Information Security

Policies, Procedures & Security Baselines

Parthasarathy Muthukrishnan

08-10-2022

Objective

- What is Policy, Procedures and Security Baselines ?
- Why are they required for the organization ?
- How can the help the organization ?
- How to select Information Security Governance as a career path ?

Information Security Policy (To Do)

- Directive
- High Level statement
- Outlines security Goals
- Adherence is Mandatory
- Clear and simple
- Board shall approve the policies

Examples,

Acceptable use policy

Data Classification

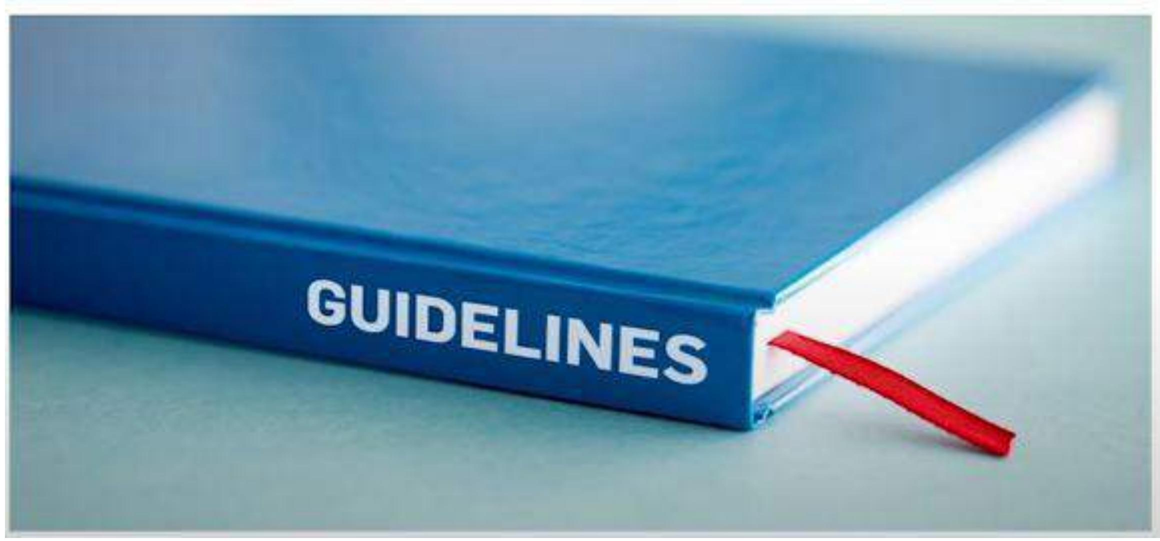
Information Security Procedure (How to do)

- Mandatory step by step instruction to complete a process or task.
- Like a tutorial – very detailed
- Produce repeatable result.
- Aids –Someone who is new to role.
- Format of SOP will be defined by the organization.

Document Owner Responsibility

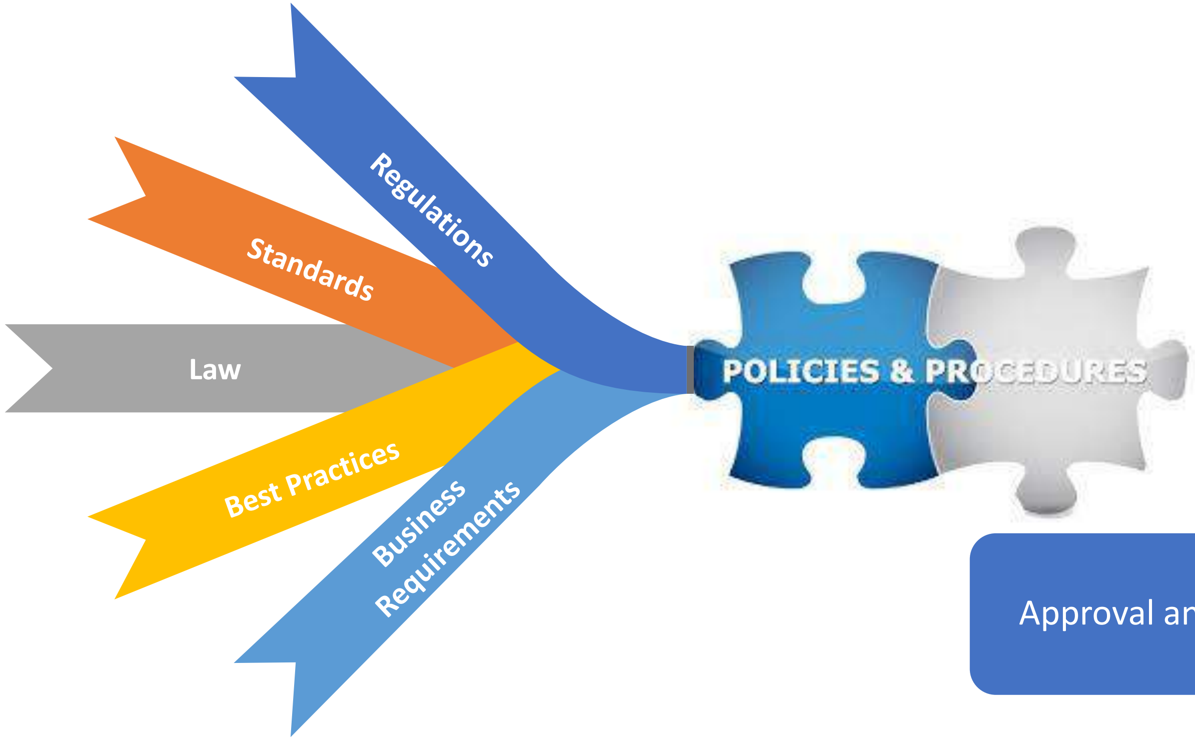
- ➢ Responsible – Circulate and obtain approval from all stakeholder.
- ➢ Maintain editable version of document.
- ➢ Provide training for effective implementation of SOP
- ➢ Ongoing Monitoring and periodic review.

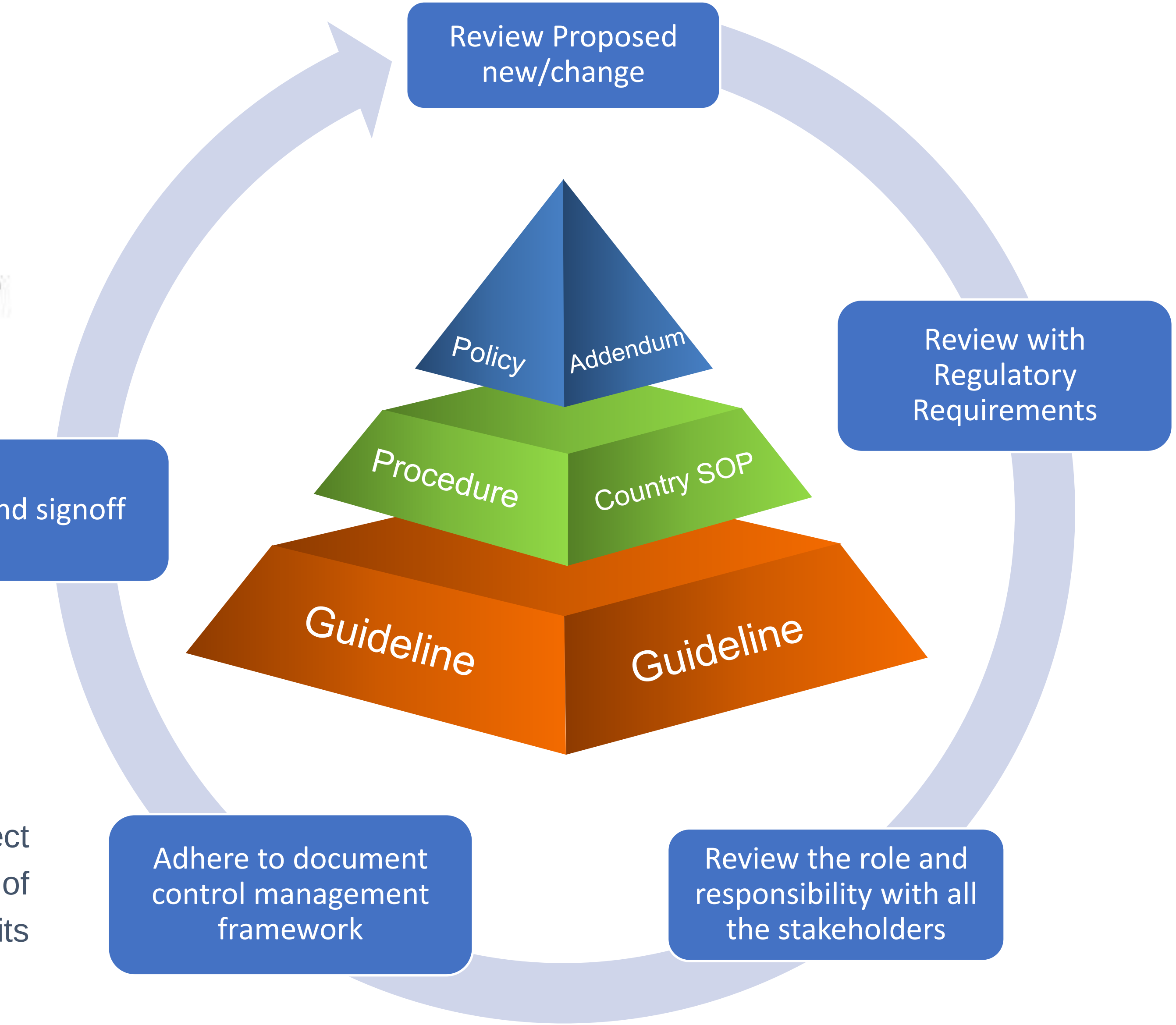
Guideline (Guide to do)



- Recommendations –Outline best practice
- Suggestions - Not mandatory
- Not required – Help employees follow the rule
- User friendly - Screenshots and diagrams can be included.
- Avoid word like shall, will or must

Policy & Procedure

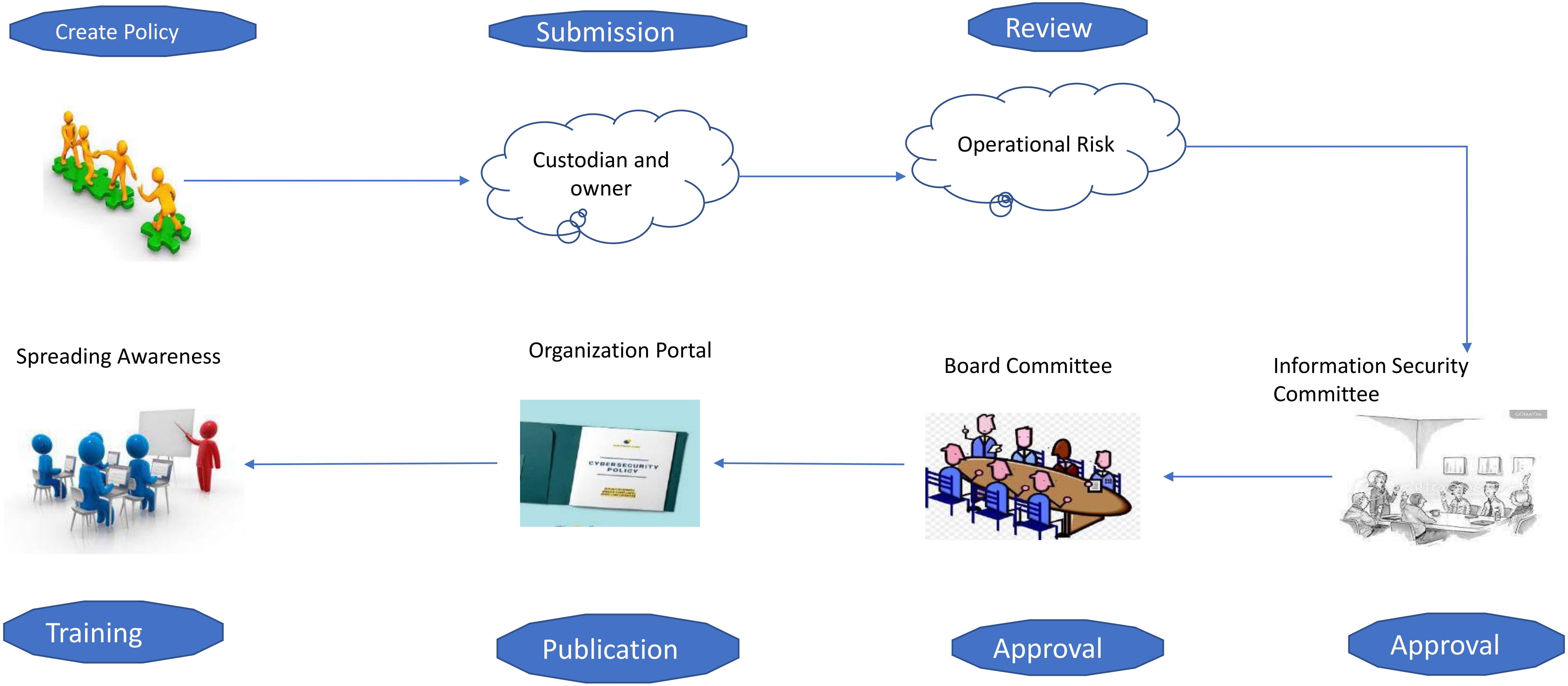



Review Proposed new/change
Review with Regulatory Requirements
Review the role and responsibility with all the stakeholders
Adhere to document control management framework
Approval and signoff
Policy
Addendum
Procedure
Country SOP
Guideline
Guideline

Purpose

Information Security policies, procedures are defined to protect confidentiality, maintain integrity, and ensure availability of information stored, processed and transmitted through its information systems

Policy Management Lifecycle



Create Policy

Submission

Custodian and owner

Review

Operational Risk

Information Security Committee

Approval

Board Committee

Approval

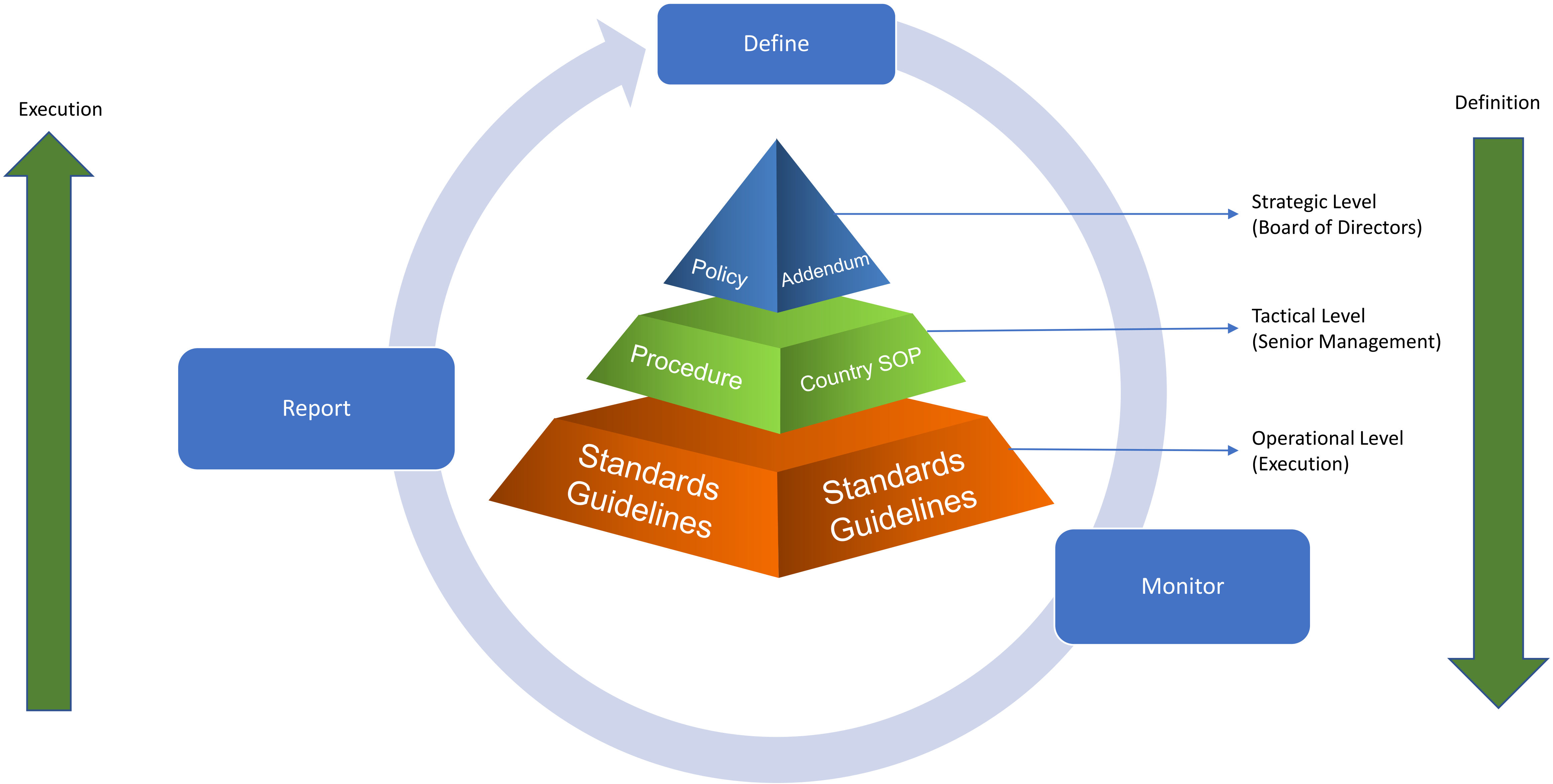
Organization Portal

Publication

Spreading Awareness

Training

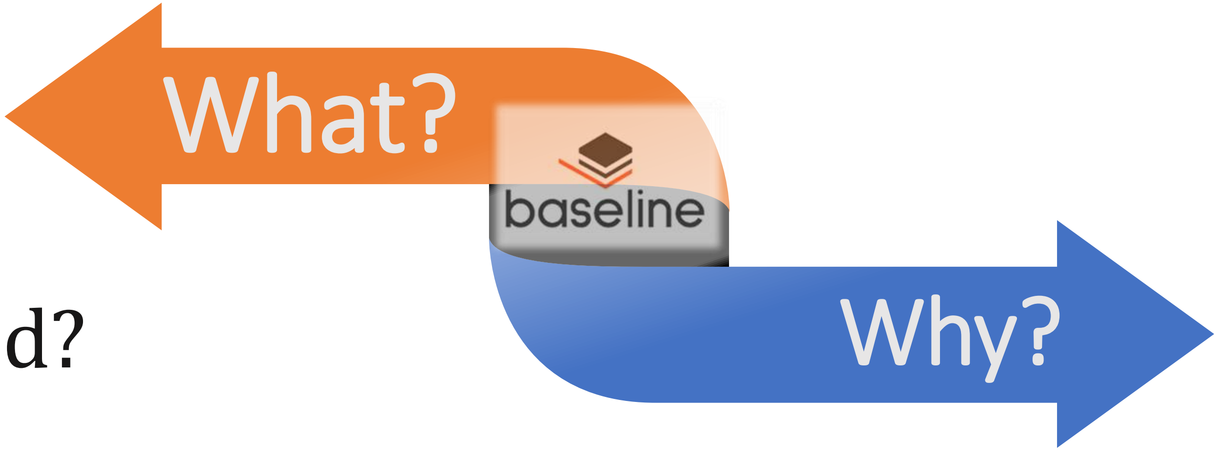
Policy Governance Framework



Security Baseline

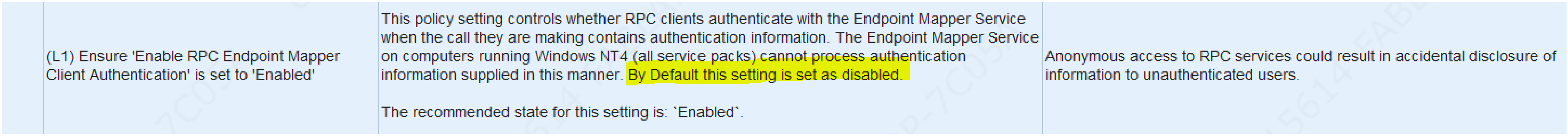
What is MSB?

It’s a bare minimum-security baseline standards
(hardening guide) to be applied on Various technologies
(OS, Database, Security Devices, Network devices,
storage, etc.)



Why is MSB needed?

The basic purpose of implementing MSB
(Hardening Guide) is to primarily it is to minimize the risk of inherent vulnerabilities due to vendor default configurations.



	(L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. By Default this setting is set as disabled. The recommended state for this setting is: `Enabled`.	Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

Can Baseline help improve security ?

PrintNightmare – Vulnerability

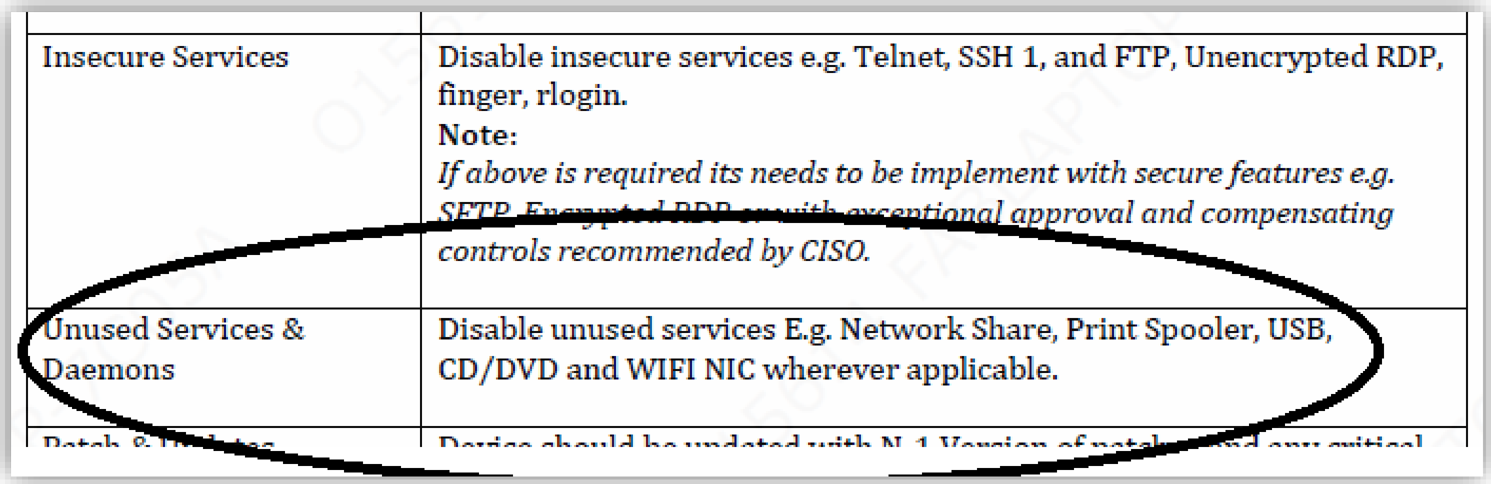
CVE-2021-34527

An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data;
or create new accounts with full user rights.

KB5005010

Mandates administrators to disable the Windows Print spooler service in Domain Controllers and systems that do not print.
Additionally, administrators should employ the following best practice from Microsoft's how-to guides

How to mitigate Print Spooler Print Nightmare vulnerability on Windows 10 | Windows Central



Insecure Services	Disable insecure services e.g. Telnet, SSH 1, and FTP, Unencrypted RDP, finger, rlogin. **Note:** *If above is required its needs to be implement with secure features e.g. SFTP, Encrypted RDP or with exceptional approval and compensating controls recommended by CISO.*
Unused Services & Daemons	Disable unused services E.g. Network Share, Print Spooler, USB, CD/DVD and WIFI NIC wherever applicable.
Patch & Updates	Device should be updated with N-1 Version of patch and any critical

Security Baseline

Who can mandate MSB ?

France: -
- European Central Bank - TARGET 2 Payment Standard (29 January 2021)

Hong Kong:-
- HKMA TM-G-1

India:-
- RBI Cyber Security Framework

KSA:-
- SAMA- Cyber Security

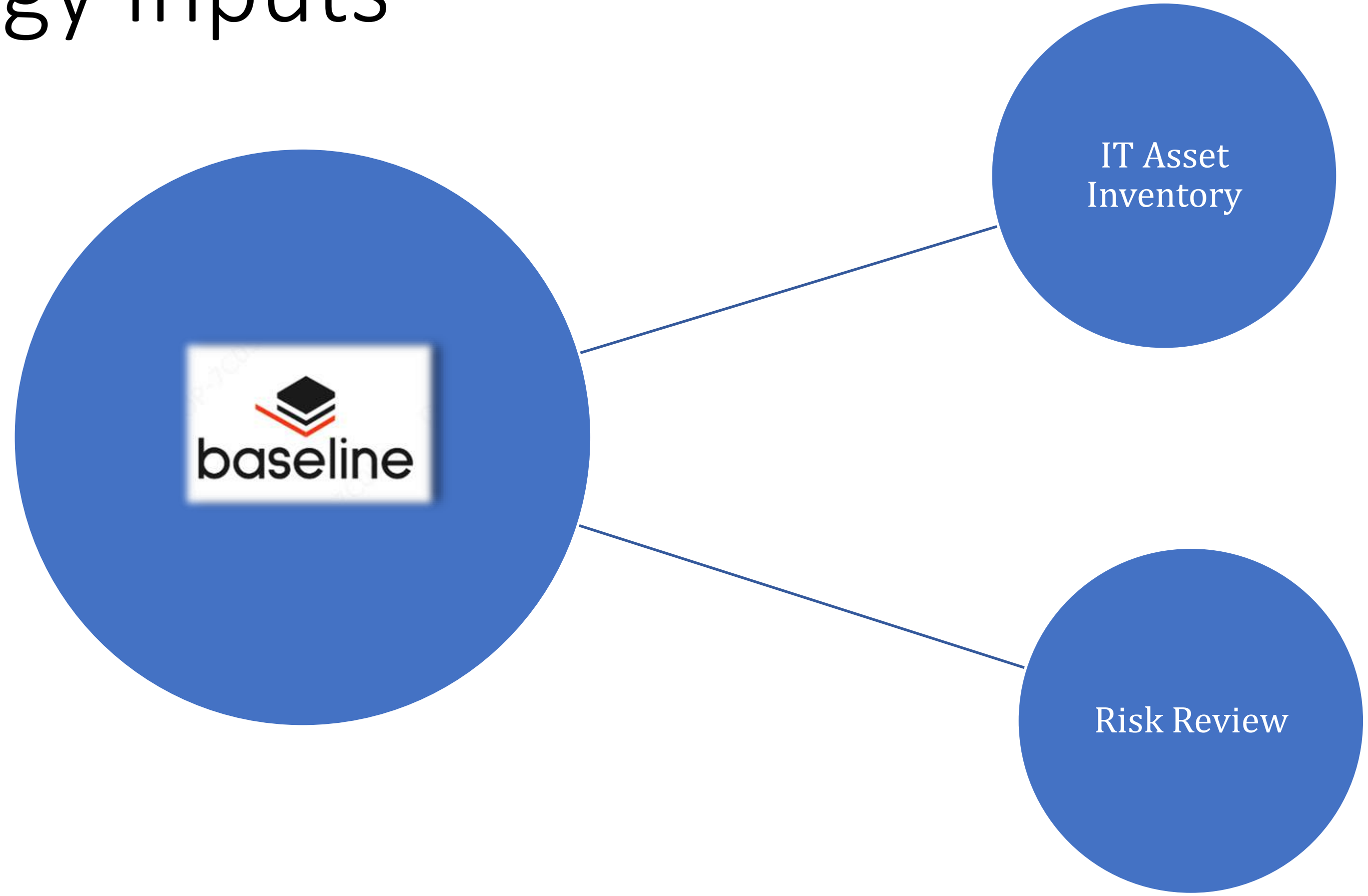
Kuwait:-
- Cyber Crisis Management Strategy and plan

Oman:-
- BM 1136 16062015 Security of Electronic Banking System

Singapore:-
- MAS - Technology Risk Management Guidelines

USA:-
- NIST SP 800-53 (Revision 4)
- FFIEC Information Technology Examination Handbook -Information Security

Technology Inputs



baseline

IT Asset Inventory

Risk Review

Security Baseline

Technologies

- Operating system
  - Windows
  - Red hat
  - Solaris
  - Centos

- Webservers
  - Apache
  - IIS
  - IBM WebSphere

- Database
  - MS SQL
  - Oracle DB
  - Mongo DB
  - Sybase
  - MySql DB

Security Baseline

Technologies

- Network
  - Cisco Switch
  - HP Switch
  - Wireless Controllers
  - Storage

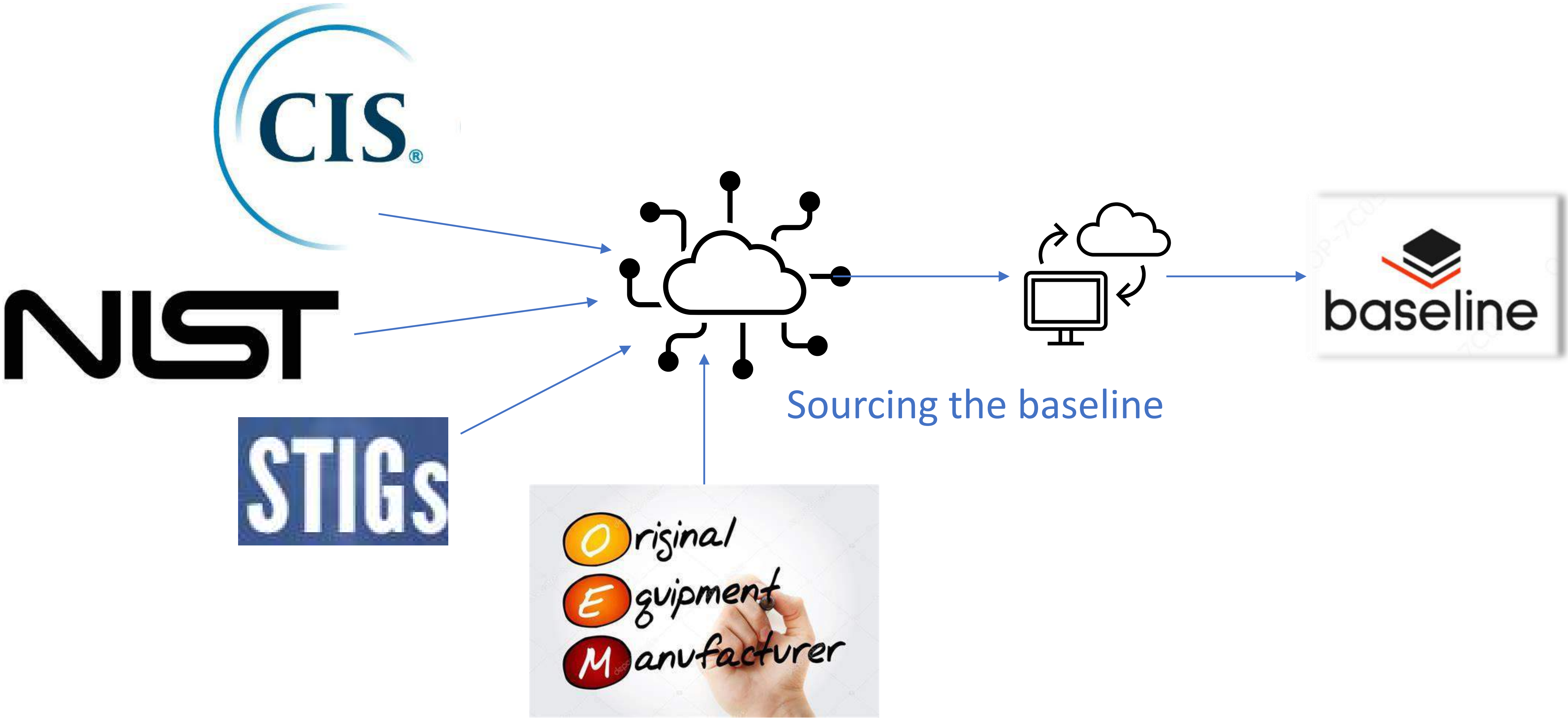
- End Point Application
  - Anti Virus
  - Internet Browsers
  - Citrix

- Network security
  - Firewall Devices
  - IPS
  - WAF
  - VPN
  - Proxy Devices
  - Mail Gateway
  - NAC

Secure Email Gateway

Security Baseline

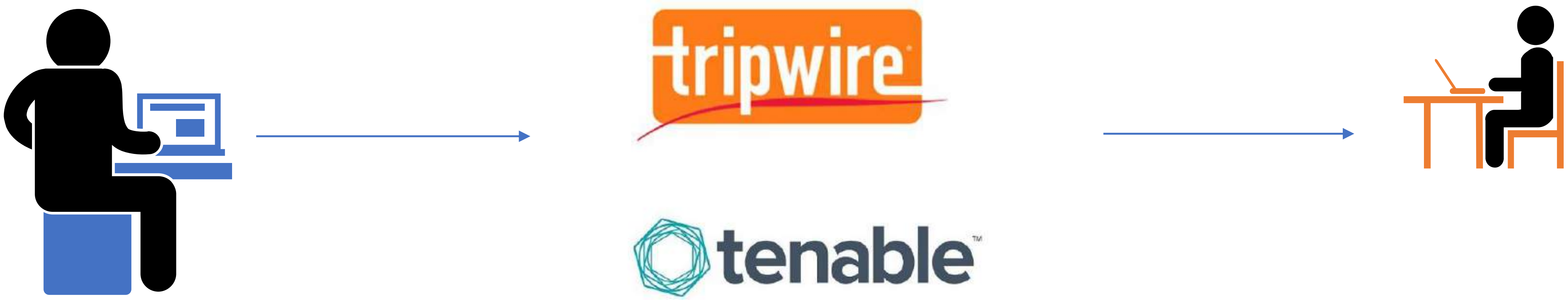
Who provides Baseline ?



Sourcing the baseline

Security Baseline

Baseline Compliance Process



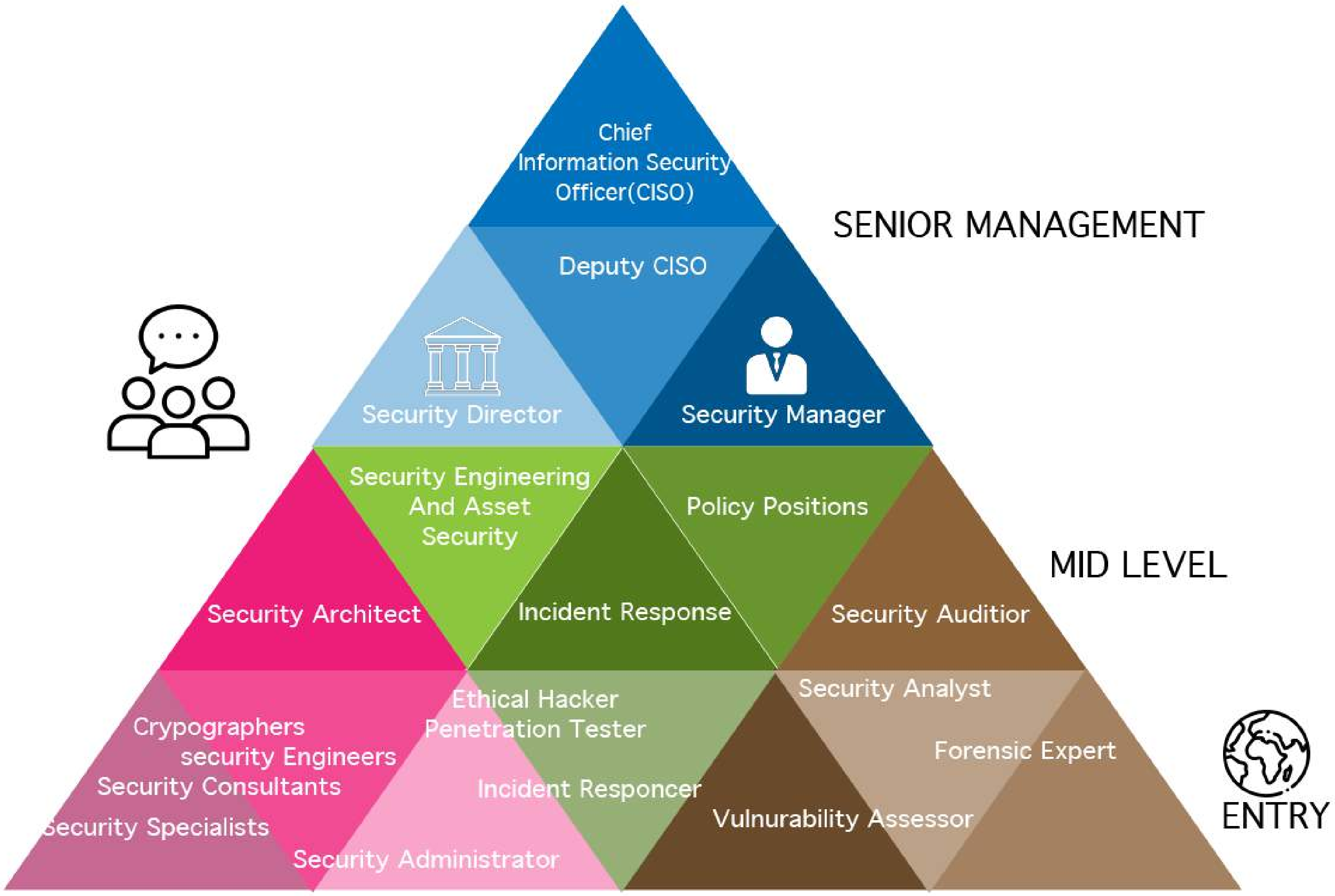
Draft Baseline

Verify Baseline compliance

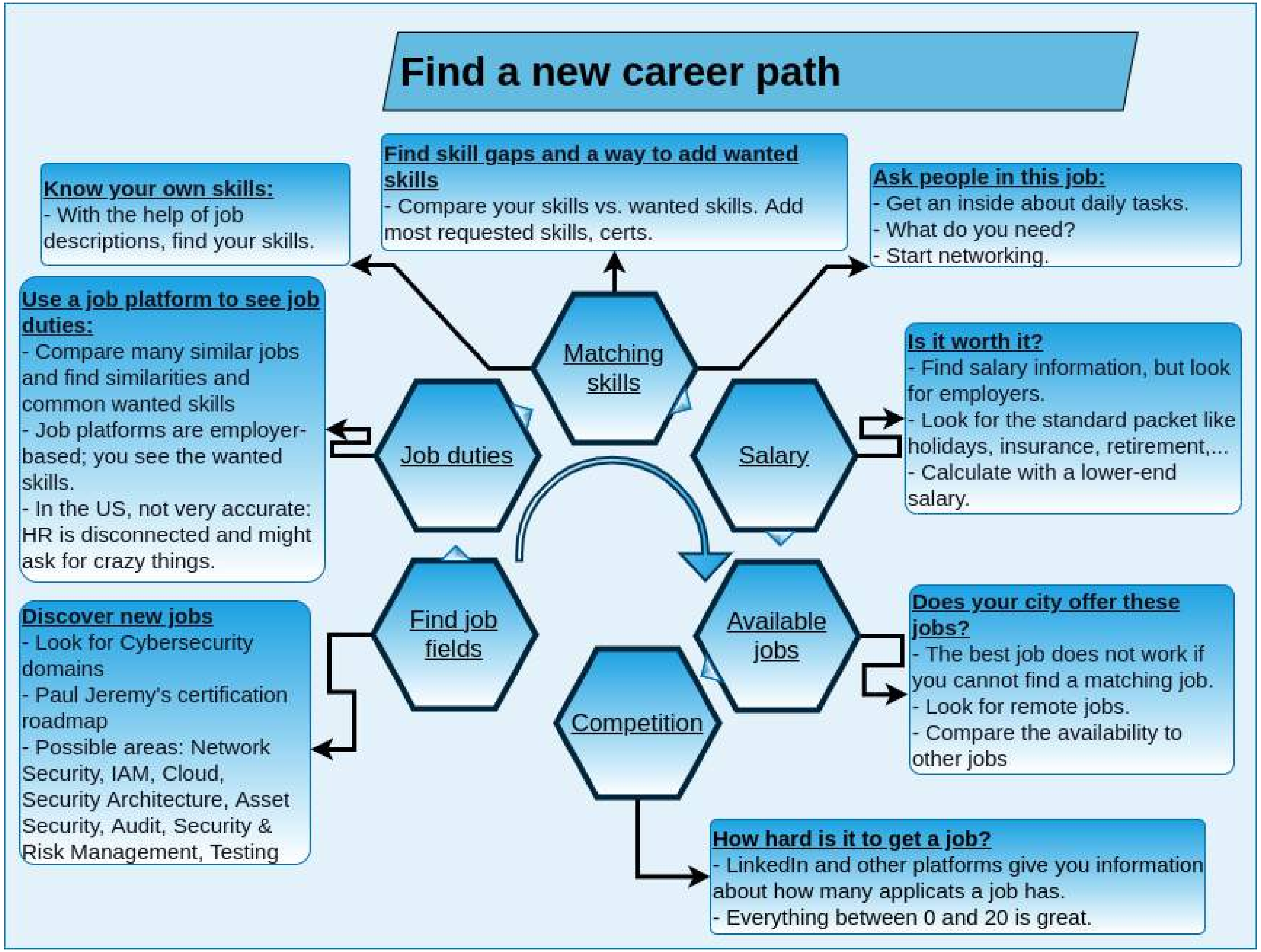
Report Baseline Compliance

Information Security as a Career

Information Security Career Path



Selecting the Career Path ?



Find a new career path

Find skill gaps and a way to add wanted skills
- Compare your skills vs. wanted skills. Add most requested skills, certs.

Know your own skills:
- With the help of job descriptions, find your skills.

Ask people in this job:
- Get an inside about daily tasks.
- What do you need?
- Start networking.

Use a job platform to see job duties:
- Compare many similar jobs and find similarities and common wanted skills
- Job platforms are employer-based; you see the wanted skills.
- In the US, not very accurate: HR is disconnected and might ask for crazy things.

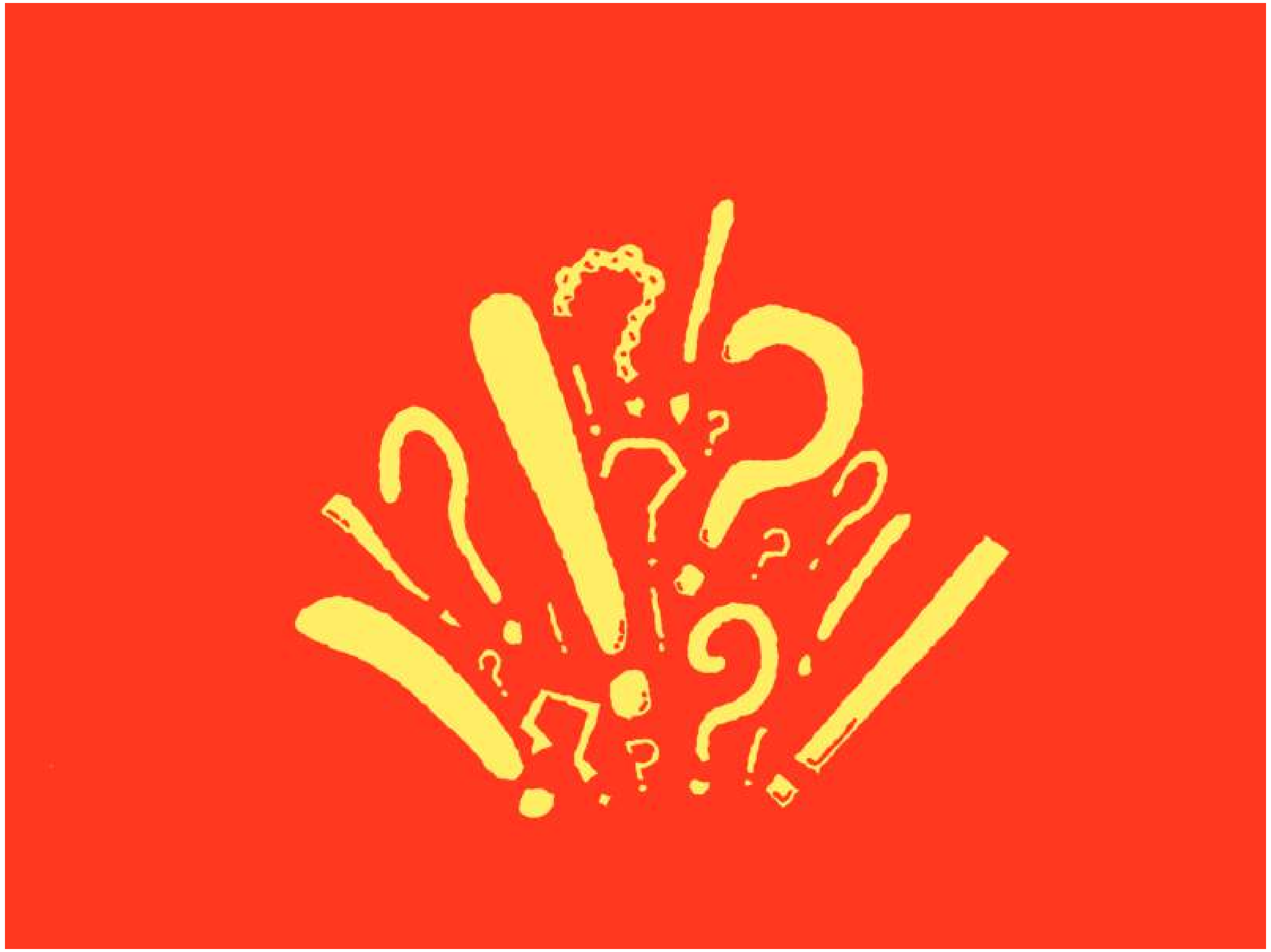
Is it worth it?
- Find salary information, but look for employers.
- Look for the standard packet like holidays, insurance, retirement,...
- Calculate with a lower-end salary.

Discover new jobs
- Look for Cybersecurity domains
- Paul Jeremy's certification roadmap
- Possible areas: Network Security, IAM, Cloud, Security Architecture, Asset Security, Audit, Security & Risk Management, Testing

Does your city offer these jobs?
- The best job does not work if you cannot find a matching job.
- Look for remote jobs.
- Compare the availability to other jobs

How hard is it to get a job?
- LinkedIn and other platforms give you information about how many applicats a job has.
- Everything between 0 and 20 is great.

Questions



Thank you