks to all corporate assets (tangible/intangible) are assessed and against all risks appropriate treatment is done.
v. Physical, logical and remote accesses to the information and associated information processing facilities shall be controlled.
vi. Business information and information processing facilities shall be protected from physical security threats and environmental hazards. Business information and information processing facilities supporting critical or sensitive business activities shall be housed in secure areas with appropriate entry controls
vii. Security shall be applied on operating system to restrict unauthorized access to computer resources.
viii. All information system and the security control systems shall be monitored to detect deviation from access control policy.
ix. All security requirements related to Human Resource shall be fulfilled.
x. All resources in terms of technical, tactical and human capital resources in order to defined, implement, monitor and improve the information security management system shall be provided adequately.
xi. Awareness of information security requirements, policies and procedures must be given to all staff.
xii. Mechanism shall be in place to facilitate the prompt reporting of information security incidents.

1.4 POLICY COMMUNICATION

Internal: This policy must be available to all employees through the company's intranet.
External: To all external parties, the uncontrolled copy of will be provided in hard copy format, if and when requested/required.
Vendors/ Contractors: priori to start the activity, the policy will be handed over to all those contractors/vendors who will be given physical / logical access to ABC's premises, information assets, information system and/or information processing facilities.

1.5 REVIEW

This policy has been approved by the company management and shall be reviewed annually for its continuing suitability, adequacy, and effectiveness.

1.6 ENFORCEMENT

The policy is applicable to all employees and all those people who perform work at organization's premises or who is granted the access to organization's information assets. Any employee or contractor

Topic No 207: Security Documentation: Standards

- Policies
- **Standards**
- Procedures
- Guidelines

Standards

Standards are **mandatory actions or rules** that give formal policies support and direction. One of the more difficult parts of writing standards for an information security program is getting a company-wide consensus on what standards need to be in place.

This can be a time-consuming process but is vital to the success of your information security program.

1. Used to indicate expected user behavior. For example, a consistent company email signature.
2. Might specify what hardware and software solutions are available and supported.
3. Compulsory and must be enforced to be effective. (This also applies to policies!)

Topic No 208: Security Documentation: Procedures

- Policies
- Standards
- Procedures
- Guidelines

Procedures

Procedures are detailed step by step instructions to achieve a given goal or mandate. They are typically intended for internal departments and should adhere to strict change control processes.

Procedures can be developed as you go. If this is the route your organization chooses to take it's necessary to have comprehensive and consistent documentation of the procedures that you are developing.

collection of, instructions, and information

1. Often act as the "cookbook" for staff to consult to accomplish a repeatable process.
2. Detailed enough and yet not too difficult that only a small group (or a single person) will understand.
3. Installing operating systems, performing a system backup, granting access rights to a system and setting up new user accounts are all example of procedures.

Topic No 209: Security Documentation: Guidelines

- Policies
- Standards
- Procedures
- **Guidelines**

Guidelines

Guidelines are recommendations to users when specific standards do not apply. Guidelines are designed to streamline certain processes according to what the best practices are.

Guidelines, by nature, should be open to interpretation and do not need to be followed to the letter.

1. Are more general vs. specific rules.
2. Provide flexibility for unforeseen circumstances.
3. Should NOT be confused with formal policy statements.

Topic No 210: How to Develop Effective Security Policies

6 Steps To Security Policy Excellence

Purpose Of Policies & Procedures

- Policies and procedures establish **guidelines to behavior and business processes** in accordance with an organization's strategic objectives. While typically developed in response to legal and regulatory requirements, their primary purpose should be to convey accumulated wisdom on how best to get things done in a **risk-free, efficient and compliant way.**

Policy Pitfalls an unexpected negative outcome

1. Poorly worded policies
2. Badly structured policies
3. Out-of-date policies
4. Inadequately communicated policies
5. Unenforced policies
6. Lack of management scrutiny

Six Steps:

1. **Create & Review**

Documents must be written using language that is appropriate for the target audience and should spell out the consequences of non-compliance. Smaller, more manageable documents are easier for an organization to review and update, while also being more palatable for the intended recipients.

2. Distribute

Organizations need to effectively distribute policies, both new and updated, in a timely and efficient manner. These need to be consistently enforced across an organization.

3. Achieve Consent

A process needs to be implemented that monitors users' response to policies. Policy distribution should be prioritized, ensuring that higher risk policies are signed off earlier by users than other lower risk documents.

For example, an organization may want to ensure that a user signs up to their Information Governance policy on the first day that they start employment, whilst having up to two weeks to sign up to the Travel & Expense Policy.

Systems need to in place to grant a user two weeks to process a particular document, after which the system should automatically force the user to process it.

4. Understanding

Any areas that show weaknesses can be identified and corrected accordingly. Additional training or guidance may be necessary or, if it's the policy that is causing confusion, it can be reworded or simplified.

5. Auditability

The full revision history of all documents needs to be maintained as well as who has read what, when & if possible, how long it took; who declined a policy and why. This record should be stored for future reference & may be stored in conjunction with test results.

6. Reporting

To affect change and improve compliance it helps if key performance indicators relating to policy uptake are clearly visible across all levels of an enterprise. Dashboard visibility of policy uptake compliance by geographical or functional business units helps to consolidate information and highlights exceptions.

Topic No 211: ISMS: Leading InfoSec Governance Framework

- ISO27001:2013 (ISMS)
  - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
  -
  - Long annex

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

Merits of ISO27001:2013 (ISMS):

- Exceptional framework with comprehensive coverage of mandatory requirements (clauses 4-10) and discretionary controls (annex)
- Highly beneficial as a framework for security program
-
- Provides a structure and organized sequence for security controls
- Complements security transformation model as serves as a reference and guideline for activities and controls
- Very broad
- Generic framework – leaves it to organization how to implement the measures and
- Not suited for orgs that are new to security program

How to best use advantages of ISO27001:2013 (ISMS):

- Implement security transformational model
- Cap off security transformation project with ISO27001:2013 (ISMS) certification
- ISMS as a complementary reference and checklist rather than main framework

Topic No 212: Clauses 4-6 Of ISO27001:2013 (ISMS)

- **4: Context:**
  - Understanding org and its context; internal and external issues relevant to its purpose and that affect its ability to achieve intended outcomes of ISMS
  - Needs and expectations of interested parties (e.g. legal and regulatory reqmts and contractual obligations)
  - Scope (boundaries); interfaces and dependencies
- **5: Leadership & Commitment**
  - Policy & objectives are established and are compatible with strategic direction of
  - Integrating ISMS into org processes
  - Resources for ISMS available
  - Communicating importance
  - Ensuring ISMS achieves intended outcomes
  - Directing & supporting persons
  - Promoting continual improvement
  - Assign and communicate roles, responsibilities & authorities
- **6: Planning**
  - Address org risks & opportunities & prevent or reduce undesired effects
  -
  - Identify, analyze, evaluate risks
  - Ensure
  - Ensure information security objectives are measurable, communicated
  - For objectives determine what will be done, what resources reqd, who will be responsible, when completed, how to evaluate results

Topic No 213: Clauses 7-10 Of ISO27001:2013 (ISMS)

Lets have a look at clauses 7-10

- **7: Support**
  - Org shall provide the resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS
  - Ensure competence of staff for the ISMS
  - Awareness related to the policy and ISMS will be ensured among staff
  - Communication mechanisms related to ISMS internal and external to the org
  - Documentation with appropriate identification, description, format, review & approval mechanism
  - Documentation change control, protection, distribution, retention, & disposal
- **8: Operations**
  - Plan, implement, and control processes
  - Control planned changes
  - Outsourced processes controlled
  - and
- **9: Performance Evaluation**
  - Monitoring, measurement, analysis, and evaluation
  - What needs to be monitored, methods, who will monitor, when to monitor, who shall analyze and evaluate results?
  - Internal audit implemented at planned intervals
  - Define audit criteria and scope for each audit
  - Reporting of auditing results
  - Retain auditing docs
  - Internal audit implemented at planned intervals
  - Define audit criteria and scope for each audit
  - Reporting of auditing results
  - Retain auditing docs

- Planned intervals
- Status of actions
- Changes in external and internal environment
- Review non-conformities and corrective actions, monitoring & measurement results, audit reports, other

- **10: Improvement**
  - Non-conformities and corrective actions
  - Continual improvement

Topic No 214: ISO27001:2013 Controls Appendix; Part 1

- Lets have a look at the ISO27001:2013 (ISMS) controls (appendix) in more detail

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

A.5 INFORMATION SECURITY POLICIES

A.5.1 MANAGEMENT DIRECTION FOR INFORMATION SECURITY		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	POLICIES FOR INFORMATION SECURITY	***Control:*** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	***Control:*** The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.1 **INTERNAL ORGANIZATION**		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	INFOSEC ROLES & RESPONSIBILITIES	***Control:*** All information security responsibilities shall be defined and allocated.
A.6.1.2	SEGREGATION OF DUTIES	***Control:*** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.1 **INTERNAL ORGANIZATION**	
A.6.1.1	INFOSEC ROLES & RESPONSIBILITIES
A.6.1.2	SEGREGATION OF DUTIES
A.6.1.3	CONTACT WITH AUTHORITIES
A.6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS
A.6.1.5	INFORMATION SECURITY IN PROJECT MNGMT

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.1.3	CONTACT WITH AUTHORITIES	***Control:*** Appropriate contacts with relevant authorities shall be maintained
A.6.1.4	CONTACT WITH SPECIAL INTEREST GROUPS	***Control:*** Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6 ORGANIZATION OF INFORMATION SECURITY

A.6.2 **MOBILE DEVICES & TELEWORKING**	
A.6.2.1	MOBILE DEVICE POLICY
A.6.2.2	TELEWORKING

A.6.2.2	TELEWORKING	***Control:*** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Topic No 215: ISO27001:2013 Controls Appendix; Part 2

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

A.7 HUMAN RESOURCES SECURITY

A.7.1 **PRIOR TO EMPLOYMENT**
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A.7 HUMAN RSOURCES SECURITY

A.7.1 **PRIOR TO EMPLOYMENT**	
A.7.1.1	SCREENING
A.7.1.2	TERMS & CONDITIONS OF EMPLOYMENT

A.7.2 **DURING EMPLOYMENT**	
A.7.2.1	MANAGEMENT RESPONSIBILITIES
A.7.2.2	INFOSEC AWARENESS, EDUCATION & TRAINING
A.7.2.3	DISCIPLINARY PROCESS

A.7 HUMAN RESOURCES SECURITY

A.7.1.1	**SCREENING**	***Control:*** Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations & ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.1.2	**TERMS & CONDITIONS OF EMPLOYMENT**	***Control:*** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

A.7.2 **DURING EMPLOYMENT**	
A.7.2.1	MANAGEMENT RESPONSIBILITIES
A.7.2.2	INFOSEC AWARENESS, EDUCATION & TRAINING
A.7.2.3	DISCIPLINARY PROCESS

A.7.2.1	**MANAGEMENT RESPONSIBILITIES**	**Control:** Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.1.2	**TERMS & CONDITIONS OF EMPLOYMENT**	***Control:*** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

A.7.3 **TERMINATION & CHANGE OF EMPLOYMENT**	
A.7.3.1	TERMINATION OR CHANGE OF EMPLOYMENT RESONSIBILITIES

A.7.3.1	**TERMINATION OR CHANGE OF EMPLOYMENT RESONSIBILITIES**	***Control:*** Information security responsibilities and duties that or change of employment shall be defined, communicated to the employee or contractor and enforced

Topic No 216: ISO27001:2013 Controls Appendix; Part 3

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

A.8.1 **RESPONSIBILITY FOR ASSETS**	
A.8.1.1	INVENTORY OF ASSETS
A.8.1.2	OWNERSHIP OF ASSETS
A.8.1.3	ACCEPTABLE USE OF ASSETS
A.8.1.4	RETURN OF ASSETS

A.8.1.1	**INVENTORY OF ASSETS**	***Control:*** [redacted] associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.3	**ACCEPTABLE USE OF ASSETS**	***Control:*** Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

A.8.2 **INFORMATION CLASSIFICATION**	
A.8.2.1	CLASSIFICATION OF INFORMATION
A.8.2.2	LABELLING OF INFORMATION

A.8.2.3	HANDLING OF ASSETS

A.8.2.1	**CLASSIFICATION OF INFORMATION**	***Control:*** Information shall be [redacted] legal requirements, value, criticality and sensitivity to unauthorized disclosure or [redacted]
A.8.2.3	**HANDLING OF ASSETS**	***Control:*** Procedures for handling assets shall be developed and implemented in accordance with the [redacted] classification scheme adopted by the organization.

A.8.3 **MEDIA HANDLING**	
A.8.3.1	MANAGEMENT OF REMOVABLE MEDIA
A.8.3.2	DISPOSAL OF MEDIA
A.8.3.3	PHYSICAL MEDIA TRANSFER

A.8.3.1	**MANAGEMENT OF REMOVABLE MEDIA**	***Control:*** Procedures shall be implemented for the management of removable Media in accordance with the classification scheme adopted by the Organization.
A.8.3.3	**PHYSICAL MEDIA TRANSFER**	***Control:*** Media containing information shall be protected against unauthorized access, misuse or corruption during transportation

Topic No 217: ISO27001:2013 Controls Appendix; Part 4

A.9.1 **BUSINESS REQUIREMENTS OF ACCESS CONTROL**	
A.9.1.1	ACCESS CONTROL POLICY
A.9.1.2	ACCESS TO NETWORKS AND NETWORK SERVICES

A.9.1.2	**ACCESS TO NETWORKS & NETWORK SERVICES**	***Control:*** Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

A.9.2 **USER ACCESS MANAGEMENT**	
A.9.2.1	USER REGISTRATION & DE-REGISTRATION
A.9.2.2	USER ACCESS PROVISIONING
A.9.2.3	MNGMT OF PRIVILEGED ACCESS RIGHTS
A.9.2.4	MANAGEMENT OF SECRET AUTHENTICATION INFO OF USERS
A.9.2.5	REVIEW OF USERS ACCESS RIGHTS
A.9.2.6	REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

A.9.2.3	**MANAGEMENT OF PRIVILEGED ACCESS RIGHTS**	***Control:*** The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.5	**REVIEW OF USER ACCESS RIGHTS**	***Control:*** Asset owners shall review users' access rights at regular intervals.

A.9.2.6	**REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS**	***Control:*** Access rights of all employees and external party users to info & info processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9.3 **USER RESPONSIBILITIES**	
A.9.3.1	USE OF SECRET AUTHENTICATION INFORMATION

A.9.3.1	**USE OF SECRET AUTHENTICATION INFORMATION**	***Control:*** Users shall be required to follow the organization's practices in the use of secret authentication information.

A.9.4 **SYSTEM & APPLICATION ACCESS CONTROL**	
A.9.4.1	INFORMATION ACCESS RESTRICTION
A.9.4.2	SECURE LOG-ON PROCEDURES
A.9.4.3	PASSWORD MANAGEMENT SYSTEM
A.9.4.4	USE OF PRIVILEGED UTILITY PROGRAMS
A.9.4.5	ACCESS CONTROL TO PROGRAM SOURCE CODE

A.9.4.3	**PASSWORD MANAGEMENT SYSTEM**	***Control:*** Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.5	**ACCESS CONTROL TO PROGRAM SOURCE CODE**	***Control:*** Access to program source code shall be restricted.

Topic No 218: ISO27001:2013 Controls Appendix; Part 5

In this module lets look at ISO27001:2013 (ISMS) related to cryptography, and physical & environmental security.

A.10 CRYPTOGRAPHY

A.10.1 CRYPTOGRAPHIC CONTROLS	
A.10.1.1	POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS
A.10.1.2	KEY MANAGEMENT

A.10.1.2	**KEY MANAGEMENT**	***Control:*** A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.1 SECURE AREAS	
A.11.1.1	PHYSICAL SECURITY PERIMETER
A.11.1.2	PHYSICAL ENTRY CONTROLS
A.11.1.3	SUCURING OFFICES, ROOMS, AND FACILITIES
A.11.1.4	PROTECTING AGAINST EXTERNAL & ENVIRONMENTAL THREATS
A.11.1.5	WORKING IN SECURE AREAS
A.11.1.6	DELIVERY & LOADING AREAS

A.11.1.1	**PHYSICAL SECURITY PERIMETER**	***Control:*** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical info & information processing facilities.
A.11.1.2	**PHYSICAL ENTRY CONTROLS**	***Control:*** Secure areas shall be protected by appropriate entry controls to Ensure that

		only authorized personnel are allowed access.
A.11.1.5	**WORKING IN SECURE AREAS**	***Control:*** Procedures for working in secure areas shall be designed and applied.

A.11 PHYSICAL & ENVIRONMENTAL SECURITY

A.11.2 **EQUIPMENT**	
A.11.2.1	EQUIPMENT SITING & PROTECTION
A.11.2.2	SUPPORTING UTILITIES
A.11.2.3	CABLING SECURITY
A.11.2.4	EQUIPMENT MAINTENANCE
A.11.2.5	REMOVAL OF ASSETS
A.11.2.6	SECURITY OF EQUIPMENT & ASSETS OFF-PREMISES

A.11.2.2	**SUPPORTING UTILITIES**	***Control:*** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.4	**EQUIPMENT MAINTENANCE**	***Control:*** Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.11 PHYSICAL & ENVIRONMENTAL SECURITY	
A.11.2 **EQUIPMENT…**	
A.11.2.7	SECURE DISPOSAL OR RE-USE OF EQUIPMENT
A.11.2.8	UNATTENDED USER EQUIPMENT
A.11.2.9	CLEAR DESK & CLEAR SCREEN POLICY

A.11.2.9	**CLEAR DESK & CLEAR SCREEN POLICY**	***Control:*** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Topic No 219 & 220: ISO27001:2013 Controls Appendix; Part 6 & 7

A.12 OPERATIONS SECURITY	
A.12.1 **OPERATIONAL PROCEDURES & RESPONSIBILITIES**	
A.12.1.1	DOCUMENTED OPERATING PROCEDURES
A.12.1.2	CHANGE MANAGEMENT
A.12.1.3	CAPACITY MANAGEMENT
A.12.1.4	SEPARATION OF DEVELOPMENT, TESTING, AND OPERATIONAL ENVIRONMENTS

A.12.1.1	**DOCUMENTED OPERATING PROCEDURES**	***Control:*** Operating procedures shall be documented and made available to all users who need them.
A.12.1.2	**CHANGE MANAGEMENT**	***Control:*** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

A.12.1.3	**CAPACITY MANAGEMENT**	***Control:*** The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4	**SEPARATION OF DEVELOPMENT, TESTING, AND OPERATIONAL ENVIRONMENTS**	***Control:*** Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

A.12.2 **PROTECTION FROM MALWARE**	
A.12.2.1	CONTROLS AGAINST MALWARE

A.12.2.1	**CONTROLS AGAINST MALWARE**	***Control:*** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A.12.3 **BACKUP**	
A.12.3.1	INFORMATION BACKUP

A.12.3.1	**INFORMATION BACKUP**	***Control:*** Backup copies of information, software and system images shall be taken and tested regularly in accordance with an

		agreed backup policy.

A.12.4 **LOGGING & MONITORING**	
A.12.4.1	EVENT LOGGING
A.12.4.2	PROTECTION OF LOG INFORMATION
A.12.4.3	ADMINISTRATOR & OPERATOR LOGS
A.12.4.4	CLOCK SYNCHRONISATION

A.12.4.1	EVENT LOGGING	***Control:*** Event logs recording user activities, exceptions, faults and information Security events shall be produced, kept and regularly reviewed.
A.12.4.3	ADMINISTRATOR & OPERATOR LOGS	***Control:*** System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

A.12.5 **CONTROL OF OPERATIONAL SOFTWARE**	
A.12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL

	SYSTEMS

A.12.5.1	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS	***Control:*** Procedures shall be implemented to control the installation of software on operational systems.

A.12.6 **TECHNICAL VULNERABILITY MANAGEMENT**	
A.12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES
A.12.6.2	RESTRICTIONS ON SOFTWARE INSTALLATION

A.12.6.1	MANAGEMENT OF TECHNICAL VULNERABILITIES	***Control:*** Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
A.12.6.2	RESTRICTIONS ON SOFTWARE INSTALLATION	***Control:*** Rules governing the installation of software by users shall be established and implemented.

A.12.7 **INFORMATION SYSTEMS AUDIT CONSIDERATIONS**

A.12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS

A.12.7.1	INFORMATION SYSTEMS AUDIT CONTROLS	***Control:*** Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

Topic No 221: ISO27001:2013 Controls Appendix; Part 8

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

A.13 COMMUNICATIONS SECURITY

A.13.1 COMMUNICATIONS SECURITY	
A.13.1.1	**NETWORK CONTROLS**
A.13.1.2	**SECURITY OF NETWORK SERVICES**
A.13.1.3	**SEGREGATION IN NETWORKS**

A.13.1.1	NETWORK CONTROLS	***Control:*** Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	SECURITY OF NETWORK SERVICES	***Control:*** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
A.13.1.3	SEGREGATION IN NETWORKS	***Control:*** Groups of information services, users and information systems shall be segregated on networks.

A.13.2 **INFORMATION TRANSFER**	
A.13.2.1	INFORMATION TRANSFER POLICIES & PROCEDURES
A.13.2.2	AGREEMENTS ON INFORMATION TRANSFER
A.13.2.3	ELECTRONIC MESSAGING
A.13.2.4	CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS

A.13.2.1	INFORMATION TRANSFER POLICIES & PROCEDURES	***Control:*** Formal transfer policies, procedures and controls shall be in place to protect the

		transfer of information through the use of all types of communication facilities.
A.13.2.2	AGREEMENTS ON INFORMATION TRANSFER	***Control:*** Agreements shall address the secure transfer of business information between the organization and external parties.

Topic No 222: ISO27001:2013 Controls Appendix; Part 9

SYSTEM ACQUISITION, DEVELOPMENT, & MAINTENANCE

A.14.1 **SECURITY REQMTS OF INFORMATION SYSTEMS**	
A.14.1.1	INFORMATION SECURITY REQMTS ANALYSIS & SPECIFICATION
A.14.1.2	SECURING APPLICATION SERVICES ON PUBLIC NETWORKS
A.14.1.3	PROTECTING APPLICATION SERVICES TRANSACTIONS

A.14.1.1	INFORMATION SECURITY REQMTS ANALYSIS & SPECIFICATION	***Control:*** The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

A.14.2 **SECURITY IN DEV. & SUPPORT PROCESSES**	
A.14.2.1	SECURE DEVELOPMENT POLICY
A.14.2.2	SYSTEM CHANGE CONTROL PROCEDURES
A.14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES
A.14.2.4	RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES
A.14.2.5	SECURE SYSTEM ENGINEERING PRINCIPLES
A.14.2.6	SECURE DEVELOPMENT ENVIRONMENT
A.14.2.7	OUTSOURCED DEVELOPMENT
A.14.2.8	SYSTEM SECURITY TESTING
A.14.2.9	SYSTEM ACCEPTANCE TESTING

A.14.2.3	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES	***Control:*** When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4	RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES	***Control:*** Modifications to software packages shall be discouraged, limited to

		necessary changes and all changes shall be strictly controlled.
A.14.2.5	SECURE SYSTEM ENGINEERING PRINCIPLES	***Control:*** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system Implementation efforts.
A.14.2.8	SYSTEM SECURITY TESTING	***Control:*** Testing of security functionality shall be carried out during development.

A.14.3 **TEST DATA**	
A.14.3.1	PROTECTION OF TEST DATA

A.14.3.1	PROTECTION OF TEST DATA	***Control:*** Test data shall be selected carefully, protected and controlled.

Topic No 223: ISO27001:2013 Controls Appendix; Part 10

SUPPLIER RELATIONSHIPS

A.15.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS	
A.15.1.1	INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

A.15.1.2	ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS
A.15.1.3	INFORMATION & COMMUNICATION TECHNOLOGY SUPPLY CHAIN

A.15.1.1	**INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS**	***Control:*** Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A.15.2 SUPPLIER SERVICE DELIVERY MANAGEMENT	
A.15.2.1	MONITORING & REVIEW OF SUPPLIER SERVICES
A.15.2.2	MANAGING CHANGES TO SUPPLIER SERVICES

A.15.2.1	**MONITORING & REVIEW OF SUPPLIER SERVICES**	***Control:*** Organizations shall regularly monitor, review and audit supplier service delivery**.**
A.15.2.2	**MANAGING CHANGES TO SUPPLIER SERVICES**	***Control:*** Changes to the provision of services by suppliers, including maintaining & improving existing information security policies, procedures & controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Topic No 224: ISO27001:2013 Controls Appendix; Part 11

INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1 MNGMT OF INFOSEC INCIDENTS & IMPROVEMENTS	
A.16.1.1	RESPONSIBILITIES & PROCEDURES
A.16.1.2	REPORTING INFOSEC SECURITY EVENTS
A.16.1.3	REPORTING INFOSEC WEAKNESSES
A.16.1.4	ASSESSMENT OF & DECISION ON INFOSEC EVENTS
A.16.1.5	RESPONSE TO INFOSEC INCIDENTS
A.16.1.6	LEARNING FROM INFOSEC INCIDENTS
A.16.1.7	COLLECTION OF EVIDENCE

A.16.1.2	REPORTING INFORMATION SECURITY EVENTS	***Control:*** Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.2	REPORTING INFORMATION SECURITY EVENTS	***Control:*** *Information security events shall be reported through appropriate management channels as quickly as possible.*
A.16.1.3	REPORTING INFORMATION SECURITY	***Control:*** *Employees and contractors using the organization's information*

	WEAKNESSES	*systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.*
A.16.1.5	**RESPONSE TO INFORMATION SECURITY INCIDENTS**	*Control:* ***Information security incidents shall be responded to in accordance with the documented procedures.***
A.16.1.6	**LEARNING FROM INFORMATION SECURITY INCIDENTS**	*Control:* *Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.*

Topic No 225: ISO27001:2013 Controls Appendix; Part 12

INFOSEC ASPECTS OF BUSINESS CONTINUITY MNGMT

A.17.1 INFORMATION SECURITY CONTINUITY	
A.17.1.1	PLANNING INFOSEC CONTINUITY
A.17.1.2	IMPLEMENTING INFOSEC CONTINUITY
A.17.1.3	VERIFY, REVIEW, & EVALUATE INFOSEC CONTINUITY

A.17.1.1	PLANNING INFOSEC CONTINUITY	***Control:*** The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	IMPLEMENTING INFOSEC CONTINUITY	***Control:*** The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
A.17.1.3	VERIFY, REVIEW, & EVALUATE INFOSEC CONTINUITY	***Control:*** The organization shall verify the established and implemented info security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

A.17.2 REDUNDANCIES	
A.17.2.1	**AVAILABILITY OF INFORMATION PROCESSING FACILITIES**

A.17.2.1	**AVAILABILITY OF INFORMATION PROCESSING FACILITIES**	***Control:*** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Topic No 226: ISO27001:2013 Controls Appendix; Part 13

COMPLIANCE

A.18.1 COMPLIANCE WITH LEGAL & CONTRACTUAL REQUIREMENTS	
A.18.1.1	IDENTIFICATION OF APPLICABLE LEGISLATION & CONTRACTUAL REQMTS
A.18.1.2	INTELLECTUAL PROPERTY RIGHTS
A.18.1.3	PROTECTION OF RECORDS
A.18.1.4	PRIVACY & PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION
A.18.1.4	REGULATION OF CRYPTOGRAPHIC CONTROLS

A.18.1.1	**IDENTIFICATION OF APPLICABLE LEGISLATION & CONTRACTUAL REQMTS**	***Control:*** All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organiz.
A.18.1.2	**INTELLECTUAL PROPERTY RIGHTS**	***Control:*** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

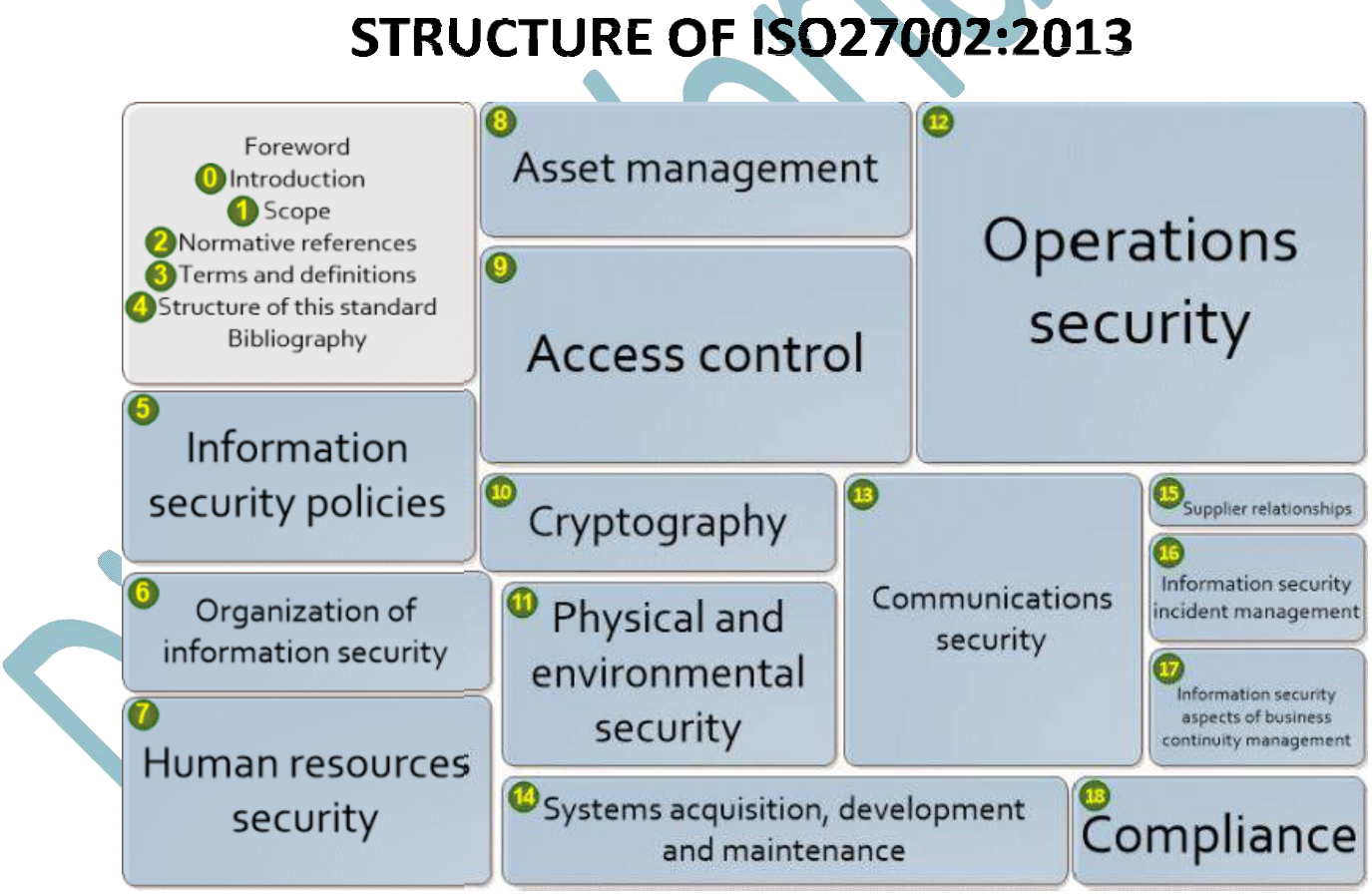
A.18.2 INFORMATION SECURITY REVIEWS	
A.18.2.1	**INDEPENDENT REVIEW OF INFORMATION SECURITY**
A.18.2.2	**COMPLIANCE WITH SECURITY POLICY & STANDARDS**
A.18.2.3	**TECHNICAL COMPLIANCE REVIEW**

A.18.2.1	**INDEPENDENT REVIEW OF INFORMATION SECURITY**	***Control:*** The organization's approach to managing information security & its implementation (i.e. control objectives, controls, policies, processes & procedures for info security) shall be reviewed independently at planned

		intervals or when significant changes occur.
A.18.2.2	**COMPLIANCE WITH SECURITY POLICY & STANDARDS**	***Control:*** Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3	**TECHNICAL COMPLIANCE REVIEW**	***Control:*** Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Topic No 227: How to Use ISO27002:2013

- **What is ISO27002:2013?**
  - Information technology -- Security techniques -- Code of practice for information security controls
  - Renamed from ISO 17799
- **0.1 Background & Context**
  - This Int'l Standard is designed for orgs to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001; or as a **guidance document** for organizations implementing commonly accepted information security controls.



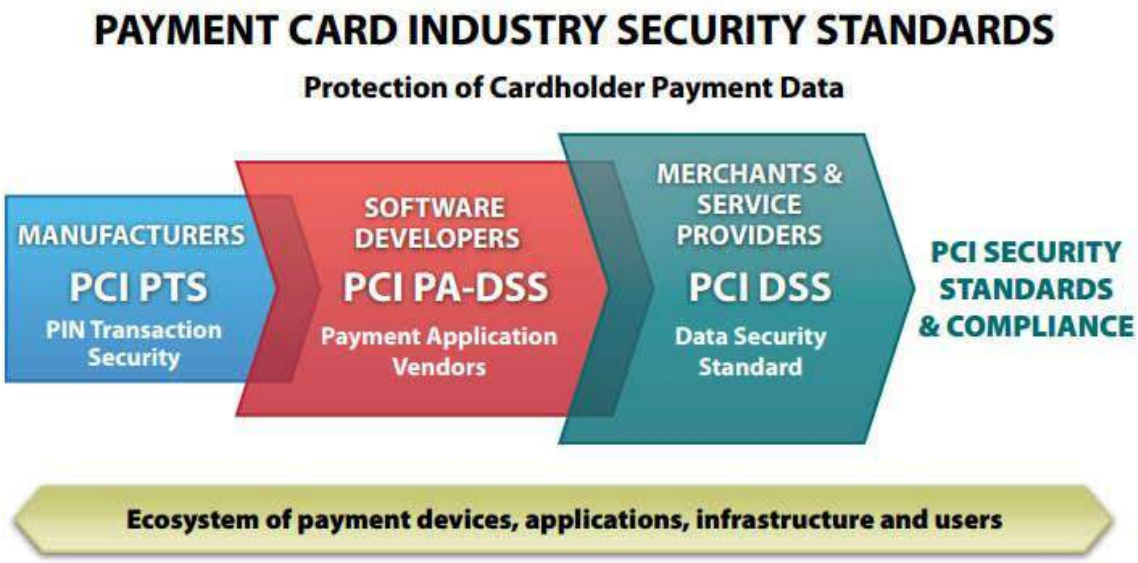
- Lets have a look at control A.5.1.2 (**Review Of The Policies Of Information Security**)

ISO27001:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	**Control:** The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		27002: Implementation Guidance: Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the org's policies and approach to managing Infosec in response to changes to the org environment, business circumstances, legal conditions or tech environment.

Topic No 228: PCI DSS V3

- **PCI Data Security Standard (DSS):**
  - Designed to ensure that ALL companies that accept, process, store or transmit credit card into maintain a secure environment
  - Managed by Security Standards Council
  - SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB
  - 6 Broad goals and 12 requirements



Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

REQMT	TEST PROCEDURES	GUIDANCE
7.1.4 Require documented approval by authorized parties specifying required privileges.	7.1.4 Select a sample of user IDs & compare with documented approvals to verify that: -Documented approval exists for the assigned privileges -The approval was by authorized parties -That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with privileges are known and authorized by management, and that their necessary for their job
8.1.4 Remove/ disable inactive user accounts within 90 days.	8.1.4 Observe user accounts to verify that any inactive accounts over 90 days .	Accounts that are regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access

- PCI is specific to the card environment to protect cardholder data
- PCI controls are very specific and in-depth compared to generic and high-level controls of ISO27001

Topic No 229: SANS/CIS CRITICAL SECURITY CONTROLS

- A very useful collection of controls for improving security posture

SN	CONTROL
1	**Inventory** of Authorized and Unauthorized **Devices**
2	**Inventory** of Authorized and Unauthorized **Software**
3	**Secure Configurations** for Hardware and Software
4	Continuous **Vulnerability Assessment** and Remediation
5	Controlled Use of **Administrative Privileges**
SN	CONTROL
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports
10	Data Recovery Capability
SN	CONTROL
11	Secure Configurations for Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know

15	Wireless Access Control
SN	CONTROL
16	Account Monitoring an Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

CONTROL 1.1: INVENTORY OF AUTH & UNAUTH DEVICES

Deploy an **automated asset inventory discovery tool** and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

CONTROL 2.1: INVENTORY OF AUTH & UNAUTH SW

Devise a that is required in the enterprise **for each type of system**, including servers, workstations, and laptops of various This list should be **monitored by file integrity checking tools** to v.

CONTROL 3.1: SECURE CONFIGS FOR HW & SW

Establish **standard secure configurations of your operating systems and software applications.** Standardized **images should represent hardened versions** of the underlying **operating system and the applications** installed on the system. These images should be **validated and refreshed on a regular basis** to update their security configuration in light of recent vulnerabilities and attack vectors.

CONTROL 4.1: CONTINUOUS VULNERABILITY ASSESSMENT & REMEDIATION

Run **automated vulnerability scanning tools** against all systems on the network on a **weekly or more frequent basis** and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator **along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.**

Use a y scanner that looks for both code vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

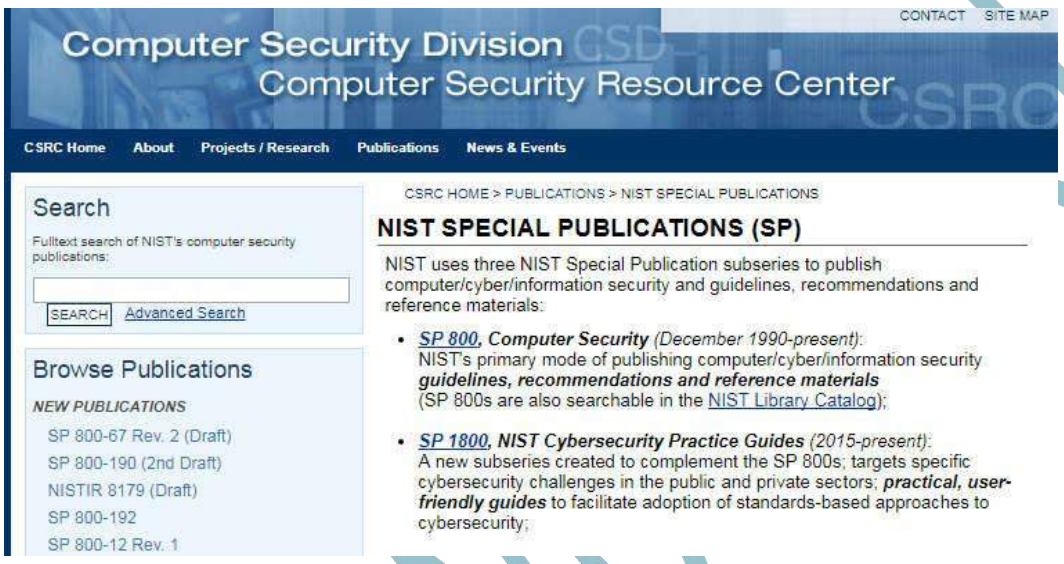
CONTROL 5.1 CONTROLLED USE OF ADMIN PRIVILEGES

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged .

- An ideal framework for more detailed and specific guidance on deeper and more stringent security controls

Topic No 230: NIST FRAMEWORK

- The Computer Security Resource Center (CSRC) website guides users to NIST resources on **computer, cyber, and information security and privacy.**
- Its content includes **publications, projects, research, news and events** from the NIST Information Technology Laboratory's (ITL) two security divisions



- ***SP 800*, Computer Security** *(December 1990-present)*:

  NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the NIST Library Catalog);

SP 800s - Computer Security

Number	Date	Title
SP 800-193 (Draft)	May 2017	**DRAFT Platform Firmware Resiliency Guidelines** Announcement and Draft Publication
SP 800-192	June 2017	**Verification and Test Methods for Access Control Policies/Models** SP 800-192 FAQ doi:10.6028/NIST.SP.800-192 [Direct Link]
SP 800-190 (Draft)	July 2017	**DRAFT Application Container Security Guide (2nd Draft)** Announcement and Draft Publication
SP 800-188 (Draft)	December 2016	**DRAFT De-Identifying Government Datasets (2nd Draft)** Announcement and Draft Publication
SP 800-187 (Draft)	November 2016	**DRAFT Guide to LTE Security** Announcement and Draft Publication
SP 800-185	December 2016	**SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash** SP 800-185 FAQ doi:10.6028/NIST.SP.800-185 [Direct Link] Comments Received on Draft SP 800-185
SP 800-184	December	**Guide for Cybersecurity Event Recovery**

NIST Special Publication 800-147B

BIOS Protection Guidelines for Servers

Andrew Regenscheid

http://dx.doi.org/10.6028/NIST.SP.800-147B

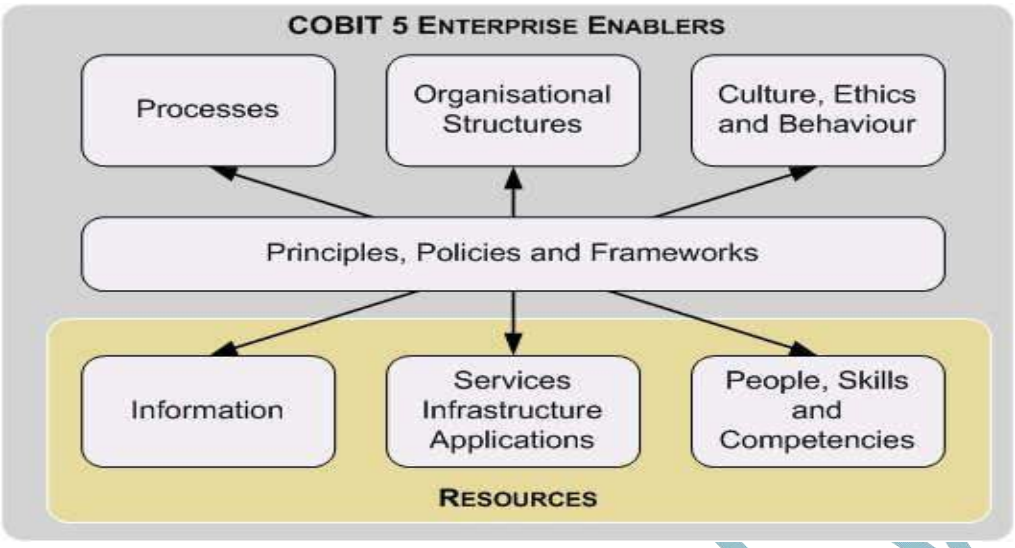
AUGUST 2014
32 PAGES DOC

- NIST has a tremendous library of free documentation on a diverse range of topics
- **Relevance is often average, however, depth and detail of material is extra-ordinary**

Topic No 231: COBIT

- COBIT:
  - ISACA framework for IT Governance
  - COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)

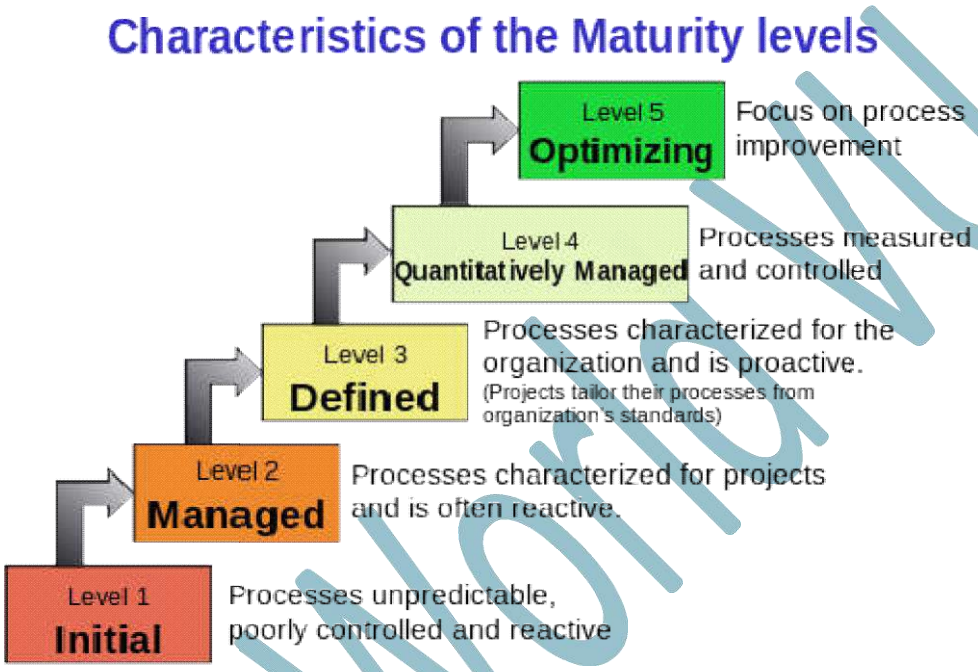
- COBIT 5 brings together **five principles** that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of **seven enablers** that optimises IT investment and use for the benefit of stakeholders (ISACA)



- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions & options; setting **direction** through prioritisation & decision making; & **monitoring** performance, compliance and progress against agreed direction and objectives **(EDM)**
- **Management plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives **(PBRM)**
- COBIT 5 is a detailed framework for IT governance developed by ISACA which has principles, enablers, and processes
- These tools assist implementers and customer organizations to successfully deploy the framework
- Certifiable framework

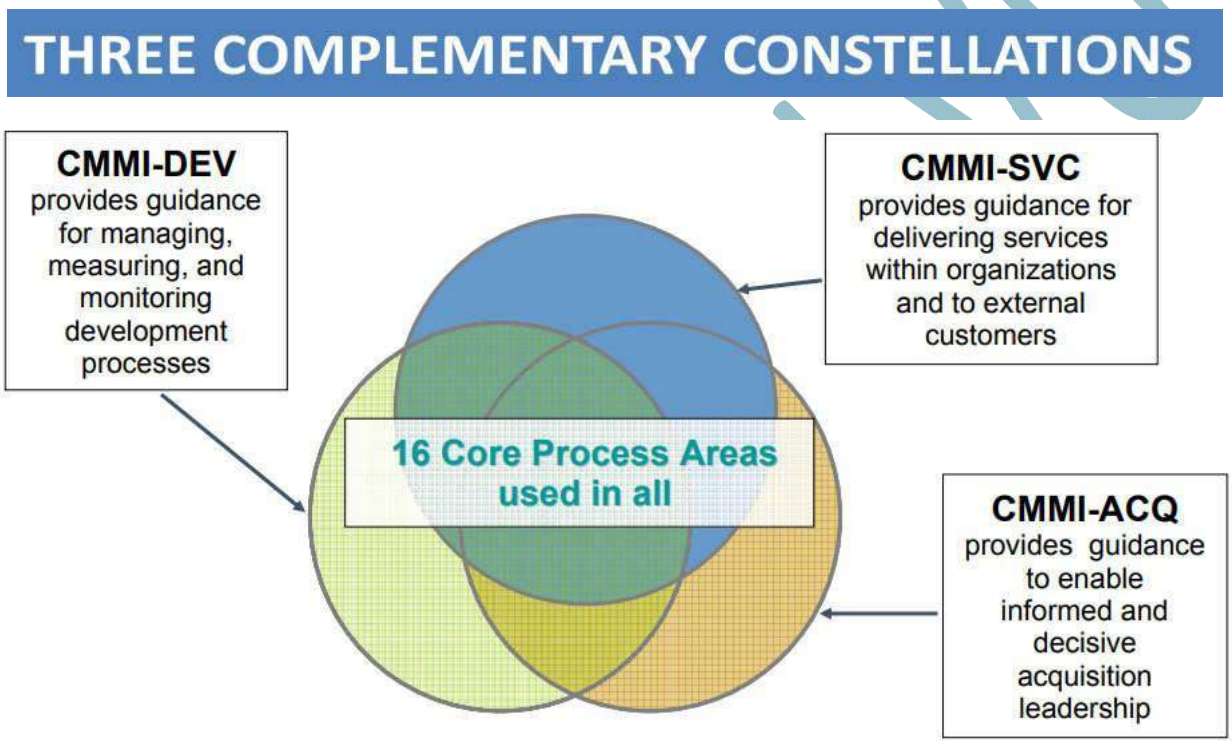
Topic No 232: CMMI

- **The Capability Maturity Model** (CMM) is a methodology used to **develop & refine an org's software dev process**. The model describes a **five-level evolutionary path** of increasingly organized & systematically more mature processes.



- CMM was developed and is promoted by the Software Engineering Institute (SEI), a research and development center sponsored by the U.S. Department of Defense (DoD)
- **Now CMMI Institute (ISACA)**
- **The Capability Maturity Model Integration (CMMI®)** is a performance improvement model for competitive organizations that want to achieve **high-performance operations.**
- Building upon an org's business performance objectives, **CMMI provides a set of practices for improving processes,** resulting in a performance improvement system that paves the way for **better operations and performance.**
- More than any other approach, CMMI **doesn't just help to improve org processes.** CMMI also has **built-in practices** that help to improve the way you use any performance improvement approach, setting you up to achieve a **positive return on your investment**

- CMMI does not provide a single process. Rather, the CMMI provides **guidance on what to do to improve your processes, not define your processes.** CMMI is designed to **compare an organization's existing processes to proven best practice** developed by members of industry, govt, & academia; reveal possible areas for improvement; & provide ways to measure progress.
- CMMI helps you to build & manage performance improvement systems that fit your unique environment.

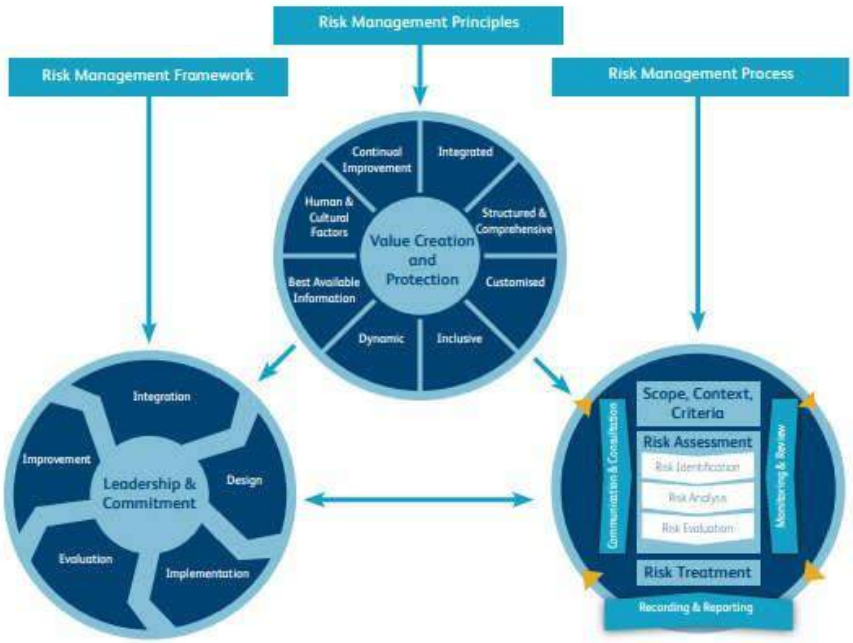


- CMMI is a very well regarded framework especially in the software industry
- Very useful for demonstrating process & quality capabilities to **customers, partners, and investors.**

Topic No 233: ISO31000:2018 – RISK MANAGEMENT – AN INTRO

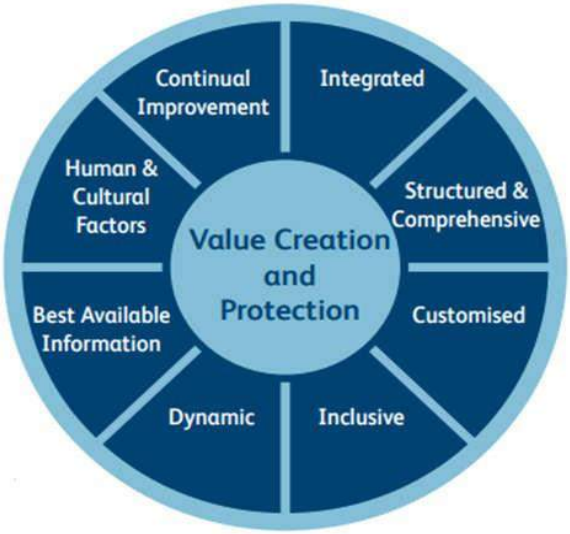
A Risk Practitioners Guide To ISO31000:2018

Figure 3: Principles, framework and risk management process from ISO 31000



Framework
5 components

8 PRINCIPLES



ISO31000 objectives:

- ISO 31000 states that the guidelines should be used by people who create and protect value in organisations by managing risks, making decisions, setting and achieving objectives and improving performance.
- ISO 31000 states that the guidelines should be used by people who create and protect value in organisations by managing risks, making decisions, setting and achieving objectives and improving performance.

ISO31000 purpose:

- ISO 31000 states that the purpose of risk management is the creation and protection of value.

Topic No 234: ISO31000:2018 – RISK MANAGEMENT – 8 PRINCIPLES

PRINCIPLES:

1. Framework and processes should be customized and proportionate.
2. Appropriate and timely involvement of stakeholders is necessary.
3. Structured and comprehensive approach is required.
4. Risk management is an integral part of all organizational activities.
5. Risk management anticipates, detects, acknowledges and responds to changes.
6. Risk management explicitly considers any limitations of available information.
7. Human and cultural factors influence all aspects of risk management.
8. Risk management is continually improved through learning and experience.

- The first five principles provide guidance on how a risk management initiative should be designed, and principles six, seven and eight relate to the operation of the risk management initiative.
- The latter principles confirm that the best information available should be used; human and cultural factors should be considered; and the risk management arrangements should ensure continual improvement.
- The first five principles are concerned with the design and planning of the risk management initiative and these principles are often summarized as proportionate, aligned, comprehensive, embedded and dynamic (PACED), as shown in Table 1.

Table 1: Principles of risk management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organisation.
Aligned	Risk management activities need to be aligned with the other activities in the organisation.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organisation.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

Topic No 235: ISO31000:2018 – RISK MANAGEMENT – FRAMEWORK

- The principles of risk management and the **framework** are closely related.
- For example, one of the principles is that risk management should be integrated and one of the components of the framework is **integration**.
- The principle outlines what must be achieved, and the framework provides information on how to achieve the required **integration**.
- The ISO 31000 guidelines are centered on leadership and commitment.
- The effectiveness of risk management will depend on its **integration** into all aspects of the organization, including decision-making.
- The remaining components of the framework are **design, implementation, evaluation and improvement**. This approach is often represented in management literature as plan-do-check-act.
- ISO 31000 provides narrative description of how the framework should support risk management activities in an organization.
- This is often referred to as the **risk architecture, strategy and protocols** of the organization, as set out in Table 2.

RISK MANAGEMENT FRAMEWORK

- ARCHITECTURE
- STRATEGY
- PROTOCOLS

Table 2: Risk management framework

Risk management architecture

- Committee structure and terms of reference
- Roles and responsibilities
- Internal reporting requirements
- External reporting controls
- Risk management assurance arrangements

Risk management strategy

- Risk management philosophy
- Arrangements for embedding risk management
- Risk appetite and attitude to risk
- Benchmark tests for significance
- Specific risk statements/policies
- Risk assessment techniques
- Risk priorities for the present year

Risk management protocols

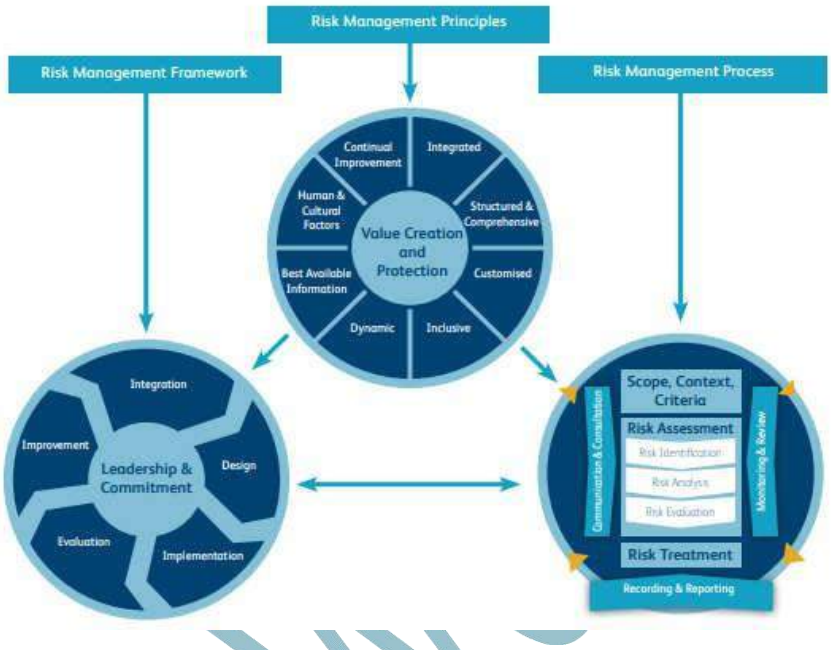
- Tools and techniques
- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Audit procedures and protocols
- Reporting/disclosures/certification

Topic No 236: ISO31000:2018 – RISK MANAGEMENT – PROCESS

A Risk Practitioners Guide To ISO31000:2018

https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

Figure 3: Principles, framework and risk management process from ISO 31000



At the center of the risk management process are the activities of **risk assessment and risk treatment**.

Risk assessment is described as having the three stages of **risk identification, risk analysis and risk evaluation**.

- Each of the three stages is described in detail in ISO 31000 and it provides valuable insight into how risks can be **identified**, how they can be **analyzed** in terms of likelihood and consequences and finally,

how they can be **evaluated** in relation to the **established risk criteria (risk appetite)** to determine whether additional action is required.

- Risk **treatment** is also a vitally important part of the risk management process and ISO 31000 provides information on the selection of **risk treatment options**, the preparation and implementation of **risk treatment plans**.
- ISO 31000 states that the selection of **risk treatment options** involves balancing the potential benefits of introducing further risk treatment (controls) against the associated cost, effort or disadvantages.
- The **risk treatment plan** should clearly identify the timescale and responsibilities for implementing the selected **risk treatments**.

Topic No 237: ISO31000:2018 – RISK MANAGEMENT – HOW TO IMPLEMENT

A Risk Practitioners Guide To ISO31000:2018

https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

Successful implementation of a risk management initiative is an ongoing process that involves working through 10 activities below on a continuous basis. These activities relate to:

(1) Plan;

(2) Implement;

(3) Measure; and

(4) Learn.

Plan:

1. Identify intended benefits of the RM initiative and gain board support
2. Plan the scope of the RM initiative and develop common language of risk
3. Establish the RM strategy, framework and the roles and responsibilities

Implement:

4. Adopt suitable risk assessment tools and an agreed risk classification system
5. Establish risk benchmarks (risk criteria) & undertake risk assessments
6. Determine risk appetite and risk tolerance levels and evaluate the existing controls

Measure:

7. Evaluate effectiveness of existing controls and introduce improvements

8. Embed risk-aware culture and align RM with other activities in the organization

Learn

9. Monitor and review risk performance indicators to measure RM contribution

10. Report risk performance in line with obligations and monitor improvement

Although ISO 31000 covers the full scope of requirements for a management system, it is for the organization to convert those requirements into a checklist and action plan.

Topic No 238 & 239: INCIDENT MANAGEMENT- I & II

Information Security Incident Management

- Have a look at ISO27002: 2013 (Page 67+) for best practices guidance

Objective:

- "To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses."

Top 10 Considerations For Incident Response

https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf

1. Audit & Due Diligence

Performing an audit will let you know how well prepared the organization is for Incident Responsein terms of:

- People
- Process
- Equipment

2. Create Response Team

- An Incident Response team should consist of people with sufficient technical skills. It is important that the team members consist of SME's (Subject Matter Experts) or Knowledge Engineers from different domains across the organization.
- Team lead
- Triage officer
- Incident handler

3. Create Documented IR Plan

- An organization should have a well-documented IR plan that would guide the IR Team during an incident.
- A comprehensive plan at minimum, should cover Roles & Responsibilities, Investigation, Triage and Mitigation, Recovery, and Documentation process.

4. Identify Indicators & Triggers

- What would be categorized as an incident at your organization?
- How important or weighty are the factors that would trigger an incident?
- Clearly define what can trigger an incident

5. Investigate the Problem

- Establishing , clearly what has occurred
- Identify what systems, people or processes have been compromised or affected based on incident
- Determine what happened & what was compromised
- Determine the point of origin of the incident where possible. This infers that you establish the source of the threat or attack vector
- Specify your investigation objectives, triage and resolution methodology

6. Triage & Mitigation

Investigation leads to the triage and resolution process. As the team identifies potential exposure, they should plan and execute effective mitigation accordingly:

- Classification of Incident
- Incident Prioritization
- Assigning specific tasks to specific people

7. Recovery

- Once a thorough investigation has been carried out, recovery is a significant step for restoring services or materials that might have been affected during an incident. This could be the task of the technical team (transition from active incident to standard monitoring)

8. Documentation & Reporting

- A comprehensive incident report is required in keeping with best practices and with the Incident Response plan. The type of reports that might be required might vary but should help in managing and reviewing incidents satisfactorily.

9. Process Review

Make intelligent decisions about important factors:

- Should I increase or decrease the number of Incident Handlers?
- What risks did we identify during the incident that needs to be followed up for action and monitored closely?

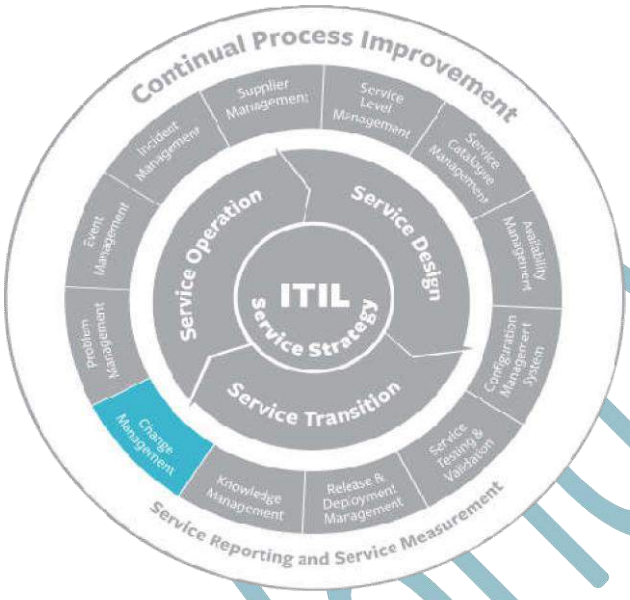
10. Practice, Practice, Practice

- Do not wait until an incident occurs before you put your team to work. Once the organization has a workable plan in place, it is advisable to run through part or all of it as a tabletop exercise, and run through various scenarios and drills.

Topic No 240: CHANGE MANAGEMENT-I

Until Change Management Best Practices

http://www.bmc.com/guides/itil-change-management.html



ITIL change management is a process designed to understand and minimize risks while making IT changes. Businesses have two main expectations of the services provided by IT:

1. The services should be stable, reliable, and predictable.
2. The services should be able to change rapidly to meet evolving business requirements.
3. These expectations are in conflict. The objective of change management is to enable IT service management to meet both expectations—to enable rapid change while minimizing the possibility of disruption to services.

Types of Changes

Standard changes are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront.

- These changes are managed according to policies that are the IT organization already has in place.
- Since these changes are subject to established policies and procedures, they are the easiest to prioritize and implement, and often don't require approval from a risk management perspective.

Normal Changes

- **T**hose that must go through the change process before being approved and implemented. If they are determined to be high-risk, a change advisory board must decide whether they will be implemented.

Emergency Changes

- Arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately.

Topic No 241: CHANGE MANAGEMENT-II

Mission

The mission of the IT change management process is to implement changes in the most efficient manner, while minimizing the negative impact on customers when changes are implemented. KPIs for tracking success of the IT change management process are:

i. Successful changes: The number of changes that have been completed successfully compared to the total number of completed changes. The higher the percentage of successful changes, the better.

ii. Backlog of changes: The number of changes that are not yet completed. While this absolute number depends on the size of the organization, it should not grow over time.

iii. Emergency changes: The number of completed "emergency" changes. This absolute number depends on the size of the organization and should not increase over time.

Scope

The scope of the IT change management process is limited to change implementations that will cause:

i. A service to become unavailable or degraded during service hours

ii. The functionality of a service to become different

iii. The CMDB to require an update

iv. Other IT changes don't usually require formal change management. Instead, they can be tracked as standard IT activities.

IT Change Management Procedures

a. Request for change review: Change coordinators use this procedure when they are dealing with requests for change.

b. Change planning: Change coordinators and specialists employ this process to prepare the implementation plans for changes.

c. Change approval: The change manager and approvers (e.g., customer representatives and service owners) follow this procedure to approve planned changes.

d. Change implementation: Specialists use this process to implement infrastructure changes.

e. change closure: Specialists follow this procedure when they perform production tests after changes have been implemented, and change coordinators employ it to close out changes.

Topic No 242: CHANGE MANAGEMENT-III

CHANGE MANAGEMENT ROLES

The **change initiator** recognizes and identifies the need for change.

- The initiator should be someone who works directly with support services tools.
- Members of your team who provide support services to customers may be best suited for this position due to their frequent interaction with the system.
- The **change coordinator** assesses requests for change that originate from incident management, problem management, release management, or continuity management.
- The change coordinator registers changes as needed to handle requests for change or receives change requests from other change initiators; determines the risk and impact for requested changes;
- Prepares implementation plans by creating tasks; and monitors the progress of changes.
- The **change manager** is generally needed in mid-sized and larger organizations. If your IT department is part of a larger company, you will need to pick one or multiple persons to perform the role of change manager.

- These individuals are responsible for managing change procedures, receiving and prioritizing change requests, evaluating the risk level associated with requests, and keeping thorough records of the outcome of each change.
- The **change advisory board** is responsible for authorizing changes and further evaluating requests when the change manager determines that there is a high risk associated with these requests.
- The board takes into account the impact that a requested change may have on all affected parties.
- When these high-risk changes are brought to the attention of the change advisory board, the board will schedule a meeting with a detailed agenda to determine how to proceed.
- The **approver** decides whether to approve or reject changes.
- The **change implementation team** consists of the specialists on your team who are responsible for actually making changes.
- You will likely be part of this team and employees directly under you may also be assigned to implement changes.
- As an IT manager, you will often be responsible for overseeing changes.

Topic No 243: PROJECT MANAGEMENT FOR INFOSEC: PART 1

- **PART 1:**
  - Importance Of Project Management For Information Security
- **CYBER SECURITY CHALLENGES:**
  - Reactive
  - Superficial
  - Contention
  - Box-Approach
  - Governance-Overkill

Denial During The Last 10 Years

- Effective project management makes or breaks any project
- Project management is the sum-total of managing, organizing, and prioritizing all resources, and tasks in order to achieve a successful outcome within the stipulated timeframe
- Successful Security Transformation Implementation is heavily dependent upon the project being in the hands of an experienced project manager:
  - Has **authority**
  - Has **domain knowledge**
  - Has ability to suggest **solutions**
- In a nut-shell, effective project management for Security Transformation is about understanding the landscape, understanding what is required to solve the problem, **and being fully committed to ensure that the successful outcome is achieved within time**
- **Common Challenges During Projects:**
  - Discipline during the one year duration
  - Prior shortage of resources
  - New initiatives (diversions)
  - Constant slippage of tasks
  - Lack of commitment by team members

- Without bold, well-organized, disciplined, and committed project management, the Security Transformation cannot be achieved within an organization
- Effective project management is the cornerstone of achieving success for Security Transformation projects

Topic No 244: PROJECT MANAGEMENT FOR INFOSEC: PART 2

PART 2:

– STRUCTURE

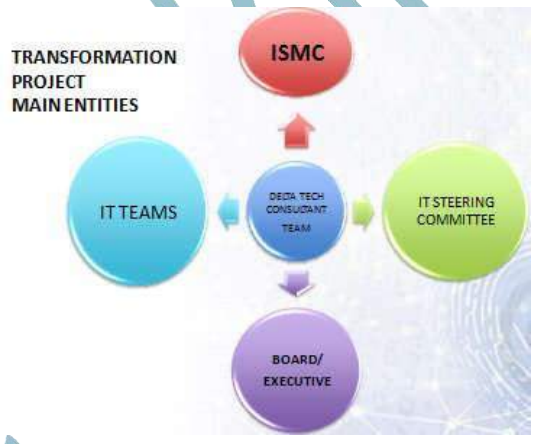
- **Structure** refers to the hierarchy and organization of teams, their interaction along with frequency, reporting, and problem-resolution mechanisms

- An effective project manager has a thorough understanding of what needs to be achieved, and is able to orchestrate resources, teams, hierarchy, and reporting in order to achieve a successful project outcome

Topic No 245: PROJECT MANAGEMENT FOR INFOSEC: PART 3

- **PART 3:**
  - REPORTING
- **Reporting** is a critical component of effective project management and has the following objectives:
- **Reporting Objectives:**

1. Creating visibility
2. Keeping resources engaged for their inputs and involvement
3. Keeping management informed of successes & challenges
4. Creating credibility
5. Ensuring team members are on their toes



- **Dashboard Objectives:**

1. Provide simple & single view of all project tracks, and where the project stands
2. Highlight problem areas for management intervention and support
3. Monthly Steering Committee & Quarterly Board reports

Forum	Frequency	Report Format	Objectives
ISMC	WEEKLY	PDF MINS OF MEETING	IDENTIFY TASKS, RESPONSIBILITY, TIMELINE
STEERING COMMITTEE	MONTHLY	PPT PRESENTATION	INFORM RELEVANT HEADS OF PROGRESS, IDENTIFY CHALLENGES
BOARD MEETING	QUARTERLY	PPT PRESENTATION	CRITICAL LOOK AT PROGRESS ACHIEVED, IDENTIFY CHALLENGES & SOLUTIONS, SEEK ASSISTANCE

- By creating an accurate, honest, and disciplined reporting mechanism, the project manager ensures that all project stakeholders are informed, involved and helping where necessary for project success

Topic No 246: PROJECT MANAGEMENT FOR INFOSEC: PART 4

- **PART 4:**
  - LEADERSHIP
- The Security Transformation requires **significant effort** over a one year period
- All resources have to be **tightly focused** on the successful outcome
- Without leadership, the transformation cannot take place
- **Leadership:**

1. Authenticity
2. Openness and transparency
3. Respect for all individuals and teams
4. Creating motivation
5. Integrity
6. Boldness to take a stand

- Technical resources will always respect a leader who has knowledge of his/her domain, and is able to provide a clear and effective strategy
- **Security Transformation Leadership** is about creating trust, and a team environment to facilitate efforts resulting in positive outcome
- Security Transformation Leadership is about working with people, at all levels to create a credible and successful project

Topic No 247: Capacity Management – Part 1

- ISO27001:2013
  - 12.1.3: The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance
- What is capacity management?
  - *A*ims to ensure that the **capacity of IT services and the IT infrastructure is able to deliver the agreed service level** targets in a cost effective and timely manner.
  - The Capacity Management process **considers all resources required to deliver the IT service, and plans for short, medium and long term** business requirements.
- ITIL suggests three sub-processes:
  - **Business** capacity management
  - **Service** capacity management
  - **Component** capacity management
- **Business** capacity management:
  - Translates business plans and needs into requirements for IT services and architecture
  - As customers' business changes, so are service requirements changing. Change in service requirements usually has an impact on demand for capacity.
- **Service** capacity management:
  - Service capacity mngmt focuses on management, control and prediction of end-to-end performance of live IT services usage and workloads.
  - It's about measuring performance and comparing it to reqmts that are set in Service Level Agreements (SLAs) or Service Level Requirements (SLRs).
- **Component** capacity management:
  - Focuses on mngmt, control, performance prediction, utilization & capacity of technology components (e.g. a hard disc, processor, etc.).

Topic No 248: Capacity Management – Part 2

- In this module, lets look at capacity management guidance from **ISO27002:2013**
- ISO27002 guidance:
  - Capacity requirements should be identified, taking into account the **business criticality** of the concerned system.
  - **System tuning and monitoring** should be applied to ensure and, where necessary, improve the **availability and efficiency of systems**.
  - **Detective controls** should be put in place to indicate problems in due time.
  - **Projections of future capacity reqmts** should take account of **new business** and system reqmts and **current & projected trends** in the organization's info processing capabilities
  - Particular attention needs to be paid to any resources with **long procurement lead times or high costs;** therefore managers should monitor the utilization of key system resources.
  - Providing sufficient capacity can be achieved by **increasing capacity or by reducing demand.**
  - Examples of managing capacity demand include:

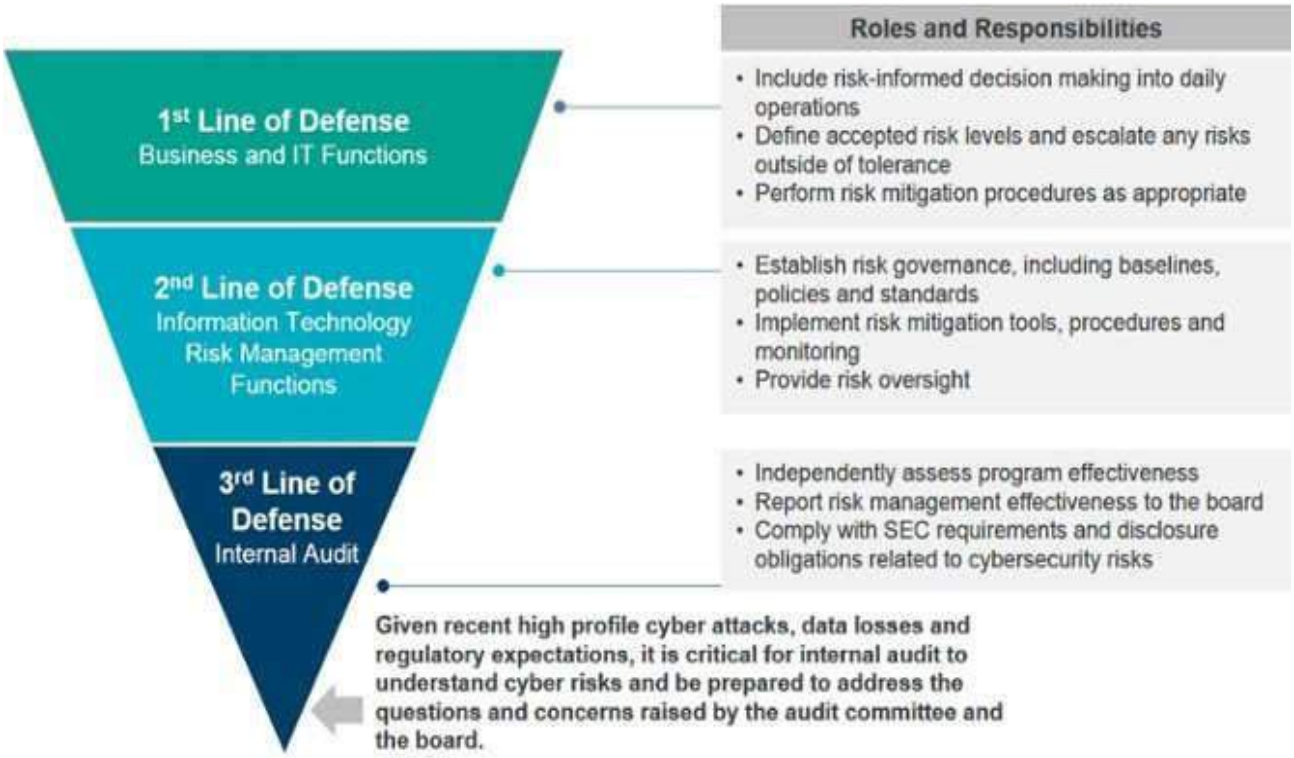
    a) **deletion of obsolete data** (disk space);

    b) **decommissioning** of applications, systems, databases or environments;

    c) **optimising** batch processes & schedules;
  - A documented capacity management plan should be considered for mission critical systems
  - Also consider human resources & offices/facilities
- **ITIL** looks at capacity management more in-depth under **service design phase**
- **ISO27002** provides some useful guidance
- In the industry we find that capacity management is not formalized as a process and lacks documentation

Topic No 249: RISK MANAGEMENT & INTERNAL AUDIT-I

Three Lines of Cyber Defense:



1. Business & IT Functions (Management Control):

The first line encompasses the information security department as well as various business units that own their cyber risks. These entities need to understand how their assets are vulnerable and actively manage their cyber risks within organizationally acceptable tolerances. Sometimes called management control, this function is tasked with managing cyber risks by executing various controls. This means handling risk events, updating key risk indicators (KRIs), and deploying and managing controls that affect people, processes and technology.

2. Risk Management

- The second line of defense is composed of risk managers looking at aggregate risks at an enterprise level. It is often simply termed risk management but can also include compliance, legal, quality control and financial control.

- The second line looks at cybersecurity control frameworks, defines KRIs and metrics, creates risk assessments, and tests and reviews conformance by tracking the actions of the first line of defense and analyzing the impact of those actions to determine their effectiveness in mitigating cyber risks. In other words, this function monitors how

management is doing in its handling of cyber risks by determining the extent that risks are actively monitored and appropriately managed.

- It is often performed under an umbrella of senior management and some board directors or a board-level committee, such as the audit committee or a risk committee. And, importantly, this second line can challenge the first line.

ISSUES WITH RISK MANAGEMENT IN PAKISTAN

1. Risk Management hierarchy not trained in IT
2. Separate Dept – not suitable given security maturity level
3. Seen as outsider
4. Low cooperation levels with IT

Topic No 250: RISK MANAGEMENT & INTERNAL AUDIT-I

Three Lines of Cyber Defense:

3. Internal Audit

- The third line of defense is internal audit. It may also include input from external auditors and/or regulators. This function, sometimes termed independent assurance, evaluates the overall process of cyber risk governance for the entire organization.
- It ensures that the organization's internal control framework is adequate for dealing with the risks the organization faces.
- As with the second line of defense, the third line can push back on the assertions of the previous lines regarding the adequacy of the controls in place. This function usually reports directly to the board or the audit committee.

Issues With Internal Audit In Pakistan

a. Not on the same page with other Depts
b. KPI seems to be highest number of observations – not organizational benefit
c. No common security vision in the organization
d. Large number of point observations do not help to improve the security posture
e. Internal audit not aware of IT team or security team framework being adopted

Topic No 251: MANAGEMENT REVIEW

How To Conduct ISO27001 Management Review

Purpose

- The purpose of the Management Review is to ensure the ISMS and its objectives continue to remain suitable, adequate and effective given the organisation's purpose, issues and risks.

Results

- The results of the management review will enable senior management to make well informed, strategic decisions that will have a material effect on information security and the way the organisation manages it.

What should be covered?

a) The status of actions from previous management reviews;

b) Changes in external and internal issues that are relevant to the information security management system;

c) Feedback on the information security performance, including trends in:

i. nonconformities and corrective actions;
ii. monitoring and measurement results;
iii. Audit results; and fulfillment of information security objectives.

d) Feedback from interested parties;

e) Results of risk assessment and status of risk treatment plan; and

f) Opportunities for continual improvement.

Who Should Attend?

- For the ISMS to be effective in an organization it needs senior management commitment and, as such, it makes sense for the members of an ISMS "Board' to have authority in matters pertaining to information security.

- Typically an ISMS Board might include the Chief Information Security Officer (CISO), Senior Information Risk Owner (SIRO), Chief Technical Officer and maybe even the CEO.
- The outputs of the management review will include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Topic No 252: Human Resource Security

In this module, lets look at human resource security.

- **Prior to employment (ISO27001):**
  - Screening
  - Terms & conditions of employment
- **ISO27002 guidance (Screening):**
  - availability of satisfactory character references, e.g. one business and one personal;
  - a verification (for completeness and accuracy) of the applicant's CV;
  - confirmation of claimed academic and professional qualifications;
  - independent identity verification (passport or similar document);
  - more detailed verification, such as **credit review or review of criminal records**
- **During employment (ISO27001):**
  - Management responsibilities
  - Awareness, education, and training
  - Disciplinary process
- **ISO27002 guidance (Disciplinary Process):**
  - The disciplinary process should not be commenced without prior verification that an infosec breach has occurred.
  - The formal disciplinary process should ensure **correct and fair treatment for employees** who are suspected of committing breaches of info security

- The formal disciplinary process should provide for a **graduated response that takes into consideration factors such as the nature and gravity of the breach** and its impact on business;

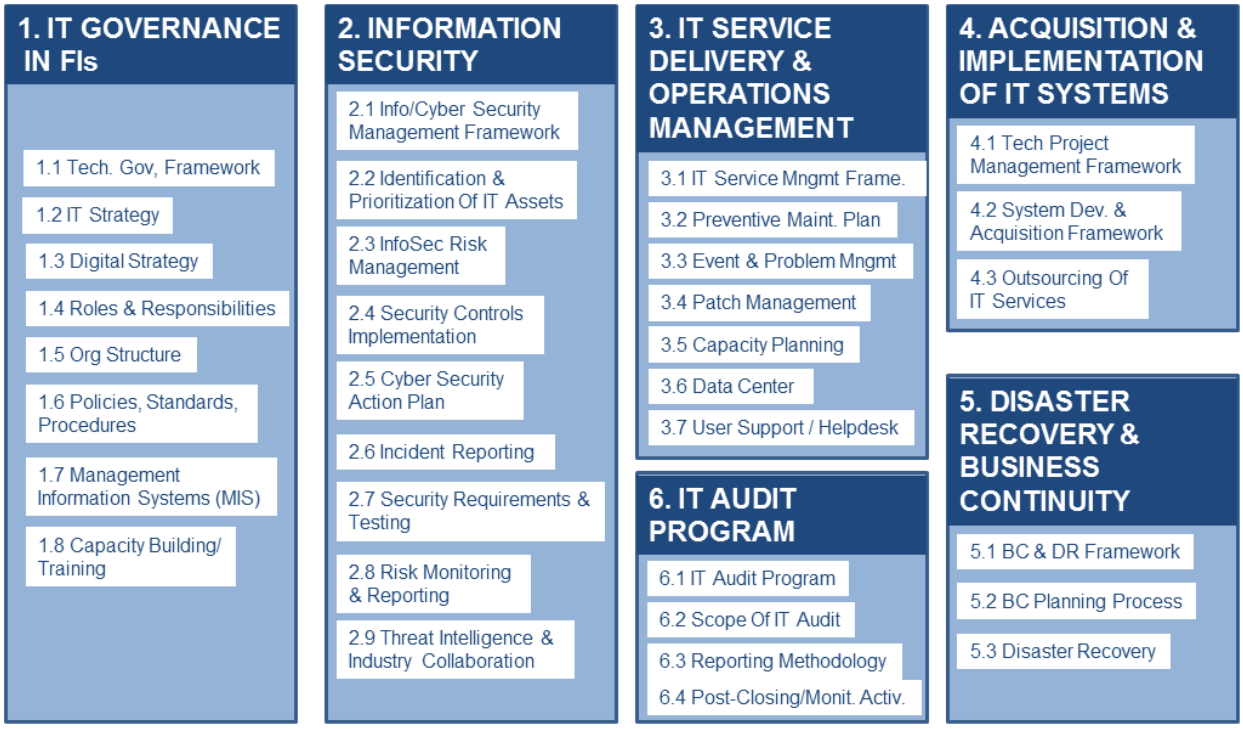
- **Termination or change of employment (ISO27001):**
  - Infosec responsibilities & duties are defined, communicated to employee or contractor & enforced

- **ISO27002 guidance (termination/change):**

- The communication of termination responsibilities should include **on-going infosec reqmts & legal responsibilities** &, where appropriate, responsibilities contained within any **confidentiality agreement & the terms & conditions of employment** continuing for a defined period after the end of the employee's or contractor's employment.
- As you can see, human resource security has quite a bit of detail
- ISO27002 provides very useful guidance and elaborates the ISO27001 controls

Topic No 253: SBP CIRC. # 5, TECHNOLOGY GOVERNANCE FRAMEWORK

Sbp Technology Governance And Risk Management Framework



OBJECTIVES

- The framework aims to provide enabling regulatory environment for managing risks associated with the acquisition, development, deployment and use of technology and shall serve as **SBP's baseline requirements for all FI(s).**
- The FI(s) shall **upgrade their systems, controls and procedures to ensure compliance** with this framework latest by **June 30, 2018.**
- The FI(s) shall assess and conduct a **gap analysis** between their current status & this framework and draw a **time-bound action plan to address the gaps and comply** with the guidelines in this framework

OVERVIEW

- The instructions are focused on **enhancing the proactive and reactive environments** in FI(s) to various facets and dimensions of technology including information security, technology operations, audit, business continuity, project/performance management and related domains (pg 5)

- FI(s) shall adopt an **integrated risk management approach to identify, measure, monitor and control technology risks** (page 5)
- The Framework consists of **6 domains and 35 sub-domains**
- Overall the **Framework is a combination of COBIT, ITIL, and ISO27001:2013 (ISMS)**

Implementation Mechanism

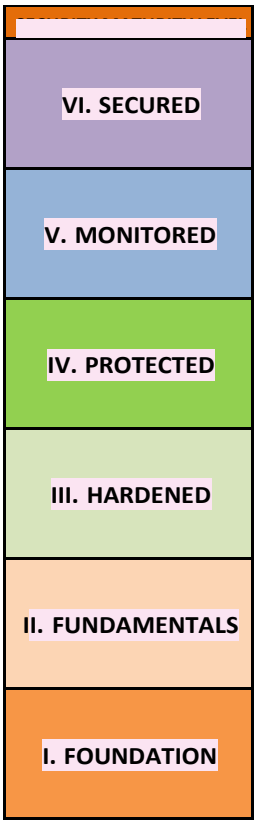
- Gap analysis
- Documentation
- Implementation

Topic No 254: CYBER SECURITY MATURITY MATRIX - OVERVIEW

In this module we will introduce the Cyber Security Maturity Matrix (CSMM)

Industry Security Challenges:

- Grass-roots security controls have not been implemented
- Haphazard, reactive security approach
- Not following any structured security architecture or framework



What challenges does CSMM address?

- 5 characteristics of Information Security in Pakistan:
  - Reactive
  - Superficial
  - Box approach
  - Contention
  - Governance overkill

How is the local industry coping with security implementation?

a. Large organizations

b. Medium sized organizations

c. Small organizations

Issues with large organizations:

1. Missed out on security hardening
2. Vulnerability management effectively not being done as per Int'l best-practice
3. Attempting automation or box approach

Issues with medium sized organizations:

1. Don't have sufficient security expertise and knowledge
2. Security was never a focus
3. Have built insecure IT networks just like the large organizations
4. VM and hardening missing here too

Issues with smaller organizations:

1. Mostly have pirated software
2. Enterprise antivirus and Microsoft Active Directory (AD) mostly missing
3. Not enough budget for security
4. No personnel allocated for security

The industry status:

1. Industry lacks a standard & authentic roadmap of how to achieve security
2. No mechanism to measure or certify security
3. Divergent understanding of how security will be achieved

SECURITY MATURITY LEVEL	MINIMUM CHARACTERISTICS
VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Respon
	Threat Protection
	Threat Simulation
V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection
IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls
III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle
II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool
I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

How does CSMM help?

- Offers a proactive, structured, sequential model to implement security
- Model is certifiable
- Cyber Security Certification Board (CSCB) will certify security status of organizations

Topic No 255: CSMM - LAYER 1 - FOUNDATION

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM): layer 1

I. FOUNDATION	Edge FW With Filtering
	Active Directory (WS/S)
	Licensed Enterprise AV (WS/S)
	Licensed Windows OS (WS/S) Or Open Source

: LICENSED WINDOWS OR OPEN SOURCE

- Licensed windows (MS)
- Ubuntu open source
- Other numerous open source alternatives
- Basic requirement for a secure IT setup
- Pirated software infested with malware

: LICENSED ENTERPRISE ANTI-VIRUS

- Users usually do not update their AV
- Visibility dashboard, & central mngmt reqd
- Consistent mngmt of hundreds or thousands of anti-virus agents
- Many anti-virus agents are out-of-synch with the update-server

: ACTIVE DIRECTORY (AD)

- Active Directory (AD) is essential not only to regulate account management (authentication and authorization) but also to enforce and manage security controls

: Edge FW with Filtering

- Forms first line of perimeter defense
- Filtering of incoming and outgoing traffic
- DMZ for hosted services
- Policy enforcement for security

Topic No 255: CSMM - Layer 2 - Fundamentals

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 2

II. FUNDAMENTALS	Network Segmentation With VLANs By Dept/Service, & DMZ
	Edge NGN FW With Web, Email, Anti-malware Filtering
	Min Quarterly Credential Based VM Cycle
	Licensed Or Open Source VM Tool

: LICENSED OR OPEN SOURCE VM TOOL

- Vulnerability management or patch management is a foundational layer of security practice
- Open source: OpenVAS
- Licensed: Qualys, Nessus, Rapid7

: MIN QUARTERLY CREDENTIAL BASED VM CYCLE

- For those organizations that have not conducted VM practice before
- International best-practice is weekly VM cycle

: Edge NGN FW With Web, Email, Anti-malware Filtering

- Typical NGN FW: Fortinet
- Features: VPNs, web filtering, email anti-spam filtering, Antivirus, anti-malware, application visibility & control, access-lists

2.4. Network Segmentation With VLANs by Dept./Service & DMZ

- Network segmentation helps create separate broadcast domains
- Separate policies and filtering possible for each separate VLAN
- Helps manage traffic
- Segregates traffic into traffic-types

Topic No 257: CSMM - LAYER 3: HARDENED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 3

III. HARDENED	Software Security Hardening Program
	NGN FW At Data Center Entry Point With Filtering
	CIS Security Benchmarks Hardening Of All IT Assets
	Min Monthly Credential Based VM Cycle

: Minimum Monthly Credential Based VM Scan

- Now moved to monthly scan from quarterly scan
- Credential based scan from non-credential scan

: CIS BENCHMARKS HARDENING OF ALL IT ASSETS

- Hardening covered in detail in this course
- Planning, pilot, production implementation
- Usually takes 6-8 months depending upon size of organization

: NGN FW At Datacenter Entry Point With Filtering

- Filtering and malware protection at datacenter entry point often ignored
- All traffic including internal user traffic entering or exiting data center needs to be filtered

: Software Security Hardening Program

- Software security program needs to be developed
- Software security hardening: controls identification, pilot controls implementation, validation, testing, change mngmt, PROD

Topic No 258: CSMM - LAYER 4: PROTECTED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 4

IV. PROTECTED	ISO27001:2013 (ISMS) Certification
	External/Internal Penetration Test (Critical Assets)
	Software Source Code Review For Critical Applications
	CIS 20 Critical Security Controls

: CIS 20 CRITICAL SECURITY CONTROLS

- Aggregate control set covering all aspects of IT
- CIS benchmarks covered individual asset hardening
- Excellent set of security controls
- Sets out International best-practices

: Software Source Code Review For Critical Applications

- Source code review is a specialized activity which may be conducted in a manual or automated manner
- Specific to the software technology platform
- Peer or third-party

: External/Internal Penetration Test (Critical Assets):

- and security hardening has been performed
- Third-party review of vulnerabilities and hacker-view of assets

: ISO27001:2013 (ISMS) Certification

- Global gold standard for Information Security governance
- Needs to be wisely used as it is both deep and broad
- Utilize as security governance framework leveraging VM and security hardening

Topic No 259: CSMM - LAYER 5: MONITORED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 5

V. MONITORED	Security Operations Center (SOC) Implementation
	Critical Data Encryption
	Data Loss Prevention (DLP) Solution
	SIEM Solution For Security Events Detection

: SIEM SOLUTION FOR SECURITY EVENTS DETECTION

- SIEM solutions provide security log collection, dashboard reporting, root-cause analysis, and correlation
- Leading SIEM solutions: LogRhythm, IBM Q-Radar, Splunk, Elastic Search

: DATA LOSS PREVENTION (DLP) SOLUTION

- Classification, visibility, and control of data
- Monitoring and blocking of data leakage and data exfiltration
- Network DLP and system DLP (agent)

: CRITICAL DATA ENCRYPTION

- Protect intellectual property and confidential information
- Confidentiality and integrity of data
- Encrypt data at rest, in transit, and in use
- Laptop HDD and removable media

: SECURITY OPERATIONS CENTER (SOC) IMPLEMENTATION

- After implementation of the first four layers, its time to consolidate security operations
- People, process, and technology/tools
- Similar to a NOC but for security purposes
- SIEM is starting point

Topic No 260: CSMM - LAYER 6: SECURED

- In this module we will introduce the Cyber Security Maturity Matrix (CSMM), layer 6

VI. SECURED	Red Team Penetration Testing
	Security Orchestration, Automation, & Incident Response
	Threat Protection
	Threat Simulation

: THREAT SIMULATION

- Platform such as Redwolf Security (www.redwolfsecurity.com)
- Security testing, load testing, and DDOS testing
- Misconfigured security devices and incident response

: THREAT PROTECTION

- Various threat protection solutions
- Best solutions will map to the vulnerability condition of your IT assets e.g. Qualys Threat Protect
- Helps to pinpoint most critical assets and prioritize patching
- Protection Live Threat Intelligence Feed displays the latest vulnerability disclosures and maps them to your impacted IT assets. You can see the number of assets affected by each threat, and drill down into asset details.

: SECURITY ORCHESTRATION, AUTOMATION, AND INCIDENT RESPONSE

- Solution such as Cybersponse (www.cybersponse.com)
- From triaging and investigating alerts to collaboration and remediation between team members, CyberSponse takes your security operation team to the next level.

: RED TEAM PENETRATION TESTING

- Red team and blue team
- Attack & defense simulation
- Continuously find holes in security defenses
- Uncover security vulnerabilities before hackers exploit them

Topic No 261: InfoSecurity Lifecycle – Security Validation

- Lets have a re-look at the 8-Step Security Hardening Methodology

- **Validation during security hardening**:
  - Purpose here is to only **validate or confirm** that the intended controls have **been correctly and completely applied** in the pilot setup
  - Nothing mentioned for production environment
  - Nothing mentioned for **BUSINESS LAUNCH (GO-LIVE)**
- Now lets look at the more comprehensive Information Security Lifecycle (7 stages) which is not specific to security hardening

- In the Information Security Lifecycle chart, we have already gone into production **"environment"** with Stage 4
- However, formal approval for **BUSINESS LAUNCH** (GO-LIVE) has not yet been issued
- **Security accreditation has not taken place**

- In the Information Security Lifecycle chart Stage 5 & 6:
  - Refer to activities carried out in PRODUCTION "environment"

- But before Business launch (GO-LIVE) has taken place

- The formal **business launch or GO-LIVE** only takes place after Information Security team **accredits** that the new application/portal or service is secure
- Business launch or GO-LIVE also has business related activities as dependencies such as marketing, & other
- Business launch or GO-LIVE **dependencies**:
  - UAT & application **bug testing and feature testing**
  - **Facilities** readiness
  - **Sales & marketing** Launch **ceremony**
  - **Partner** readiness
  - Org **service readiness**

- Lets look at the following steps in more detail and granularity in the following modules:
  - Security **validation**
  - Security **testing**
  - Security **accreditation**

Topic No 262: What is Security Validation?

- **What does security validation mean?**
  - To confirm via **walk-through of system or device** that the security controls implemented by an IT team have **actually been implemented correctly**
- **Who implements the security controls?**
  - Under the Security Transformation Model, security controls are implemented by the IT teams
- **Who conducts security validation?**
  -
- **Why do we need to validate security controls?**
  - To check the **completeness** of the controls
  - To check the **correctness** of the controls
  - As an overall **assurance**

1. To check the **completeness** of the controls:
   - Usually **100's of controls** need to be implemented
   - There may be **genuine omissions** by technical team members
   - There may have been **errors** made
2. To check the **correctness** of controls:
   - Technical **capabilities** of **teams** vary
   - Technical capabilities of **team members** vary
   - A technical issue may not have been understood correctly

3. As an overall assurance:
   - IT team may not have sufficient resources to ensure 100% completeness and correctness
   - Implementation by IT and validation by Information Security team forms a healthy team relationship
   - This is also referred to as **maker-checker** principal

- Some of the controls may have been designated as **"not-applicable"** or **"not possible"** and the reasons and justification needs to be reviewed
- **Significant resources are allocated** to the security transformational program; **even one control missed** may affect the security posture
- **Uncovered** at the time of **hack/attack**
- **Ability, integrity and diligence** of team members are key factors
- **Healthy technical debate and cross-checks** have a **positive outcome** on the program

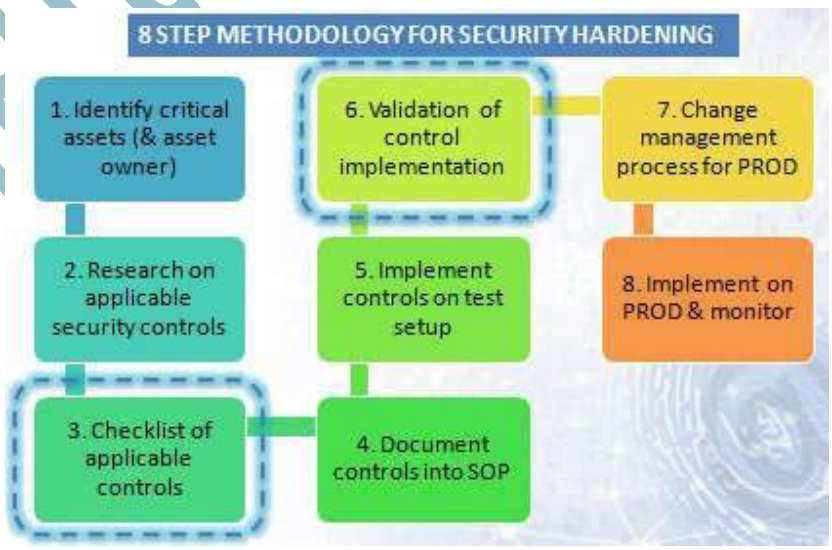
The Information Security team or the ISMC is tasked with the **overall responsibility** of the success of the program

Any **lapses discovered later** fall **squarely** under the **responsibility of InfoSec/ISMC**

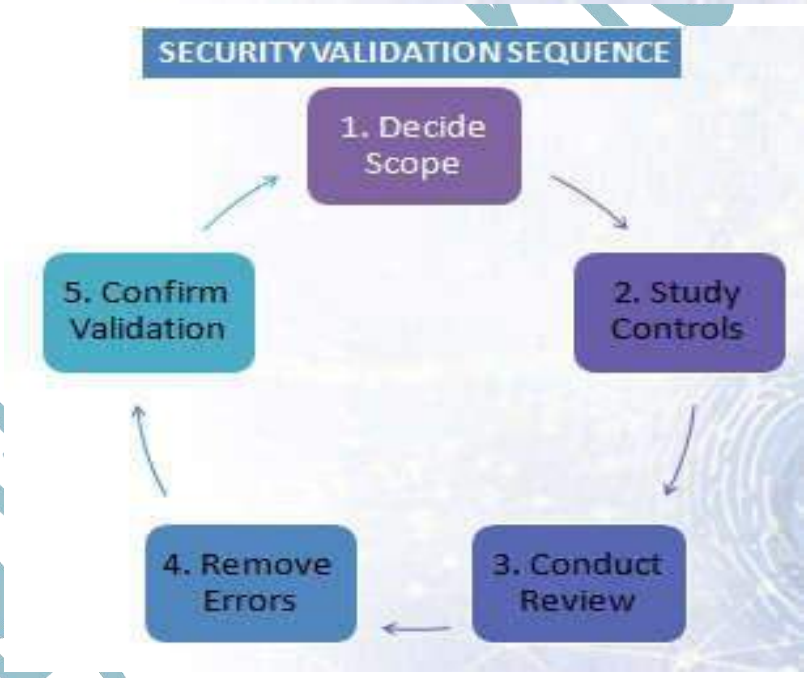
- Security validation becomes an **essential activity** and needs to be established in an environment of **healthy & professional commitment** to ensure the **100% complete and correct implementation & upkeep** of the controls

Topic No 263: How is Security Validation Performed?

- **Ownership** of security validation lies with Information Security team, alternately with an Information Security consultant
- **Driven by ISMC or Head of Information Security**
- **Security validation is the same** irrespective if performed specific to 8-Step Security Hardening (Model) or to the Information Security Lifecycle



STEP	DESCRIPTION	PERFORMED BY	FACILITATED BY
1	IDENTIFY CRITICAL ASSETS (& ASSET OWNER)	ISMC	HEAD OF IT SECTION
2	RESEARCH APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	ISMC
3	CHECLIST OF APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	TEAM LEAD
4	DOCUMENT CONTROLS INTO SOP	TEAM LEAD	INFOSEC TEAM
5	IMPLEMENT CONTROLS ON TEST SETUP	IT OPERATIONS TEAM	TEAM LEAD
6	VALIDATION OF CONTROL IMPLEMENTATION	INFOSEC TEAM	IT OPERATIONS TEAM
7	CHANGE MANAGEMENT PROCESS FOR PRODUCTION	TEAM LEAD	ISMC
8	PRODUCTION & MONITOR	IT OPERATIONS TEAM	TEAM LEAD



1. **Decide Scope**
   - Acquire checklist of applied controls from IT team
   - Decide stakeholders who will conduct review (IT & InfoSec)
   - Schedule the review and send formal email to IT (plus calendar invite)
2. **Study Controls**
   - Information Security team to acquire original controls from CIS/DISA/other

- Study & understand the controls
- Mark the checklist & ensure correctness
- Prepare docs & notes for actual review

3. Conduct Review

- One person to conduct review & one to take notes
- Walkthrough of each control
- Random sampling of controls (20-30%)
- Agree on any action items for shortcomings with timeline

Important to discuss & understand controls marked by IT team as:

- Not-applicable
- Not-possible

Understand reasoning

Verify dependencies if any

Challenge the IT team view wherever appropriate

4. Remove Errors:

- IT team to remove any shortcomings or omissions in control implementation
- IT team reports back to InfoSec team when all shortcomings fixed

5. Confirm Validation

- InfoSec team schedules another session with IT team to confirm that all shortcomings have been removed
- InfoSec team adds a confirmation column & comments column to checklist
- Status of validation communicated to relevant IT teams & stakeholders
- Records updated to register the validation activity
- Project management stats updated accordingly (% complete)

Topic No 264: What Is Security Testing?

- **What is security testing?**
  - Security testing is a process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended
- **Security testing is not validation**
  - Security testing consists of running tests through a manual process or automated tools to discover weaknesses, flaws, or bugs in the software, application or device
- **Types of security testing:**
  - Vulnerability assessment (VA)
  - Penetration testing (PT)
  - Other security tests through various automated tools
  - Code review (initiated in test environment)

1. **Vulnerability assessment:**
   - VA scanners have various tests built-in such as for malware, vulnerabilities, web application flaws (e.g. OWASP top ten)
   - Compliance scanning against CIS/DISA benchmarks

2. Penetration Testing:

- Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
- Usually outsourced to a third-party depending on nature and criticality of the application or service being launched
- Highly specialized skill not commonly found in-house
- Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target

before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

3. Other security tests:

- If the testing is being conducted in-house, the tests should be conducted in the pilot/testing/staging environment and re-validated in the Production environment
- If the testing is being conducted by a third-party specialist (such as for penetration testing), it will normally be conducted only in the Production environment (prior to GO-LIVE)

Other security tests (in-house):

- In-house testing capability & experience
- Conduct the tests (e.g. OWASP ZAP tool)
- Report findings
- Re-confirm once remediation done by IT

Other security tests (outsourced):

- As mentioned, will most likely be conducted in Production environment, prior to GO-LIVE
- Follow same sequence as for in-house testing

4. Code review:

- Code review examines flaws and vulnerabilities in programming source code
- A complete cycle, initiated early and in pilot testing phase
- May be conducted for production applications as well
- Requires a mature internal process, experience and capability
- May be integrated with software QA testing

Topic No 265 & 266: What Is Security Accreditation?

- **What is security accreditation?**
  - Accreditation is the formal acceptance of the adequacy of the system's overall security by the management (SANS)
- Whenever a new, **significant portal, application, or service is launched**, management requires **Information Security team to certify after carrying out the required security validation & security testing** that the
- Security of the new portal/application or service has been **thoroughly examined & tested** and **meets the min requirements** as per **organizational security policy**
- That the new portal/application is safe & secure & is **free from security risks**

Security Accreditation Sequence

1. **Organize**
   - Collect all security **requirements**, related security **policy & SOPs**, hardening checklists, validation **status reports**, **test reports**, completion status reports Information Security team ensures that the full context of the security risks/impact are understood
   - Subsequent security hardening & testing has been fully covered

2. **Prepare Checklist & Share With Stakeholders**
   - Checklist should cover all activities & their status for completion of accreditation
   - Share with stakeholders for feedback

3. **Confirm Tests**
   - Core activity: confirm that **all test reports are satisfactory**
   - All tests and follow-up remediation measures have been completed

4. **Documentation & Processes (Complete)**
   - Reconfirm **correct versions**
   - Re-check **checklists, SOPs**
   - **Backups & DR**
   - All **change control measures** & **sign-offs**
   - Re-check all **management approvals**
   - Re-check **UATs,** customer sign-offs
   - Check **application performance** issues

5. **Team Meeting**
   - Call team meeting and **report status** of all activities
   - List any **snags** & decide completion dates
   - Seek **stakeholder sign-off** on accreditation form

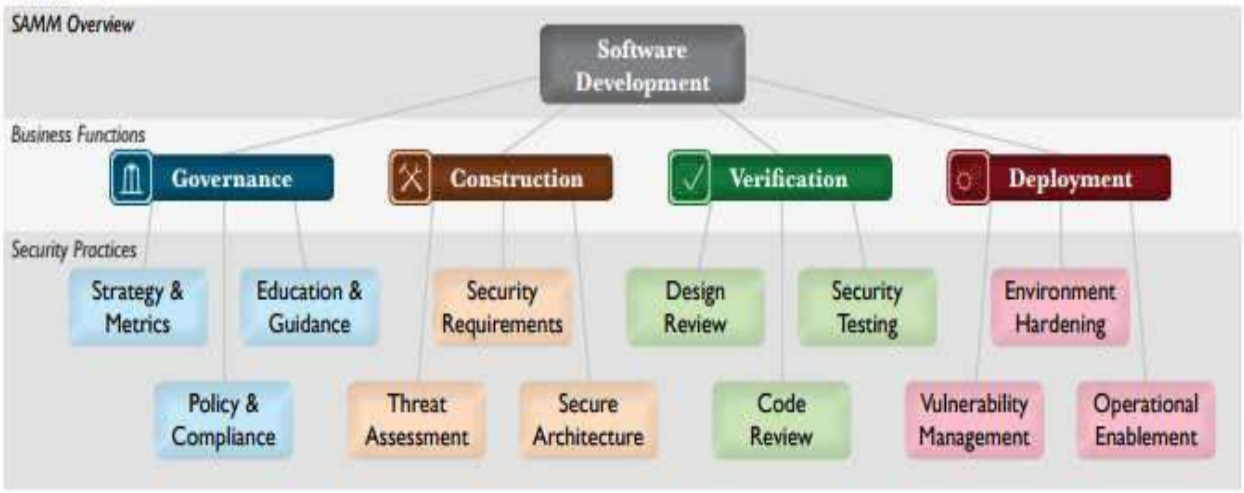
- Clarify & recap security requirements & SOPs
- Clarify **what actions will invalidate** the security accreditation

6. Issue Accreditation

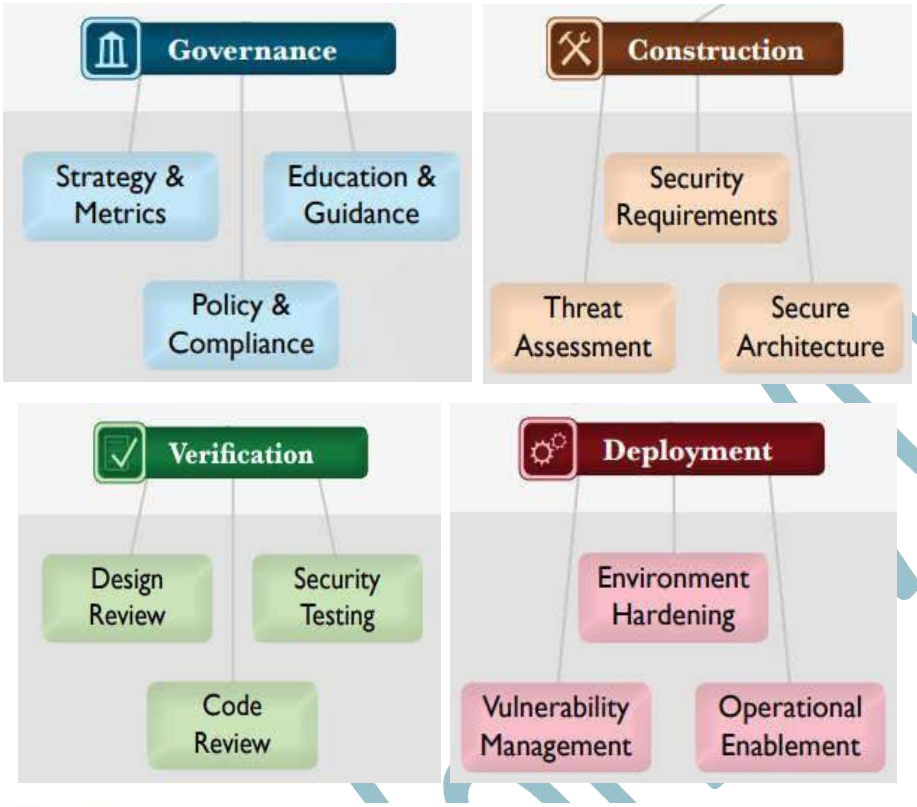
- Once all details completed on accreditation sign-off form issue accreditation
- Business has GO-LIVE permission using tested versions
- Enter activities for accredited IT assets into IT audit program
- Update Operations teams, incident management, and risk management register

Topic No 267: Embedding InfoSec Lifecycle into SDLC

- The systems development life-cycle (SDLC) should embed the Information Security activities forming a sec-SDLC (secure SDLC)
- Software Assurance Maturity Model (SAMM) developed by OWASP
  - A guide to building security into software development
  - 96 page PDF



- Four **critical business functions**
- For each business function there are **three security practices**
- For each security practice, **three maturity levels as objectives**
- The Software Assurance Maturity Model (SAMM) is an **open framework** to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.



Maturity Levels

Each of the twelve Security Practices has three defined Maturity Levels and an implicit starting point at zero. The details for each level differs between the Practices, but they generally represent:

0 Implicit starting point representing the activities in the Practice being unfulfilled

1 Initial understanding and ad hoc provision of Security Practice

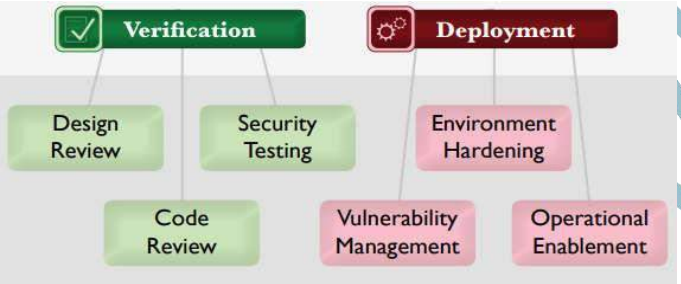
2 Increase efficiency and/or effectiveness of the Security Practice

3 Comprehensive mastery of the Security Practice at scale

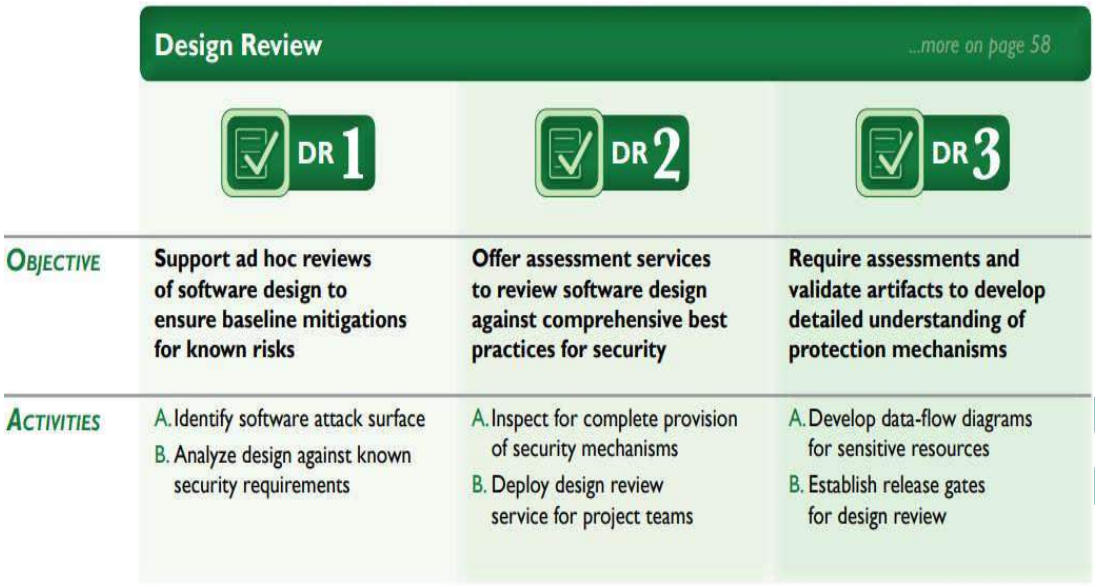
- The SAMM document sections:
  1. Understanding the model
  2. Applying the model
  3. Security practices
  4. Case studies

Topic No 268: Software Security Testing & Validation–1

- testing & validation during the following phases:
  - Verification
  - Deployment

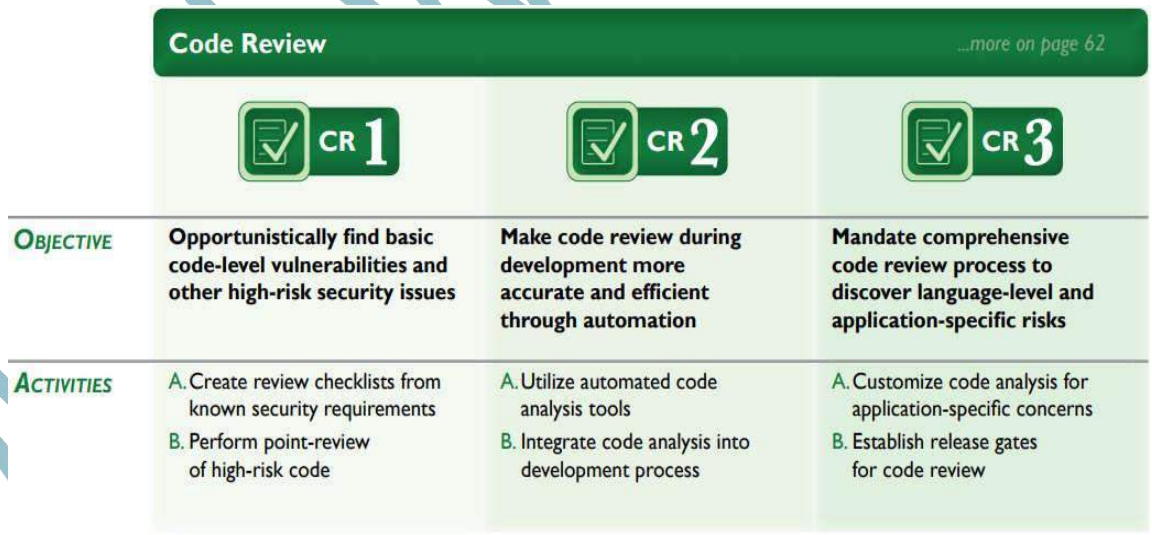


- **OWASP Software Assurance Maturity Model (SAMM) Verification Phase:**
  - Design Review
  - Code Review
  - Security Testing
- **Design Review:**
  - Focused on assessment of software design and architecture for security-related problems
  - Detect architecture-level issues early in software development and thereby avoid potentially large costs from refactoring later due to security concerns.



Design Review	DR 1	DR 2	DR 3
Objective	Support ad hoc reviews of software design to ensure baseline mitigations for known risks	Offer assessment services to review software design against comprehensive best practices for security	Require assessments and validate artifacts to develop detailed understanding of protection mechanisms
Activities	A. Identify software attack surface B. Analyze design against known security requirements	A. Inspect for complete provision of security mechanisms B. Deploy design review service for project teams	A. Develop data-flow diagrams for sensitive resources B. Establish release gates for design review

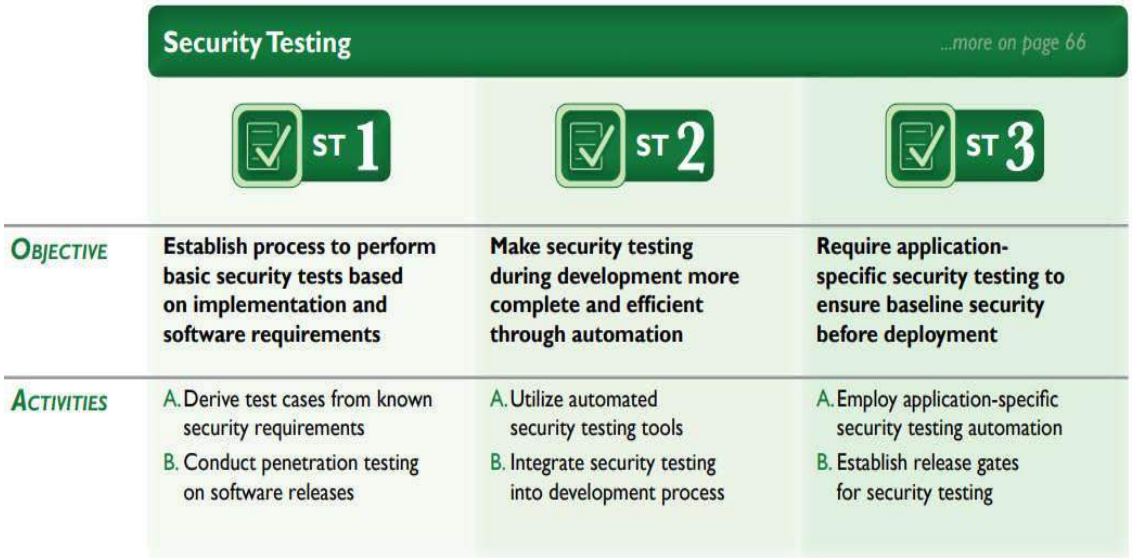
- **Code Review:**
  - Focused on inspection of software at the source code level in order to find security vulnerabilities.
  - Code-level vulnerabilities are generally simple to understand conceptually, but even **informed developers can easily make mistakes** that leave software open to potential compromise.



Code Review	CR 1	CR 2	CR 3
Objective	Opportunistically find basic code-level vulnerabilities and other high-risk security issues	Make code review during development more accurate and efficient through automation	Mandate comprehensive code review process to discover language-level and application-specific risks
Activities	A. Create review checklists from known security requirements B. Perform point-review of high-risk code	A. Utilize automated code analysis tools B. Integrate code analysis into development process	A. Customize code analysis for application-specific concerns B. Establish release gates for code review

- **Security Testing:**
  - Focused on **inspection of software in the runtime environment** in order to find security problems.

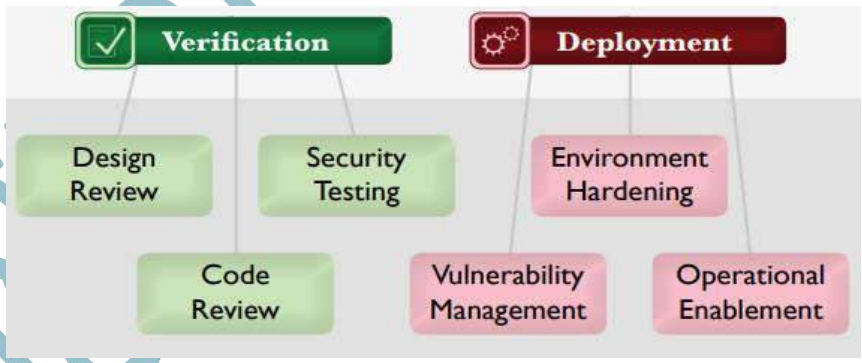
- These testing activities bolster the assurance case for software by **checking it in the same context in which it is expected to run**, thus making visible **operational misconfigurations or errors in business logic** that are difficult to otherwise find.



Security Testing	ST 1	ST 2	ST 3
OBJECTIVE	Establish process to perform basic security tests based on implementation and software requirements	Make security testing during development more complete and efficient through automation	Require application-specific security testing to ensure baseline security before deployment
ACTIVITIES	A. Derive test cases from known security requirements B. Conduct penetration testing on software releases	A. Utilize automated security testing tools B. Integrate security testing into development process	A. Employ application-specific security testing automation B. Establish release gates for security testing

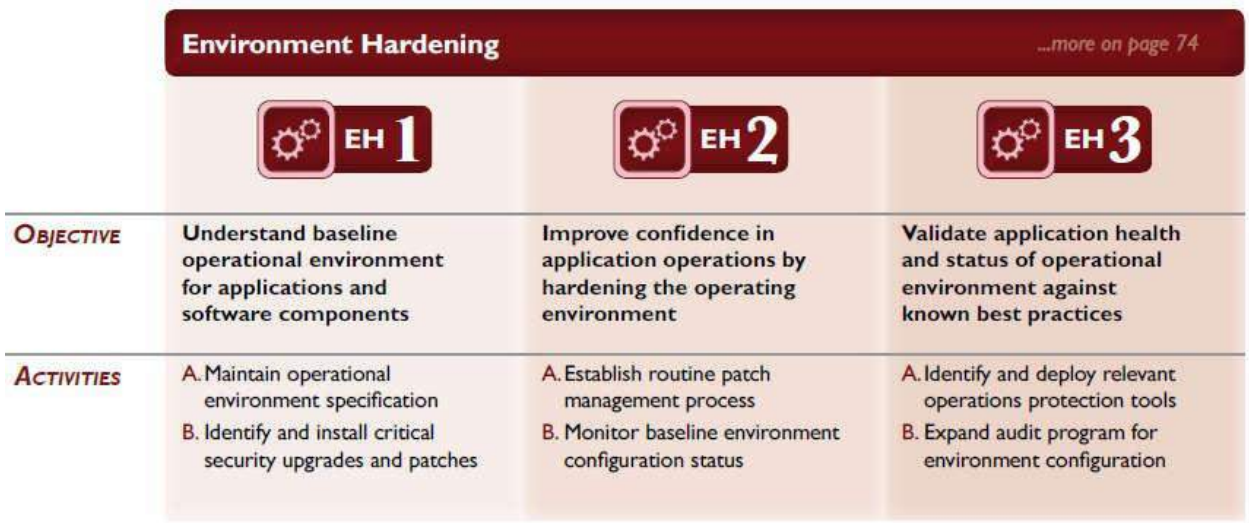
Topic No 269: Software Security Testing & Validation–2

- The OWASP Software Assurance Maturity Model (SAMM) undertakes software security testing & validation during the following phases:
  - Verification
  - **Deployment**



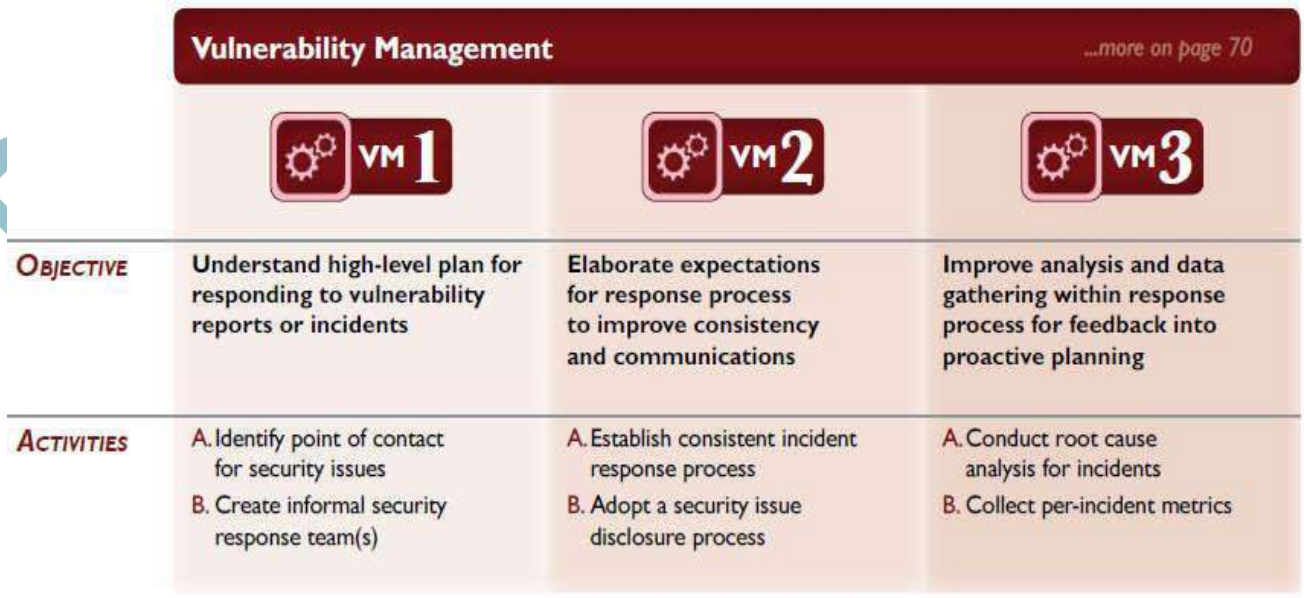
- OWASP Software Assurance Maturity Model (SAMM) **Deployment Phase:**
  - Environment Hardening
  - Vulnerability Management
  - Operational Enablement
- **Environment Hardening**:

- Focused on **building assurance for the runtime environment** that hosts the organization's software.
- Since secure operation of an application can be **deteriorated by problems in external components**, hardening this **underlying infrastructure directly improves the overall security posture** of the software



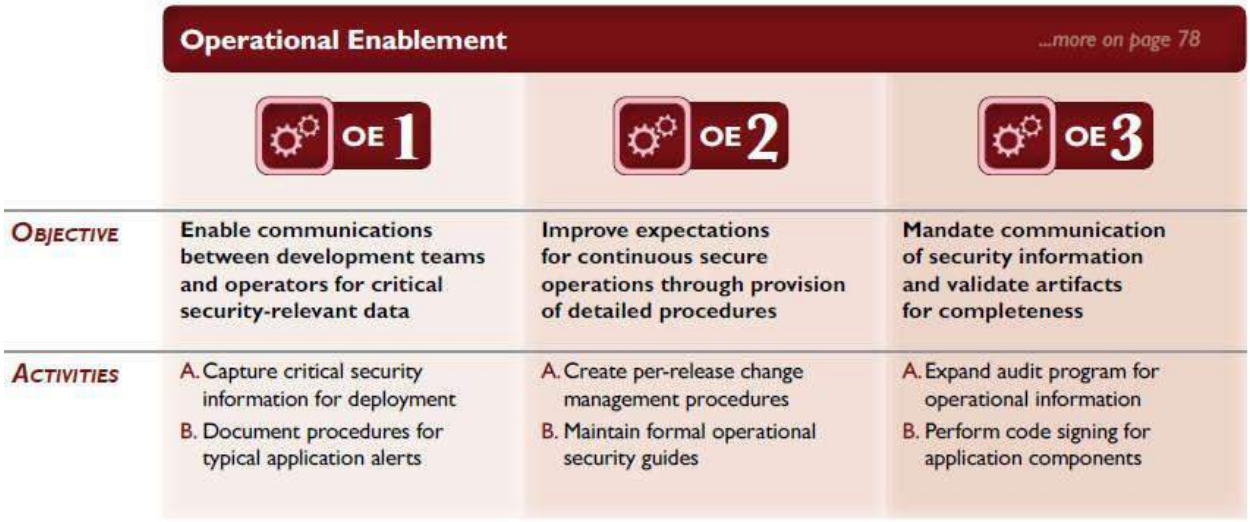
Environment Hardening	EH 1	EH 2	EH 3
OBJECTIVE	Understand baseline operational environment for applications and software components	Improve confidence in application operations by hardening the operating environment	Validate application health and status of operational environment against known best practices
ACTIVITIES	A. Maintain operational environment specification B. Identify and install critical security upgrades and patches	A. Establish routine patch management process B. Monitor baseline environment configuration status	A. Identify and deploy relevant operations protection tools B. Expand audit program for environment configuration

- **Vulnerability Management**:
  - Focused on the processes within an organization with respect to handling vulnerability reports and operational incidents.
  - By having these processes in place, an organization's projects will have consistent expectations and increased efficiency for handling these events, rather than chaotic and uninformed responses.



Vulnerability Management	VM 1	VM 2	VM 3
OBJECTIVE	Understand high-level plan for responding to vulnerability reports or incidents	Elaborate expectations for response process to improve consistency and communications	Improve analysis and data gathering within response process for feedback into proactive planning
ACTIVITIES	A. Identify point of contact for security issues B. Create informal security response team(s)	A. Establish consistent incident response process B. Adopt a security issue disclosure process	A. Conduct root cause analysis for incidents B. Collect per-incident metrics

- **Operational Enablement**:
  - Focused on gathering security critical information from the project teams building software and communicating it to the users and operators of the software.
  - Without this information, even the most securely designed software carries undue risks since important security characteristics and choices will not be known at a deployment site.

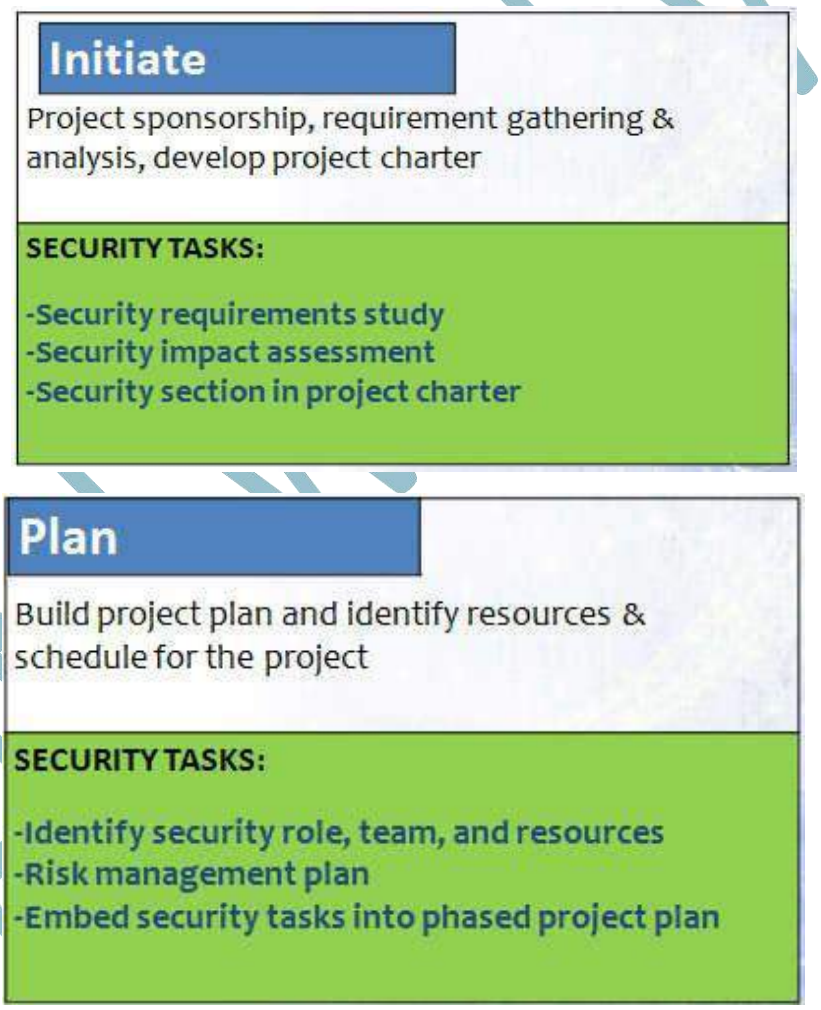


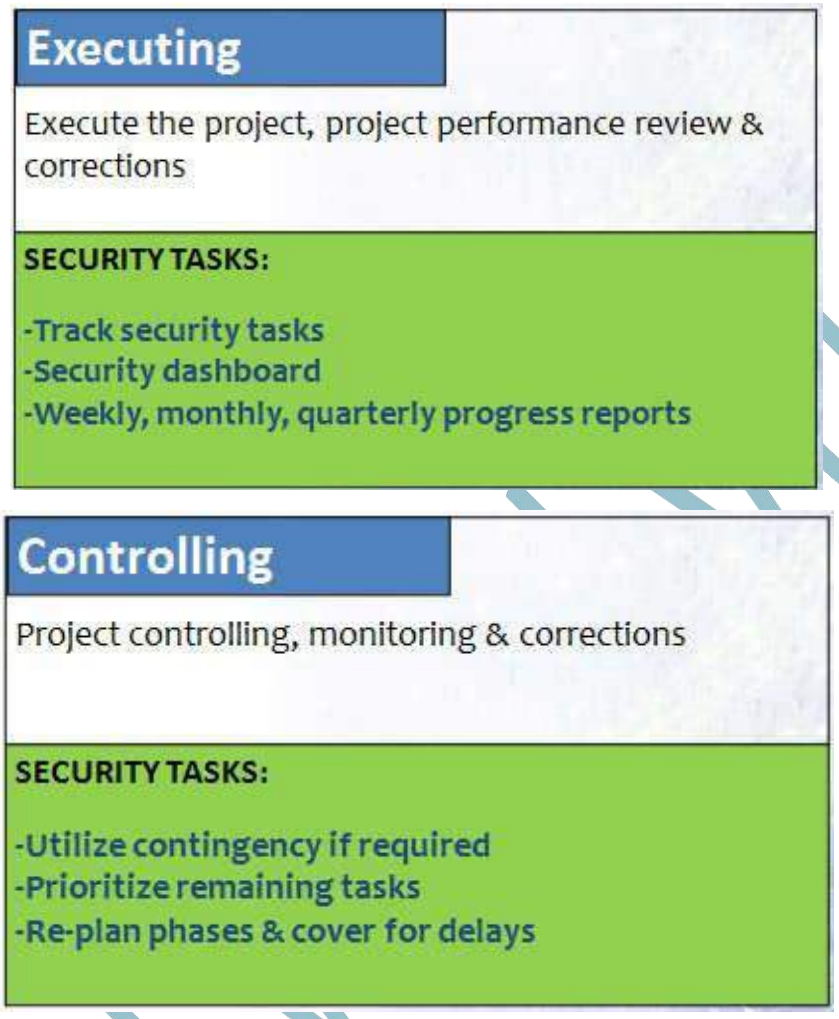
Operational Enablement			...more on page 78
	OE 1	OE 2	OE 3
OBJECTIVE	Enable communications between development teams and operators for critical security-relevant data	Improve expectations for continuous secure operations through provision of detailed procedures	Mandate communication of security information and validate artifacts for completeness
ACTIVITIES	A. Capture critical security information for deployment B. Document procedures for typical application alerts	A. Create per-release change management procedures B. Maintain formal operational security guides	A. Expand audit program for operational information B. Perform code signing for application components

- SAMM is an excellent model for software (security) assurance
- OWASP also has a multitude of additional materials, guidance, and tools for software and seb application security

Topic No 270: Embedding InfoSec Into Project Management

- PMIs five phases of project management:
  - Initiate
  - Plan
  - Executing
  - Controlling
  - Closing





- Senior management needs to ensure that security is integrated with IT project plans
- Sufficient security resources should be made available to manage the security aspects of projects

Topic No 271: How To Conduct Internal Security Assessment

- **What is an internal security assessment?**
  - An effort to assess the security posture, risks, or vulnerabilities for any project, service, application, or device
- **When is an internal security assessment required?**
  - Launch of a new IT project or service
  - When an incident has occurred
  - On change of leadership
  - Regulatory or compliance reqmts
- **Sequence of security assessment:**

1. Management approval or communication
2. Assign resources
3. Build plan, scope and objectives
4. Conduct assessment
5. Report findings & remediation measures

1. **Management approval or communication:**
   - Authority of the assessment
   - Cooperation from stakeholders
   - Determine & communicate timeline
   - Determine appropriate report format

2. **Assign resources:**
   - Assign information security resources with relevant experience
   - Identify respective resources for IT asset to be assessed
   - Hold initial meeting with respective stakeholder POC

3. **Build plan, scope & objectives**
   - Study IT asset & gather background security docs
   - Clear scope boundary
   - Clear objectives
   - Determine assessment method based on report format

- Build plan

4. **Conduct assessment:**
   - Conduct the necessary activities such as system walkthrough, vulnerability assessment, security testing, evaluation of security controls, review of process and documentation, etc

5.
   - Assimilate and analyze findings
   - Determine level of severity, risk and appropriate remediation
   - Tailor findings to report format & appropriate to forum
   - Share report

- **A few pointers:**
  - Security should not be reactive
  - Security transformation project should address security loopholes
  - Align the security assessment with benchmarks established already

Topic No 272: Different Types Of Security Assessments

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/greybox/ blackbox assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team
- **Vulnerability assessment:**
  - Technical assessment to yield as many vulnerabilities as possible in an environment along with severity and remediation priority information
  - **Best when** security maturity is low to medium, need a prioritized list of everything that's wrong, goal is to fix as many things as possible as efficiently as possible

- **Penetration test:**
  - A Penetration Test is a technical assessment designed to achieve a specific goal, e.g., to steal customer data, to gain domain administrator, or to modify sensitive salary information
  - Penetration Tests are for testing security that is assumed to be strong
  - No point in wasting the effort if hardening and vulnerability assessment have not been done
- **VA & PT difference:**
  - Vulnerability assessments look for security problems when you know/assume they exist, and penetration testing validates a configuration when you believe it to be secure
- **Audit:**
  - An audit can be technical and/or documentation-based, and focuses on how an existing configuration compares to a desired standard
  - Orgs use audits to demonstrate compliance
  - Importantly, compliance should not be used to demonstrate security
  - Compliant orgs more likely to be secure
  - Secure orgs are significantly more likely to be compliant (if checked), but compliant orgs should lay no claims to being secure just because they are in accordance with standard X or Y.
- **Lets look at the following in the next modules:**
  - Whitebox/greybox/ blackbox assessments
  - Risk assessment
  - Threat assessment
  - Bug bounty
  - Red team

Topic No 273: Types Of Security Assessments-Part 2

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/ greybox/ blackbox assessments
- Risk assessment
- Threat assessment
- Bug bounty
- Red team

TYPE OF ASSESSMENT	DESCRIPTION	BEST USED WHEN
	information available, such as network diagrams, source code, etc.	Best used with vulnerability assessments because you want to find as many issues as possible
GREYBOX	Tester has some information but not all	You want to give some information to the tester but not all
BLACKBOX	Tester is given no knowledge about the network – "attackers perspective"	Performing a penetration test

- **Risk assessment:**
  - Should involve determining what the current level of acceptable risk is, measuring the current risk level, and then determining what can be done to bring these two in line where there are mismatches. Risk Assessments commonly involve the rating of risks in two dimensions: probability, and impact.

- Umbrella term for determining what you have of value, how it can be attacked, what you would lose if those attacks were successful, and what should be done to address the issues.

- **Threat assessment:**
  - The driver for the assessment is to determine how many resources—if any—should be spent on addressing the issue in question.
  - A threat assessment is best used in situations where someone has made a claim around performing an attack in the future, or such a potential is uncovered somehow.

Topic No 274: Types Of Security Assessments-Part 3

- Vulnerability assessment
- Penetration test
- Audits
- Whitebox/greybox/ blackbox assessments
- Risk assessment
- Threat assessment
- **Bug bounty**
- **Red team**
- **Bug bounty:**
  - A Bug Bounty is a type of technical security assessment that leverages crowdsourcing to find vulnerabilities in a system. The central concept is simple: security testers, regardless of quality, have their own set of strengths, weaknesses, experiences, biases, & preferences, & these combine to yield different findings for the same system when tested by different people.
  - Best used when you have done multiple Vulnerability Assessments already and have already found the easy stuff. Bug Bounties excel at finding issues not found using other methods.
- **Red team assessment:**
  - "Red team" is: an independent group that challenges an organization to improve its (security) effectiveness
  - Services should be continuous rather than point-in-time
  - Best used when an org has covered the basics of strong vulnerability management and has at least some capability to detect and respond to malicious or suspicious behavior in the environment
- Note: the term red team is taken from the military maneuvers where a red team simulates attacks and a blue team takes evasive measures against those attacks

Topic No 275: Types Of Security Assessments-Part 4

TYPE	SUMMARY	OUTPUT
VA	Designed to find as many vulnerabilities as possible for the purpose of prioritizing remediation efforts	The output is a list of prioritized issues.
PT	Designed to determine whether an attacker can achieve specific goals when facing your current security posture, such as stealing sensitive data or other activities that would harm the org	Report stating whether the goals were achieved or not
Audit	Designed to determine how a given organization measures against a given standard. Audits, as a rule, do not test security directly, but rather test compliance with a standard.	List of areas that must be fixed in order to achieve compliance

TYPE	SUMMARY
White Box, Grey Box, Black Box Assess-ments	Measure of how much information is being provided to a security testing organization during an assessment. These can be internal, external, application-based, network-based, with or without exploitation, etc

TYPE	SUMMARY	OUTPUT
Risk Assess-ment	determining the most important risks facing a given organization for the purposes of ensuring that they are brought within acceptable levels for the business.	List of prioritized risks followed by recommen-dations.
Threat Assess-ment	Determining whether a given threat is worth spending limited resources on.	Recommendation of what—if any—amount of effort should be dedicated to the issue

TYPE	SUMMARY
Bug Bounties	Crowdsourcing for the discovery of vulnerabilities in a system. Utilizes large collection of independent researchers who all bring their own perspectives to the testing

Topic No 276: STAGES OF 3RD PARTY PENETRATION TEST

1. SYSTEM PORT SCANNING
2. IDENTIFICATION OF SYSTEM SERVICES
3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES
4. PENETRATION TESTING (SYSTEM EXPLOITATION)

1. SYSTEM PORT SCANNING

- Port scanning is one of the most important phases of a vulnerability assessment exercise prior to a penetration test.
- This will be the first tool used by an attacker once he has identified the IP address to be targeted.
- The key part here is to use a multiple of port-scanning tools in order to ensure the least false positives and the maximum information that can be gathered.

2. IDENTIFICATION OF SYSTEM SERVICES

- Once the open ports have been enumerated, it is important to determine the services that are keeping those ports open. - This is typically done by analyzing the banners thrown back when a default connection is made to the open port.
- The latest nmap version allows this to be done using the –sV switch.

3. IDENTIFICATION & VERIFICATION OF SYSTEM VULNERABILITIES

- During vulnerability identification, an assessor will perform several activities to detect exploitable weak points.

These activities include:

- Identify vulnerable services using service banners.
- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities

Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as SecurityFocus, CVE or CERT advisories.

- Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information).

- Enumerate discovered vulnerabilities.
- Estimate probable impact (classify vulnerabilities found).
- Identify attack paths and scenarios for exploitation.

4. PENETRATION TESTING (SYSTEM EXPLOITATION)

Following the approvals of individual attacks by Customer, the assessor tries to gain unauthorized access by circumventing the security measures in place and tries to reach as wide a level of access as possible.

This process will have the following steps:

- Find proof of concept code/tool
- Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and thoroughly tested, you can use it, otherwise test it in an isolated environment.
- Develop tools/scripts
- Under some circumstances it will be necessary (and cost effective) for assessors to create their own tools and scripts.
- Test proof of concept code/tool in an isolated environment
- Document findings

Topic No 277: Security Transformation: Failure?

- Let us examine the reasons for proposing a security transformation in the first place:
  - Information security almost one generation behind
  - Arduous to catch up with Information Security posture unless there is a "transformation"
- **Guaranteed failure:**

– Cosmetic commitment

– Not willing to invest in resources

– Deficient program structure

– Lack of effective project management

1. **Cosmetic Commitment:**

   – Lack of awareness & understanding

   – Short-term vision

   – Lack of priority

   – Poorly managed organization

2. **Not Willing To Invest In Resources:**

   – Deficient allocation of funds for Information Security Program

   – Not willing to allocate time for IT to perform security tasks

   – Loss-making organization

3. **Deficient Program Structure:**

   – Ineffective Information Security Management Committee (ISMC)

   – Not taking along other stakeholders

   – Inexperienced IT or security leadership

   – IT team not incentivized

4. **Lack Of Effective Project Management:**

   – Any project will fail without effective project management

   – Effective planning, execution, monitoring, and reporting

   – Experience & domain knowledge

- **Conclusion:**

- The Information Security Transformation requires a tremendous amount of hard work
- Not possible without commitment, right strategy, correct structure, and effective execution

Topic No 278: Benefits Of The Security Transformation

- Key Benefits:
  - Prevention of attacks
  - Prevention of fraud & pilferage
  - A reliable & robust IT setup
- Impact of attacks:
  - Loss of market goodwill
  - Loss of customer confidence
  - Regulatory fines, legal consequences
- Prevention Of Fraud & Pilferage:
  - An effective Information Security Program makes it harder to conduct fraud, abuse, or misuse without getting detected
  - Controls in business process
  - Audits
- A Reliable & Robust IT Setup:
  - Business continuity & DR
  - Redundancy
  - Backups
  - Capacity management
  - Change management

- Incident management

- Conclusion:
  - An effective Information Security Program (achieved through an Information Security Transformation) is essential wherever an IT setup exists
  - Not a luxury but an imperative

Topic No 279: Security Transformation Timeline

- Recommended timeline for security transformation project

- **Month 1: Planning**
  - Understand organization & security issues
  - Develop ISMC
  - Identify stakeholders for InfoSec Steering Committee
  - Identify assets for various phases
  - Project kickoff and awareness trainings

- **Months 2-3: Pilot (Phase 1)**
  - Perform hardening of key IT assets in test environment (Pilot)
  - Validate the hardening in the test environment
  - Prime IT & InfoSec teams for their roles
  - Vulnerability management pilot

- **Months 4-5 (Phase 2):**
  - Hardening of IT assets (minimum security baseline) identified for phase 2
  - Validation of hardening and moving the hardened IT assets to PROD environment through change management process

- **Months 6-7 (Phase 3):**
  - Hardening of IT assets (minimum security baseline) identified for phase 3
  - Validation of hardening and moving the hardened IT assets to PROD environment through change management process

- **Months 8-10 (Phase 4):**
  - Technical teams continue the IT assets hardening in phase 4
  - Raise vulnerability management program frequency to monthly
  - **Focus on governance (policies, SOPs, etc)**
- **Months 11-12 (Phase 5):**
  - ISO27001:2013 stage 1 and stage 2 certification
  - Stage 1 mostly documentation review
  - Stage 2 mostly implementation review

Topic No 280: Security Transformation Responsibility

- Responsibility for the security transformation is a balance between management & security team
- IT team led by the CIO plays an instrumental role in the success of the program

- **Management role:**
  - Commitment
  - Sets the tone at the top
  - Allocates resources
  - Assigns responsibility & roles
  - Conducts periodic performance review

- **Information Security Team:**
  - Builds an effective strategy & structure for the program
  - Identifies key players to enroll in ISMC
  - Ensures effective execution & project management
  - Conducts transparent reporting

- **IT Team:**
  - Mobilizes the resources for implementation of the security program
  - Ensures quality and process during the security transformation program
  - Resolves roadblocks in implementation

Conclusion:

- An effective Information Security Transformation can only be orchestrated through effective team work
- All parts of the organization have to play their due role to make the program a success

Topic No 281: Actions To Raise Management Support

- What can you do if your organizational management is not supporting for the Information Security Transformation Program?

a) Understand the organizational business requirements and potential impact
b) Understand regulations & sector best-practices
c) Evaluate the security posture
d) Assess the extent of work and resources required
e) Present your report

a. Understand the organizational business requirements & potential impact:

- Type of business/industry
- Business requirements
- Confidentiality, integrity, availability
- What can go wrong and impact?

b. Understand regulations and sector best-practices

- Financial industry (SBP)
- Telecoms & IT industry (PTA/MOITT)
- Oil & Gas (OGRA)
- Look at standards & best-practices (quality & security)

c. Evaluate the security posture

- Evaluate security posture against each of the four layers of Transformation Model
- Any recent incidents ?
- Org culture ?
- Quality and improvement emphasis ?

d. Assess the extent of work and resources required

- Size of organization and size of IT ?
- Extent of IT assets ?
- Internal software development ?
- Evaluate team size required for InfoSec and consultant option

e. Present your report

- Take key stakeholders on board
- Reach out to stakeholders before presentation
- The better researched and prepared you are, the better your chances to convince

Conclusion:

- Many of the problems associated with weak security posture are actually due to poor awareness
- Put yourself in the shoes of your audience and explain the need for a security program from their perspective
- Keep it high level

Topic No 282: Key Questions To Assess Security Posture

- What are the key questions that can be used to assess the security posture of the organization?

SN	QUESTION	PTS
1	DESIGNATED HEAD OF INFORMATION SECURITY ?	30
2	INFORMATION SECURITY POLICY (AVAILABLE ON PORTAL) ?	20
3	INTERNAL VULNERABILITY MANAGEMENT PROGRAM (INTERNAL TOOL WITH MIN QTR SCANS) ?	50
4	EXTERNAL PENETRATION TEST CONDUCTED MIN ONCE PER YEAR ?	50
5	IT ASSETS HARDENED WITH CIS/DISA OR OTHER INDUSTRY BEST-PRACTICE ?	100
6	ESTABLISHED INTERNAL PROCESSES FOR CHANGE MANAGEMENT, INCIDENT MANAGEMENT, CAPACITY PLANNING ?	25
7	IS INFOSEC TEAM SIZE MIN 15% OF IT TEAM ?	25
8	DO YOU HAVE OPERATIONAL DR SITE ?	50
9	ALL SYSTEMS HAVE LICENSED OS ?	50
10	IS ACTIVE DIRECTORY AND LICENSED AV RUNNING ON ALL WORKSTATIONS ?	50
11	DOES NETWORK PERFORM FILTERING FOR WEB, AND ANTI-SPAM AT EDGE ?	20
12	FILTER TRAFFIC AT DATA CENTER SWITCH BASED ON ACCESS LIST ?	20
13	EDGE FIREWALL AND DMZ PRESENT ?	20
14	REGULAR BACKUPS OFFSITE AND PERFORM DR DRILL ON 2X YEAR BASIS ?	20
15	DOES MANAGEMENT REVIEW INFOSEC ON A QUARTERLY BASIS ?	20
	TOTAL	500

SCORE RANGE	POSTURE	RECCOMENDED ACTIONS
LESS THAN 20%	SEVERE RISK	INFORMATION SECURITY TRANSFORMATION PROGRAM
20% TO 35%	HIGH RISK	INFORMATION SECURITY TRANSFORMATION PROGRAM
35% TO 50%	MEDIUM RISK	INFORMATION SECURITY TRANSFORMATION PROGRAM
50% TO 70%	FURTHER IMPROVEMENTS REQUIRED	THIRD-PARTY SECURITY REVIEW
70% TO 85%	SATISFACTORY	THIRD-PARTY SECURITY REVIEW
HIGHER THAN 85%	VERY GOOD!	GO FOR ISO@7001:2013 CERTIFICATION !

- By evaluating the security posture and comparing with a few other organizations (through a limited survey), the security posture can be portrayed in a quantitative manner
- The questions can be refined and customized for your organization

Topic No 283: Key Leadership Qualities Of InfoSec Head

- Lets examine the key leadership qualities of the Information Security Head or the key resource driving the Security Transformation Program
- Authenticity
- Candidness
- Fairness & fair play
- Team environment
- Recognizing talent and hard work
- Celebrating success!

- **Authenticity**
  - IT is complex
  - No one person "knows-it-all"
  - Communicate that each individual has limitations
  - Admit mistakes and failures
  - Give credit where it is due
- **Candidness:**
  - Call a spade a spade
  - Honesty and straight-talk
  - Hear feedback and give respect to views of everyone
- **Fairness & Fair Play:**
  - Promote performance and merit
  - Adjust players in the right positions based on their strengths
  - Coach and guide team to perform and achieve results
- **Team Environment:**
  - Discourage solo-flight and promote team consensus, team reviews, and team achievements
  - Single out and coach individuals playing turf tactics
- **Recognize Talent & Hard Work:**
  - Identify self-promotion versus talent combined with hard work
  - Encourage hard workers who are team players
- **Celebrate Success!**
  - Hold team celebrations
  - Recognize quiet workers and background workers as well
  - Promote team achievements