

# Unit 2

Planning and implementation of an IT  
Infrastructure Audit for compliance

## **Defining the scope for audit**

1. What is audit ?
2. Why to perform audit ? (banking, college, financial audit)

The scope for audit – what audit will cover and what it will not cover.

3. The scope can be formed on particular products or services, locations, departments, individual projects, time periods, and even specific processes.

## **Defining the scope for audit**

Let me give you some examples:

- The audit will cover the manufacture of product A and B, but not the manufacture of product C.
- The audit will cover head office plus the branches in New York, London, and Tokyo.
- The audit will cover the work period from January through to June inclusively.

Without an effective scope, both the auditor and the auditee are unsure of the boundaries of the audit and time is often wasted through checking and verifying information that is not required (out of scope).

## **Defining the scope for audit**

### **Audit scope V/s Audit criteria**

**Audit scope** includes the time period of the audit, documents that are involved, physical location, organizational unit, and all the activities and the processes that will be conducted. It is the idea that deals with the depth of the audit process and how deep the auditor will dig in to get the relevant information. It is the extent and the boundary of the audit.

Whereas **audit criteria** can be termed as the set of policies, requirements, and procedures that are required for a successful audit. It can also be defined as the principle standards abiding in which the audit will be conducted.

## **Defining the scope for audit**

### **Types of Audit**

- Compliance Audit – internal and regular standards.
- Construction audit – cost incurred in construction project.
- Financial Audit – Analyze financial statement of an organization.
- Information system Audit – identify issue in IT system.
- Investigative Audit – investigate about inappropriate action taken place.
- Operational Audit - evaluation of the operational activities.
- Tax Audit – find out how much tax is paid as an organization.

## **Identifying critical requirements (essential conditions) for the audit**

1. Establishing priority areas.
2. Identifying monitoring and continuous audit rules.
3. Determining the process' frequency.
4. Configuring continuous audit parameters.
5. Following up.
6. Communicating results.

## **Assessing IT security**

### **Why to perform IT Security Risk assesment ?**

- Reduction of Long-Term Costs
- Provides a Cybersecurity Risk Assessment Template for Future Assessments
- Better Organizational Knowledge
- Avoid Data Breaches
- Avoid Application Downtime.
- Data Loss

## **Assessing IT security**

### **How to perform IT Security Risk assesment ?**

You may want to start by auditing your data to answer the following questions:

What data do we collect?

How and where are we storing this data?

How do we protect and document the data?

How long do we keep data?

Who has access internally and externally to the data?

Is the place we are storing the data properly secured? Many breaches come from poorly configured S3 buckets, check your S3 permissions or someone else will.



## **Assessing IT security**

### **Steps to perform IT Security Risk assesment ?**

- 1.Determine Information Value
- 2.Identify and Prioritize Assets
- 3.Identify Cyber Threats
- 4.Identify Vulnerabilities
- 5.Analyze Controls and Implement New Controls
- 6.Calculate the Likelihood and Impact of Various Scenarios on a Per-Year Basis
- 7.Prioritize Risks Based on the Cost of Prevention Vs Information Value
- 8.Document Results from Risk Assessment Reports

## Obtaining Information (basics Methods to collect information)

| Methods                                   | Overall Purpose  | Advantages   | Challenges  |
|---|--|--|---|
| questionnaires,<br>surveys,<br>checklists | when need to<br>quickly and/or<br>easily get lots of<br>information from<br>people in a non<br>threatening way | <ul style="list-style-type: none"><li>-can complete<br/>anonymously</li><li>-inexpensive to<br/>administer</li><li>-easy to compare and<br/>analyze</li><li>-administer to many<br/>people</li><li>-can get lots of data</li><li>-many sample<br/>questionnaires already<br/>exist</li></ul> | <ul style="list-style-type: none"><li>-might not get careful<br/>feedback</li><li>-wording can bias<br/>client's responses</li><li>-are impersonal</li><li>-in surveys, may need<br/>sampling expert</li><li>- doesn't get full story</li></ul> |

## Obtaining Information (Methods)

| Methods              | Overall Purpose   | Advantages  | Challenges  |
|----------------------|---|---|---|
| interviews           | when want to fully understand someone's impressions or experiences, or learn more about their answers to questionnaires                       | <ul style="list-style-type: none"><li>-get full range and depth of information</li><li>-develops relationship with client</li><li>-can be flexible with client</li></ul>  | <ul style="list-style-type: none"><li>-can take much time</li><li>-can be hard to analyze and compare</li><li>-can be costly</li><li>-interviewer can bias client's responses</li></ul>   |
| documentation review | when want impression of how program operates without interrupting the program; is from review of applications, finances, memos, minutes, etc. | <ul style="list-style-type: none"><li>-get comprehensive and historical information</li><li>-doesn't interrupt program or client's routine in program</li><li>-information already exists</li><li>-few biases about information</li></ul> | <ul style="list-style-type: none"><li>-often takes much time</li><li>-info may be incomplete</li><li>-need to be quite clear about what looking for</li><li>-not flexible means to get data; data restricted to what already exists</li></ul> |

## Obtaining Information (Methods)

| Methods      | Overall Purpose  | Advantages  | Challenges   |
|--------------|--|---|--|
| observation  | to gather accurate information about how a program actually operates, particularly about processes                                       | -view operations of a program as they are actually occurring<br>-can adapt to events as they occur                          | -can be hard to analyze responses<br>-need good facilitator for safety and closure<br>-difficult to schedule 6-8 people together |
| case studies | to fully understand or depict client's experiences in a program, and conduct comprehensive examination through cross comparison of cases | -fully depicts client's experience in program input, process and results<br>-powerful means to portray program to outsiders | -usually quite time consuming to collect, organize and describe<br>-represents depth of information, rather than breadth         |

## **Factors affecting Information collection**

- .Accuracy : information gathered is accurate (google search..)
- .Precision : information gathered is precise
- .Bias : The question influences responses in favour of, or against the topic of
- .Use of language : language constrains (konkani, hindi, english, others)
- .Timing : time constrains
- .Privacy : private data
- .Cultural sensitivity : cultural offensiveness.
- .Ethics : human ethics.
- .Cost : involves money
- .Time : time spent in data collection
- .Age : age influences data collection
- .Presentation : data presented in wrong manner affects collection.

## **Documentation and Resources (The Importance of Audit Documentation)**

What is documentation ?

A document is something that has evidence or information that makes it an object of interest.

Therefore, documentation is an act of recording the information that is needed for the audit.

In the world of auditing, documentation is done to have supporting papers for the audit.

## **Documentation and Resources (The Importance of Audit Documentation)**

### **Why is Audit Documentation Important?**

- .There is an assurance that the audit that was performed was in accordance with the standards
- .This can help assist the auditors that will be hired in the future, in some cases
- .The data that has been recorded can help in ensuring and encouraging that

## **Documentation and Resources (The Importance of Audit Documentation)**

4 strategies for efficient, effective audit documentation

- .take a smart approach to planning
- .embrace standardization
- .document now, save time later
- .be prepared for what's ahead



## **Documentation and Resources (The Importance of Audit Documentation)**

### Resources used for documentation

.Dropbox paper

.Whatfix

.ProProfs

.Tettra

.GitHub

.Read the Docs

.Typora

Tettra software

Bit.ai

Dropbox Paper

Tallyfy

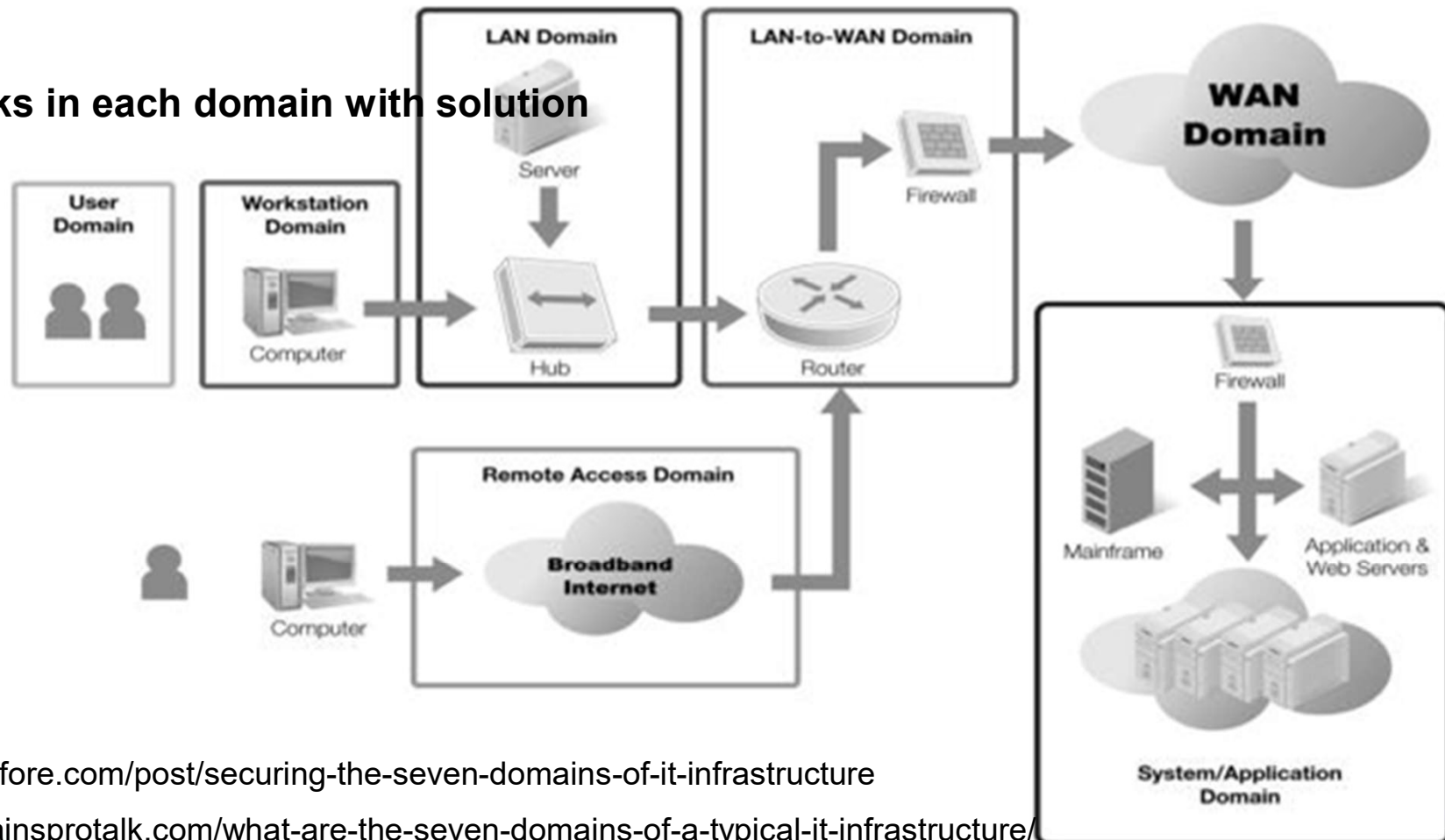
Apiary

MarkdownPad

Doxygen

## Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure

Identify risks in each domain with solution



<https://www.cyberfore.com/post/securing-the-seven-domains-of-it-infrastructure>

<https://www.domainsprotalk.com/what-are-the-seven-domains-of-a-typical-it-infrastructure/>

## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **User Domain**

- .almost 90% of cyber-attacks caused by human error or behavior , this domain needs strong scrutiny.
- .Following risks have been identified:
  - .Employees that fail to lock their computers when getting up from their desks.
  - .Employees that leave sensitive company information on their desks.
  - .Limited IT security knowledge by employees can lead to the introduction of malware and social engineering
  - .Employee negligence from a lack of policy can lead to legal ramifications for the business.

## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **Workstation Domain**

The Workstation Domain includes any computing devices used by end-users and represents how the users

- .Old operating systems represent a huge vulnerability. They are beyond their end-of-life and are not maintained.
- .Older and outdated hardware is vulnerable to hackers and data loss through outdated firmware exploits and bugs.
- .Known remote access vulnerabilities within older OS's can allow hackers to take over the workstation and access sensitive data.
- .Old hard drives can lead to failure and the data loss of critical business information.

## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **LAN Domain**

The LAN Domain includes all the equipment that makes up the local area network, including switches, hubs,

- Flat network designs lack security.
- IT Employees may lack the experience, or the time, in designing and maintaining a secure network.
- Lack of security policy governing the network.

## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **LAN-to-WAN Domain**

The LAN-to-WAN Domain is where the corporate LAN connects to the Internet (in this case, the WAN). The

- .No firewall is present, only a simple modem.
- .Lack of any defensive perimeter controls.
- .Lack of Intrusion Detection/Intrusion Prevention.

## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **WAN Domain**

The WAN Domain is represented by the Internet and stands for wide area network. All outside entities are n

.A lack of security policy and trained employees means multiple vulnerabilities may exist at the perimeter w

.Lack of firewalls and possibly improperly configured modem at the perimeter could introduce many possibl

## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **Remote Access Domain**

The Remote Access Domain is represented by any employee, vendor, or contractor that works in the field or remotely.

- Weak passwords can lead to unauthorized entry into the network from external locations.

- Weak Group Policy on Domain Controller which does not enforce account lockouts, complex passwords, or other security measures.

- Improper set up of VPN, FTP, or other remote access protocol.



## **Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure**

### **System/Application Domain**

The System/Application Domain includes all system and application software-related issues. The software

- Unpatched operating systems and software existing on the network.
- End-users lack of security mindedness and unrestricted workstation access can lead to additional unsupport
- An email that is not scanned for viruses.
- Employees that are not trained in social engineering schemes can unwittingly open infected files.
- Lack of antimalware/antivirus software to protect company assets.

## **Identifying and Testing Monitoring Requirements**

### **What is infrastructure monitoring?**

Infrastructure monitoring is the process of collecting and analyzing data from IT infrastructure, s

- The ability to optimize business requirements and user experience
- The flexibility and scalability to ingest data from a variety of sources and to handle planned and
- The ability to detect and alert on outages, resource utilization, and performance degradations t
- Pinpoint root causes to determine precisely where a problem originates in the infrastructure or
- The ability to drill down into specific faulty infrastructure components and trigger remediation

**Identifying and Testing Monitoring Requirements**

**Challenges of infrastructure monitoring in cloud environments**

## **Identifying and Testing Monitoring Requirements**

**What are the benefits of infrastructure monitoring?**

## Identifying and Testing Monitoring Requirements

### What data to use while monitoring IT infrastructure ?

- .Metrics:** Quantitative data is especially useful for creating visualizations and identifying patterns in performance over time
- .Event logs:** Every system and service generates event logs, which can give you insights into what's happening and aid in troubleshooting
- .Distributed traces:** For better insight into how various aspects of your environment interact with one another, capture distributed traces
- .Metadata:** Additional information, such as topology details, name spaces, and priority data, will help you understand the system
- .UX data:** A view into how users are experiencing your site or applications is one of the most important dimensions to understand
- .Open-source telemetry:** There are many open-source options designed to help you achieve better observability across your infrastructure
- .Cloud integrations:** Modern infrastructure includes cloud infrastructure, which is why cloud integrations, such as CloudWatch, are essential

## Identifying and Testing Monitoring Requirements

### Infrastructure monitoring best practices

- .Leverage automation:** Augment your capabilities with infrastructure monitoring tools that feature automation.
- .Configure comprehensive alerts:** When your alerts are specific, they're less likely to result in false positives.
- .Prioritize alerts:** Organize and prioritize notifications so you don't miss the most important alerts.
- .Create role-specific dashboards:** Set up dashboards for your ITOps teams, your security teams, and business units.
- .Do a test run:** Schedule a test run and make sure everything is running according to plan.
- .Regularly review metrics:** As your business goals change and your infrastructure evolves, review them accordingly.
- .Tap your vendor's expertise:** Struggling to fine-tune or optimize your infrastructure monitoring as your organization grows?

## **What Are Controls and Why Are They Important?**

Internal controls are procedures and processes put into place by a company to prevent

**The core purposes of internal controls are to:**

- .Explain the process in which internal controls are carried out
- .Identify risks
- .Mitigate risks
- .Control the sharing of information
- .Evaluate effectiveness of internal controls

## **Why Are They (controls) Important?**

- .It establishes the processes
- .It improves process performance
- .It improves operational efficiency
- .It keeps duties separated
- .It mitigates business risk
- .It organizes information
- .It produces timely financial statements
- .It reduces errors
- .It improves accountability
- .It stabilizes operations
- .It reduces audit fees

**Security controls are divided**

**a. goal based**

**b. implementation based**



## Goal based- Security Controls

| TYPES OF SECURITY CONTROLS | CONTROL FUNCTIONS       |  |  |   |
|----------------------------|-------------------------|--|--|---|
|                            |                         | PREVENTATIVE   | DETECTIVE  | CORRECTIVE  |
|                            | PHYSICAL CONTROLS       | <ul style="list-style-type: none"><li>• Fences</li><li>• Gates</li><li>• Locks</li></ul>   | <ul style="list-style-type: none"><li>• CCTV</li><li>• Surveillance Cameras</li></ul>                                | <ul style="list-style-type: none"><li>• Repair physical damage</li><li>• Re-issue access cards</li></ul>                        |
|                            | TECHNICAL CONTROLS      | <ul style="list-style-type: none"><li>• Firewall</li><li>• IPS</li><li>• MFA</li><li>• Antivirus</li></ul>                                       | <ul style="list-style-type: none"><li>• IDS</li><li>• Honeypots</li></ul>  | <ul style="list-style-type: none"><li>• Vulnerability patching</li><li>• Reboot a system</li><li>• Quarantine a virus</li></ul> |
|                            | ADMINISTRATIVE CONTROLS | <ul style="list-style-type: none"><li>• Hiring &amp; termination policies</li><li>• Separation of duties</li><li>• Data classification</li></ul> | <ul style="list-style-type: none"><li>• Review access rights</li><li>• Audit logs and unauthorized changes</li></ul> | <ul style="list-style-type: none"><li>• Implement a business continuity plan</li><li>• Have an incident response plan</li></ul> |

## **Goal based- Security Controls**

The overall purpose of implementing security controls as previously mentioned

- .Preventive controls- attempt to prevent an incident from occurring.
- .Detective controls - attempt to detect incidents after they have occurred.
- .Corrective controls - attempt to reverse the impact of an incident.
- .Deterrent controls - attempt to discourage individuals from causing an incident.
- .Compensating controls - are alternative controls used when a primary control

## **Implementation based- Security Controls**

There are several types of security controls that can be **implemented** t

**Physical security controls** include such things as data center perimet

## **Implementation based- Security Controls**

**Digital security controls** include such things as usernames and passwords.

**Cybersecurity controls** include anything specifically designed to prevent, detect, and respond to cyber threats.

**Cloud security controls** include measures you take in cooperation with your cloud provider to protect your data and applications in the cloud.

# **The Security Control Formulation and Development Process**

Design & Development of security control:

## **Why Security Controls?**

Imagine that you need to secure your home. Ask yourself,

- Why am I securing the home?Very likely, it is because you perceive some threat
- What are the threats to your home? Break-in, theft of valuables, losing your home
- What happens if the threat materializes? i.e., What is the risk?
- What are the first five steps you are likely to take to secure your home to manage

## **The Security Control Formulation and Development Process**

### **The First 5 Steps You Might Take To Secure Your Home**

- 1) Take stock of your household
- 2) Protect the periphery
- 3) Restrict further access
- 4) Recovery plan if the threat becomes real.
- 5) Educate every member of the household

# The Security Control Formulation and Development Process

## Apply This Thinking To Your IT Security.

- 1) **Take stock** – Get to know the expanse of your Information Systems. Take Inventory of your hardware and software.
- 2) **Protect your periphery** – List your networks and protect all entry and exit points. (Systems and Network Security)
- 3) **Restrict access** – Implement strong passwords, encryption, and role-based access control (identity and access management).
- 4) **Prepare for the eventuality** – Have a backup and recovery plan that is well documented and, more importantly, tested.
- 5) **Awareness and Training** – Make sure that each employee/contractor knows what steps are in place for security.

# **The Security Control Formulation and Development Process**

Examples of security controls

Reference : <https://simplicable.com/new/it-security-controls>



## **The Security Control Development Process /Life cycle**

Microsoft security development life-cycle(SDL)

<https://www.microsoft.com/en-us/securityengineering/sdl/practices>

# **The Security Control Formulation and Development Process**

<https://www.sciencedirect.com/science/article/abs/pii/S0016003221004>

## **Control Implementation through Security Architecture Design,**

Security architecture - is defined as the architectural design that includes

# Control Implementation through Security Architecture Design,

