



Welcome

***“Cyber security is a self defense system. Cyber security is not a technology. It’s an attitude.”***

# Standards vs Hackers and Lawmakers



**Michael Petrov CEO**





# Agenda of the day 2

- **Threat Modeling Walkthrough**
- **What Cybersecurity Standards are and what they are not**
- **Comparison**
- **Selecting the right framework**
- **Zero trust**
- **Information classification**
- **Risks – general facts**
- **2 Ways of thinking about risk**
- **Risk -> Controls / Controls -> Risk**
- **Common approach**
- **Implementation spiral**
- **Discussion/examples**

# Threat Modeling Walkthrough

---

KUMAR SETTY

PRINCIPAL

ZAKTI SECURITY LABS



# The Problem

---

The attacks never end.

There are new attacks and new attack surfaces which are uncovered every day.

Most organizations just recycle risks. We fail to think outside the box.

# Sun Tzu

---

*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*

*If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.*

*If you know neither the enemy nor yourself, you will succumb in every battle.*

# The Battle of Cannae

---

In 216 BCE, a pivotal battle, The Battle of Cannae, was fought between Carthage and the Roman Republic. This battle was the closest the Roman state had come to destruction in its history up to this point. The Roman Republic survived this disaster and actually ended up annexing the Carthaginian Empire (present day Tunisia).

This Battle was fought in southeast Italy between Carthaginian forces led by the general Hannibal Barca and Roman legions led by generals Lucius Paullus and Gaius Varro. After Rome won the First Punic War, they became the dominant naval power in the Mediterranean Sea, and Rome colonized Iberia to mine its silver, further enriching the Republic.

Hannibal understood Roman strategy and decided to take the initiative by taking the fight to the heart of the Roman Republic.

Hannibal started his campaign by invading Iberia. There he procured silver, supplies, and food, and then used these provisions to cross the Alps into Italy with his army and war elephants. After winning some decisive battles, Hannibal marched through to southern Italy, where he used his silver to buy off Greek and Italian vassals of Rome to join his army. He then encamped at Cannae.

He chose Cannae because it was the center of farming and grain production for the Roman heartland. Hannibal specifically chose a region in Cannae which was near the only source of water in the area. This applied tremendous pressure on the Roman legions and in this manner, he provoked a fight on *his* terms. Hannibal then outflanked the legions and crushed the Roman army. However, unfortunately for Hannibal, Rome's legions were too big to lose. This battle initiated a long drawn out campaign in which Hannibal was eventually defeated by the Roman general Scipio Africanus and Carthage was annexed by Rome.



# The Battle of Cannae - Lessons

---

What can we learn from this? Rome lost the Battle of Cannae because they underestimated and failed to understand their adversary. The Romans never imagined an army would cross the Alps from North Africa (audacious move) with elephants (unique attacker tools) and they did not anticipate what to defend (Iberia, the Alps, and southern Italy) and they failed to anticipate where they would be attacked (from the sole source of water in Cannae).

Hannibal Barca was a bold genius and unlike any adversary the Roman Republic had ever encountered. Hannibal understood his own capabilities and Rome's, he wisely utilized his assets, he knew Roman strategy and battle formations, he understood Rome's weaknesses and who might be willing to betray Rome. He employed assets to gather intelligence prior to engaging Rome in battle. Hannibal found the right attack surfaces.

Threat modeling is something the Roman Republic should have employed. Rome failed to understand Hannibal, his motivations, his strengths, and where, when, and how he would attack them. If the Romans had established a threat model, they might have won the Battle of Cannae.



# The Mongol Invasions of India

---

Well within the 13<sup>th</sup> century, the Mongolian Empire was the largest empire in the world. They ruled from Siberia and China and reached Budapest.

The Mongols tried dozens of times to invade India. Every time they failed. In one instance, just when it seemed like the Mongols would win, they were crushed as a result of a unique counterattack.

In 1299, the Mongol army led by Duwa Khan marched 200,000 cavalry, thousands of foot soldiers, and siege weapons and projectile weapons using gunpowder - all designed by Chinese engineers. This army camped outside of Delhi prepared to crush the city which was under the rule of the Delhi Sultanate, controlled by Sultan Alauddin Khalji.

# The Mongol Siege of Delhi

---

The siege went on for days and at one point it seemed that the Mongol army would breach the fortifications and annihilate the residents of Delhi.

At the brink of defeat, some of the generals of the Sultan came up with a plan.

Within the walls of the Delhi, there was a huge store of fermented ale, which was being saved for a festival. Also, there were several thousand war elephants.

During this time, it was elephant breeding season. The male elephants were irritable because their libido was high.

# Drunk Elephants

---

The army of the sultan made the male elephants thirsty and hungry.

They then placed the female elephants at the other end of the battlefield and fed the females beer so they would be docile.

They fed the male elephants ale to make them more aggressive.

In between the drunk female elephants and the drunk and libidinous male elephants were most of the Mongol army and their siege weapons.

The Sultan's army released the male elephants.

The drunk male elephants flanked and crushed and destroyed the Mongol siege weapons and crushed the invading army so that they could reach the female elephants.

The Sultan then led his archers, cavalry, and army and defeated the remaining Mongol army.

The Sultan then had the elephants crush all the surviving Mongols and thousands of heads were sent back to Mongolia as a warning not to invade India ever again.

The Mongol army tried for many years even after this disaster, but they never were able to conquer India.

# Mongolian Invasion of India - Lessons

---

The Mongol adversary model vs the Indian defender model. Model vs. model and machine vs machine.

The Mongol threat model did not take into account that within the Delhi walls there was a huge store of ale and elephants. Also, it was breeding season for the elephants. Their model did not take this into account.

The Mongol army was “dug in” and concentrated on breaching the walls of Delhi. They were inflexible at this critical point.

The generals in India used out of the box thinking in developing a counterattack. The defender model enabled flexibility so the Sultan's men could formulate this attack.

# What is Threat Modeling?

---

Threat modeling is a process through which security professionals identify threats and vulnerabilities, quantify the likelihood and impact, and then formulate techniques to mitigate attacks to protect an organization.

Combination of art and science.

A crystal ball is not possible.

The process should be ***systematic and structured***.

Goal is “forewarned is forearmed”.

# Threat Modeling

---

An important feature of a security professional is the ability to “predict” the future – future threats, future attacks, and future frauds and enablers. I put “predict” in quotes because it’s impossible to predict the future with certainty but using the right tools and methodologies we can at least ask the right questions in order to clarify our thoughts and impressions and obtain some measurements which we can use as inputs into our planning and strategic decisions.

A completely siloed approach will not work.

# One suggested approach

#	Question	Tasks	Output(s)
1	<b>KNOW YOURSELF</b>  What are you trying to protect?	1. Identify the overall system boundary and identify the flow of information into and out of these boundaries. 2. Enumerate the physical, logical assets – servers, databases, and other components. 3. Identify any intangible assets which are critical to the business.	1. Data Flow Diagram 2. Asset List 3. Surveys sent to individual stakeholders 4. Notes from group sessions.
2	<b>KNOW YOUR ENEMY</b> <b>KNOW YOUR FRIENDS</b>  Who are the attackers (internal and external)?	1. Identify potential threat actors, threats, and attack scenarios. 2. Brainstorm motivations of an attacker through cooperation with different teams and groups. 3. Identify business risks and results of other assessments such as a fraud risk assessment. 4. Who wants to steal or damage the assets? 5. Who are you most concerned about?	1. Adversary Model – resources, access, risk tolerance, and objectives. 2. Attack scenarios or “abuse cases”. 3. Surveys sent to individual stakeholders 4. Notes from group sessions.
3	<b>KNOW YOUR ENEMY</b> <b>KNOW YOUR FRIENDS</b> <b>KNOW YOURSELF</b>  What type of attack surfaces are present? Where will the organization be attacked?	1. Identify the methods, tools, where an attacker or other systems interact with the system. 2. Identify all the third-party integrations and dependencies.	1. Vulnerability Model – Using the Adversary Model above as an input, map vulnerabilities. 2. Interface or integration diagram – high-level and low-level. 3. Surveys sent to individual stakeholders 4. Notes from group sessions.
4	<b>KNOW IT ALL</b>  What are the risks, controls, likelihood, and impact? Countermeasures?	1. Using an established framework such as NIST, identify risks, controls, and calculate likelihood and impact. 2. Calculate total risk exposure by multiplying likelihood and impact. 3. Above a certain threshold for risk exposure, maybe High and Critical, document exploits. 4. Generate corresponding countermeasures for each High and Critical risk exposure.	1. NIST matrix with risks, controls, likelihoods, impact, calculated risk exposure, and detailed countermeasures.



# Caveat

---

It is not as important to generate copious paperwork as it is to *understand* the organization's posture, threats, and countermeasures.

You may not have accounted for all the threats and countermeasures, but at least you have documented your understanding and you might identify any gaps in your understanding. In essence you will know what you don't know.

# Threat Modeling Frameworks

---

The structured approaches for threat modeling are frameworks or methodologies (both interchangeable terms) and are a veritable alphabet soup of acronyms and special lingo. The main frameworks are as follows:

**NIST**

**OCTAVE**

**PASTA**

**STRIDE**

**DREAD**

**MITRE ATT&CK**

# NIST Threat Modeling Methodology

---

The U.S. National Institute of Standards and Technology has its own data-centric threat modeling methodology, which consists of four steps:

Identify and characterize the system and data of interest

Identify and select the attack vectors to be included in the model

Validate the security controls for mitigating the attack vectors

Evaluate the threat model

If you are looking for a great example of how to apply a threat modeling methodology in practice, this is a good resource.

[https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800\\_154\\_draft.pdf](https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf)

# OCTAVE

---

OCTAVE, which stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation, is a threat modeling methodology developed at Carnegie Mellon University that focuses on organizational rather than technological risks. It consists of three phases:

Build asset-based threat profiles

Identify infrastructure vulnerability

Develop a security strategy and plans

<https://resources.sei.cmu.edu/library/Asset-view.cfm?assetid=51546>

# PASTA

---

PASTA or Process for Attack Simulation and Threat Analysis is a seven-step process focused on aligning technical security requirements with business objectives. Each step is fairly involved. The overall sequence is as follows:

Define objectives

Define technical scope

Application decomposition

Threat analysis

Vulnerability and weaknesses analysis

Attack modeling

Risk and impact analysis

[https://owasp.org/www-pdf-archive/AppSecEU2012\\_PASTA.pdf](https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf)

# STRIDE

---

STRIDE was developed at Microsoft in the 1990s and popularized by developers and project managers. STRIDE emphasizes the six categories of threats which violate one of the properties of the CIA triad (confidentiality, integrity, availability):

**Spoofing identity:** An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

**Tampering with data:** Data tampering involves the malicious modification of data.

**Repudiation:** Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. Nonrepudiation refers to the ability of a system to counter repudiation threats.

**Information disclosure:** Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it.

**Denial of service:** Denial of service (DoS) attacks deny service to valid users.

**Elevation of privilege:** In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

# DREAD

---

DREAD was created as a supplement to the STRIDE methodology which enables analysts to rank threats once they have been identified. DREAD is an acronym for the six questions asked regarding each potential threat:

**Damage potential:** How great is the damage if the vulnerability is exploited?

**Reproducibility:** How easy is it to reproduce the attack?

**Exploitability:** How easy is it to launch an attack?

**Affected users:** As a rough percentage, how many users are affected?

**Discoverability:** How easy is it to find the vulnerability?



# MITRE ATT&CK

---

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations from security professionals. This framework is constantly being updated and there are variations which can be “spun off” which concentrate on a specific area, such as cloud computing or mobile security.

Version 9 was just recently released. The ATT&CK framework is an excellent resource for understanding attacker techniques and it is a great starting point for integrating common attacks into a threat model. There are also many resources available to get started on using this methodology.

If you are a visual person, the Enterprise Matrix is an excellent tool for understanding the different stages of attacks from Reconnaissance to Exfiltration to Impact and all the techniques and sub-techniques within each attack category.

<https://attack.mitre.org/resources/getting-started/>

<https://attack.mitre.org/matrices/enterprise/>

# Recommendations

---

Many frameworks exist and there are many similarities.

First understand the organization, study previous assessments, and understand exactly what you are attempting to secure.

Use the OCTAVE methodology since it has a more organizational emphasis. OCTAVE has comprehensive information for developing surveys which can be sent to individuals for completion.

Also use OCTAVE guidelines for the group sessions.

Obtain an understanding of the business risks and fraud risks. These insights should flow into the Adversary Model.

The NIST threat modeling framework as a starting point. I would then integrate the attacker techniques from the MITRE ATT&CK framework to complete the Adversary Model.

In the final stage, the overall model should include overall risk ratings and specific countermeasures. Finally, always remember that your threat model should be a living document and should be revisited and edited on a frequent basis to accommodate changes to the organization's risk profile.

# Always Remember

---

KNOW THYSELF

KNOW THINE ENEMIES AND THINE FRIENDS

KNOW IT ALL

# Who are the bad guys?





# Who are the bad guys?

- Who are they are?
- What do they want?
- How to mitigate?



# Who are the bad guys?

According to a definition - Cybercrime is a crime that in some way uses a computer to commit the crime or a computer is a target of the crime.

Most, but not all, cybercrime is committed by cybercriminals (“hackers”) in order to reach personal goals:

- Profit
- Political
- Personal



# Who are the bad guys?

When we are saying “hackers” – it can literally be anyone. These days we call “hackers” anyone ranging from novice individuals (often kids, who just launch “hacking” scripts for fun) to a very mature and complex organizations, spending huge resources on executing such “hacks”.





# Arsenal of “Bad Guys”

Plain’n’Old “hacking” - exploiting existing vulnerabilities, identifying new ones

- Virus
- Malware
- Ransomware
- DDoS attacks
- Phishing
- Cyber blackmails or extortion
- Cryptojacking



# Current Threats

- APT
- File-less/LoLBINS



# What do “Bad Guys” want?

The biggest part of hacking happens for financial profit.

For example: attacker will get access to company network.  
What would they do?

Recon -> Steal -> Encrypt -> Blackmail

Other common reasons:

- To express political/social views
- Personal (“vendetta”, learning, fun, etc)



# How to fight “Bad Guys”

There are several very simple strategies, which, when combined will give the reasonable protection.

- Understand who (or what) you are protecting against
- Understand whom do you protect with
- Understand your environment
- Pick applicable standard and follow it



# How to fight “Bad Guys”

- ❖ Always start with risk assessment
- ❖ Choose carefully WHAT do you want to protect
- ❖ This will help in defining WHEN and HOW
- ❖ Few practical recommendations
  - ❖ System snapshots are not always sufficient
  - ❖ Take approach that will allow to rebuild, rather than to simply restore
  - ❖ Segment network/traffic into smaller “pools” to restrict traffic flow
  - ❖ Separate critical systems into individual pools
  - ❖ Ship meaningful logs to central location

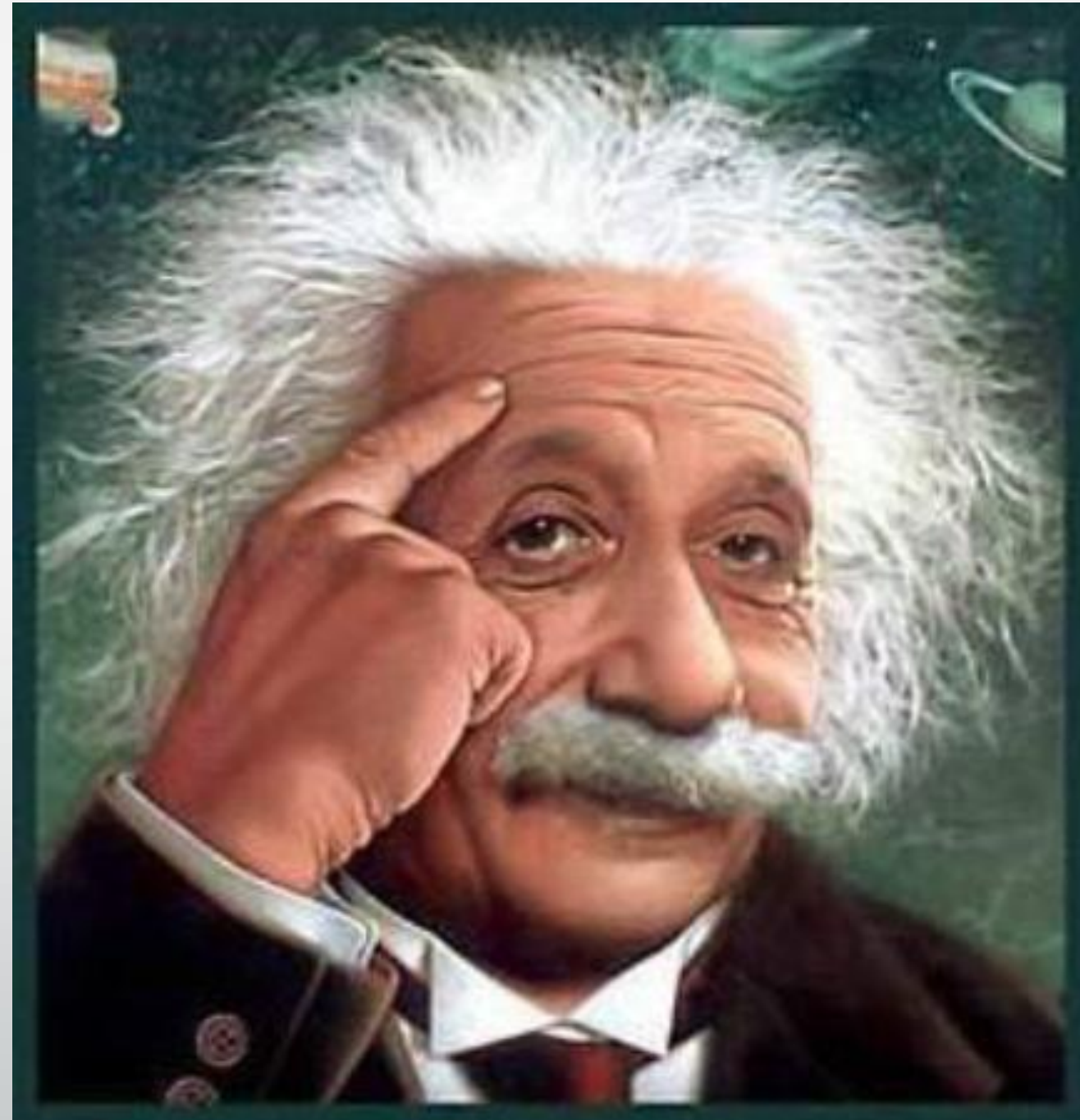


# How to fight “Bad Guys”

Cyber-security is now considered an “arms race”. There are many types of protections available, for different budgets. But hacker’s arsenal also grows, and for each new tool used to protect, there will be 2 or more to overcome. And, as most recent researches show – having more than 50 tools for ensuring cybersecurity in fact WORSENS security posture.

Most cyberattacks are fully or semi- automated. This means that hackers expect an easy target, and if you are protected in a way that is better than “average”, and follow basic rules of cyber hygiene – you will be reasonably secure. There will be much easier targets nearby 😊

# Why standards?







# Standards

- Standards are basic recommendations that are very flexible and can be easily adapted.
- Many organizations are afraid to adapt a standard as they think that they are hard or complex and would require them to change their business processes. However, standards do not require companies to change their processes. Standards do not recommend physical technology or methods as a solution.
- We will show some standard techniques to demonstrate how it can be implemented in your day-to-day operations.



# Frameworks

- anything written
- PCI?
- HITRUST??
- Cloud Security Alliance???





# Standards

- ISO
- NIST
- SSAE 18?



**NIST**





# Standards

Cyber Security standards are industry accepted principals with objectives to reduce risks and prevent or mitigate cyber attacks.

## Most accepted standards in USA:

### ISO 27001

**Pros:**

- International
- Certifiable
- Widely recognized and accepted

**Cons:**

- Procedural
- Top-down – executives have to buy in

### NIST

**Pros:**

- US national standard
- US laws are based on NIST
- Can be adapted on a department level

**Cons:**

- Not certifiable – self attestation

### PCI

**Pros:**

- Very active standard enforced by banks
- Certifiable

**Cons:**

- E-commerce specific
- Not recognized in financial and manufacturing world

### SOC

**Pros:**

- Concentrates on overall stability of the company, not just security controls.
- Certifiable

**Cons:**

- A loose report sometimes demonstrating an opinion
- The report is often not in-depth

### HITRUST

**Pros:**

- Respected
- Hard to pass
- Show maturity
- Real audit of control implementation
- Strong scoring

**Cons:**

- Very expensive
- Very long
- Hard time brackets



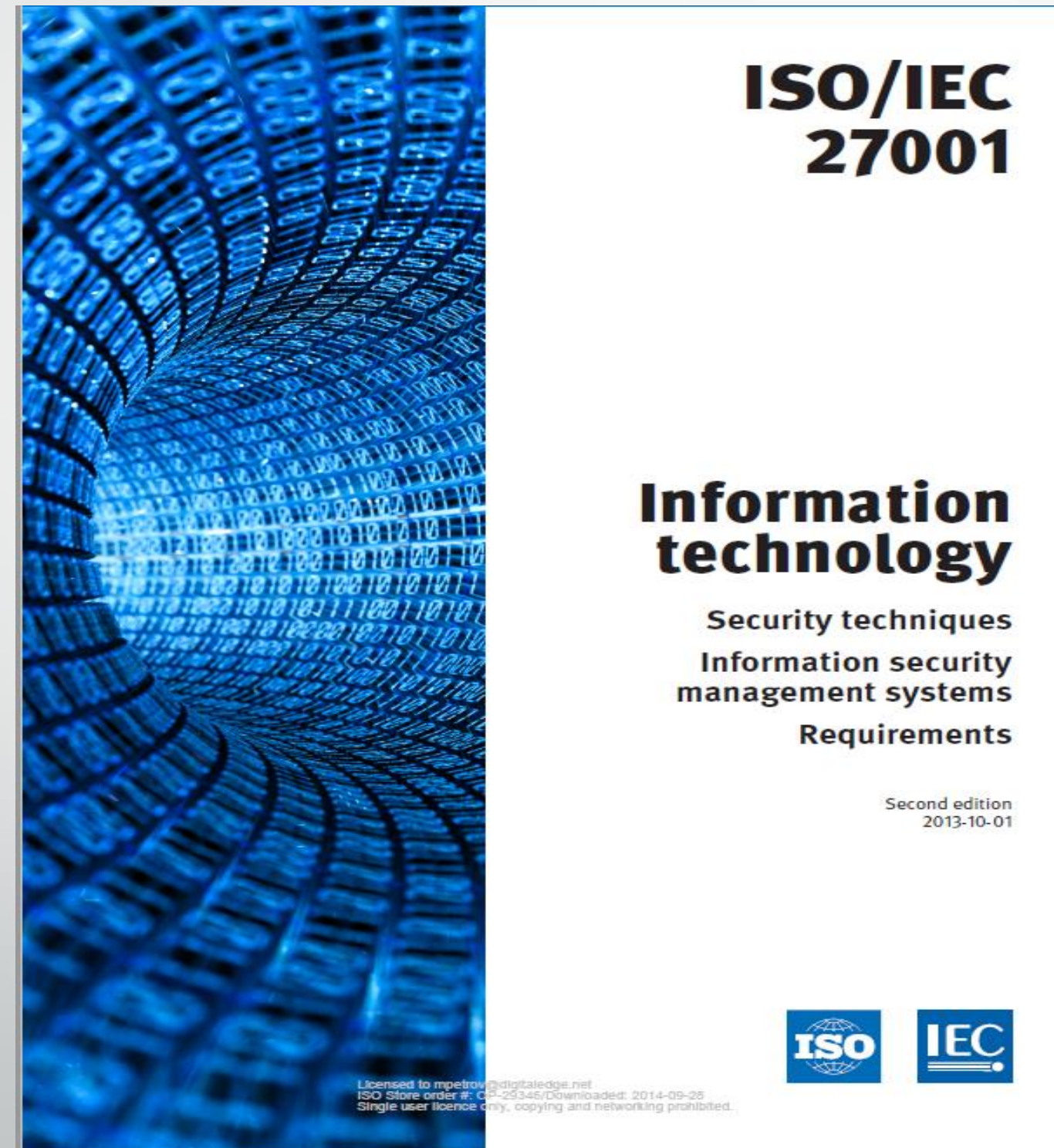
# Standards

- **Laws, regulations do not expect that all information security incidents will be prevented**
- **Standards do not guarantee that full implementation will protect from all the attacks**
- **BUT they make us responsible for implementing necessary safeguards to prevent harm. This is the essence of “Duty to Care”**
- **Judges use “Duty to Care” to determine liabilities in data breaches.**
- **FTC requires risk assessment to demonstrate reasonability of the controls**
- **GDPR requires protection of privacy based on risk analysis.**





# They look boring





# ISO structure

- 1.Context of the organization
- 2.Leadership
- 3.Planning
- 4.Support
- 5.Operation
- 6.Performance Evaluation
- 7.Improvement
- 8.Annex (Controls)



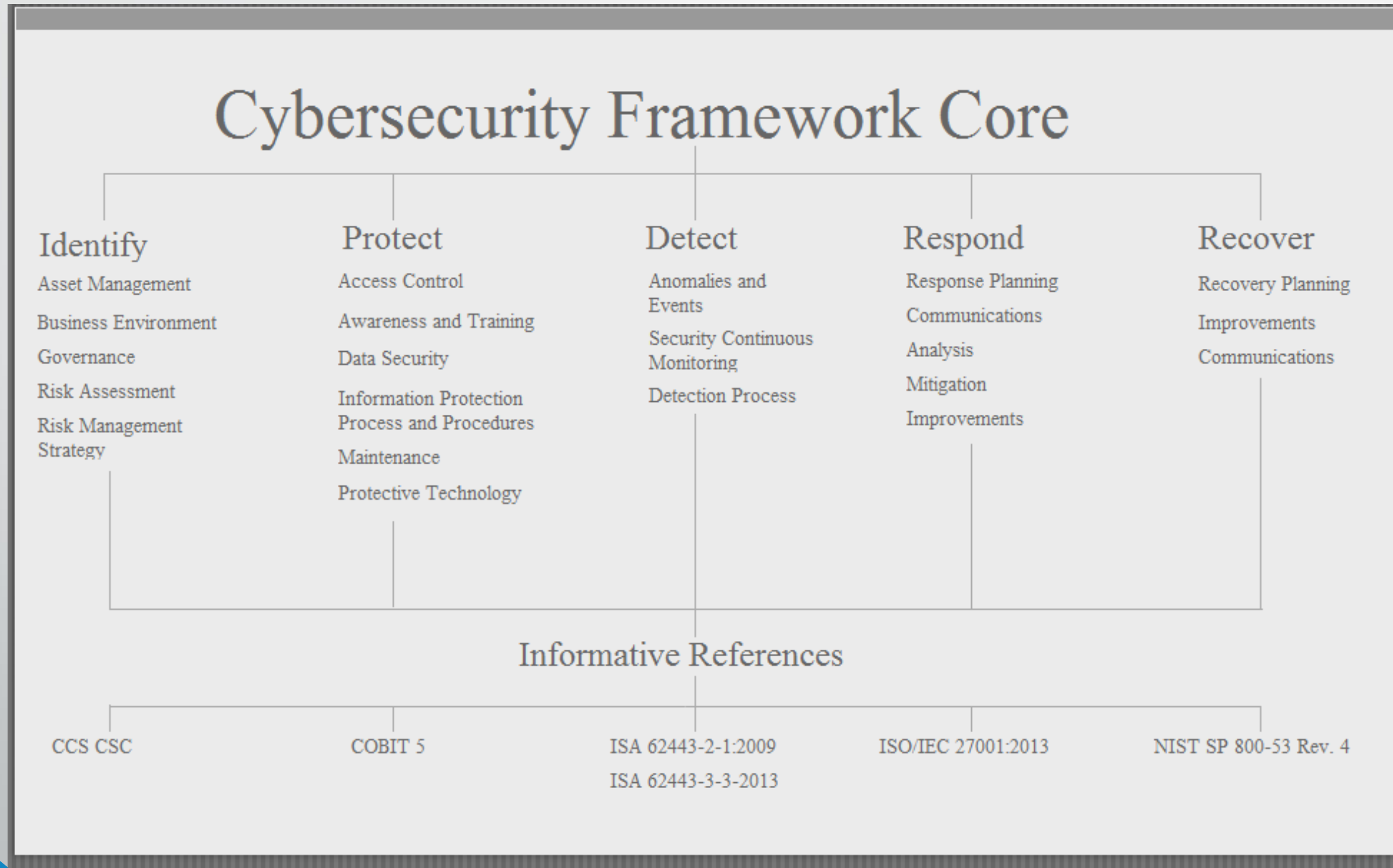
# ISO structure - Annex

1. Information Security Policies
2. Organization of Information Security
3. Human Resources Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communication Security
10. System Acquisition, Development Maintenance
11. Supplier Relationship
12. Information Security Incident Management
13. Compliance





# NIST structure





# SSAE 18 SOC2

- SECURITY PRINCIPLE:
  - ☐ ORGANIZATION AND MANAGEMENT
  - ☐ COMMUNICATIONS
  - ☐ RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS
  - ☐ MONITORING OF CONTROLS
  - ☐ LOGICAL AND PHYSICAL ACCESS CONTROLS
  - ☐ LOGICAL AND PHYSICAL ACCESS
  - ☐ SYSTEM OPERATIONS
  - ☐ CHANGE MANAGEMENT
- THE AVAILABILITY PRINCIPLE:
  - ☐ ADDITIONAL CRITERIA
- PROCESSING INTEGRITY:
  - ☐ ADDITIONAL CRITERIA
- CONFIDENTIALITY:
  - ☐ ADDITIONAL CRITERIA
- PRIVACY:
  - ☐ ADDITIONAL CRITERIA



# Zero Trust (requested by Vince Werling)

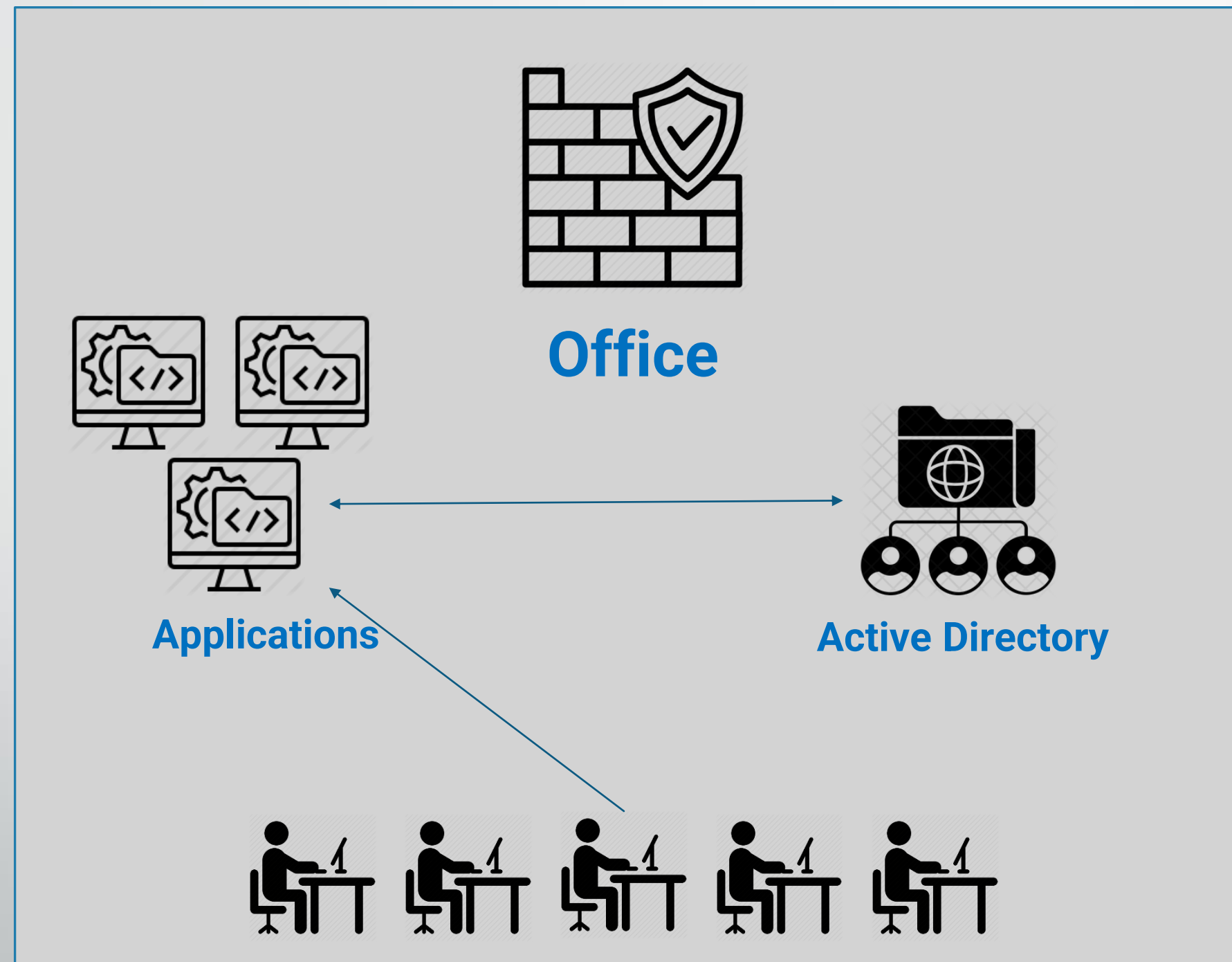
<https://www.youtube.com/watch?v=tFrbt9s4Fns>

Paul Simmonds – HYSTERICAL

...ACCESS MANAGEMENT IS REALLY KEY...

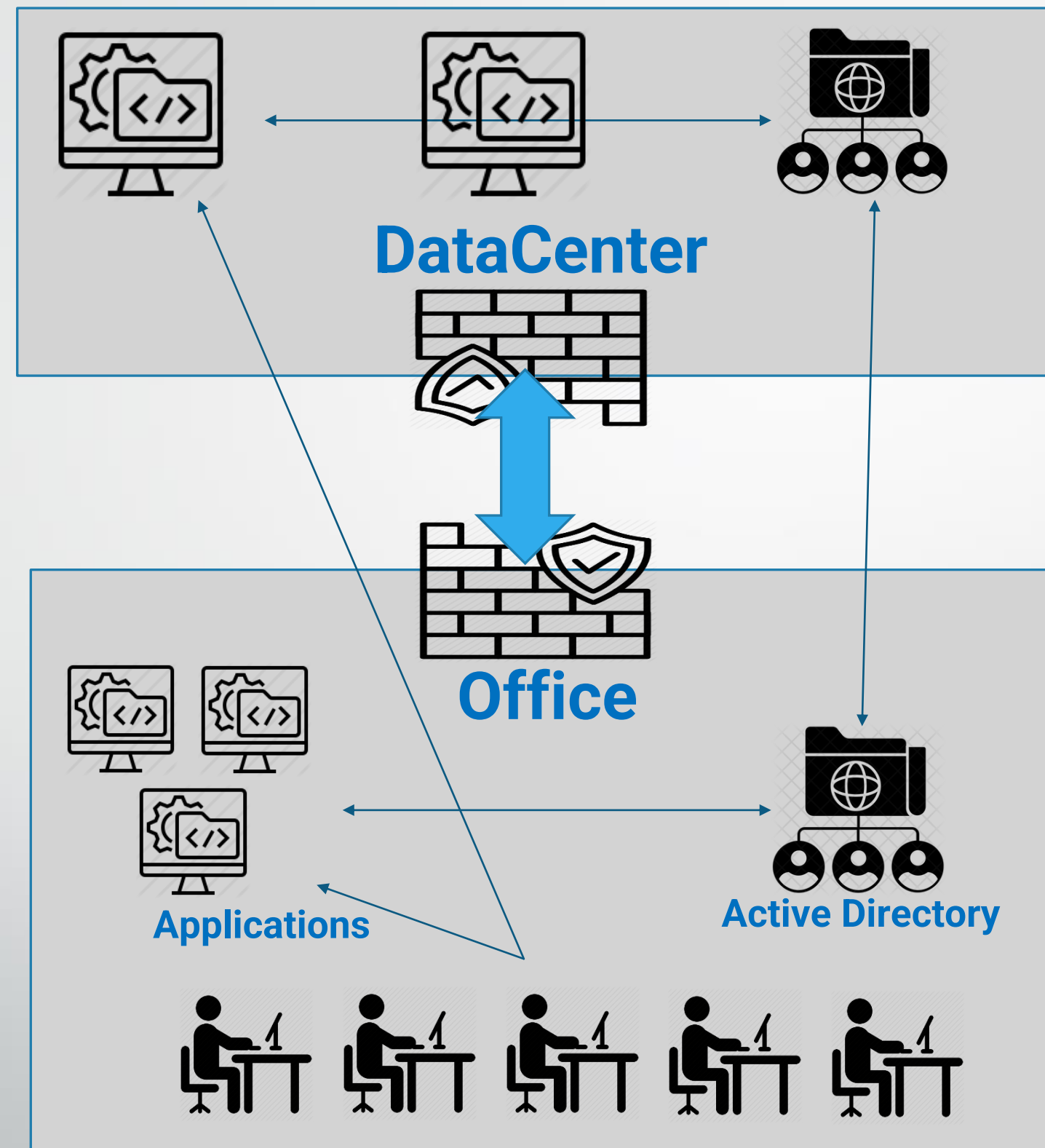


# Standard, perimeter-based security



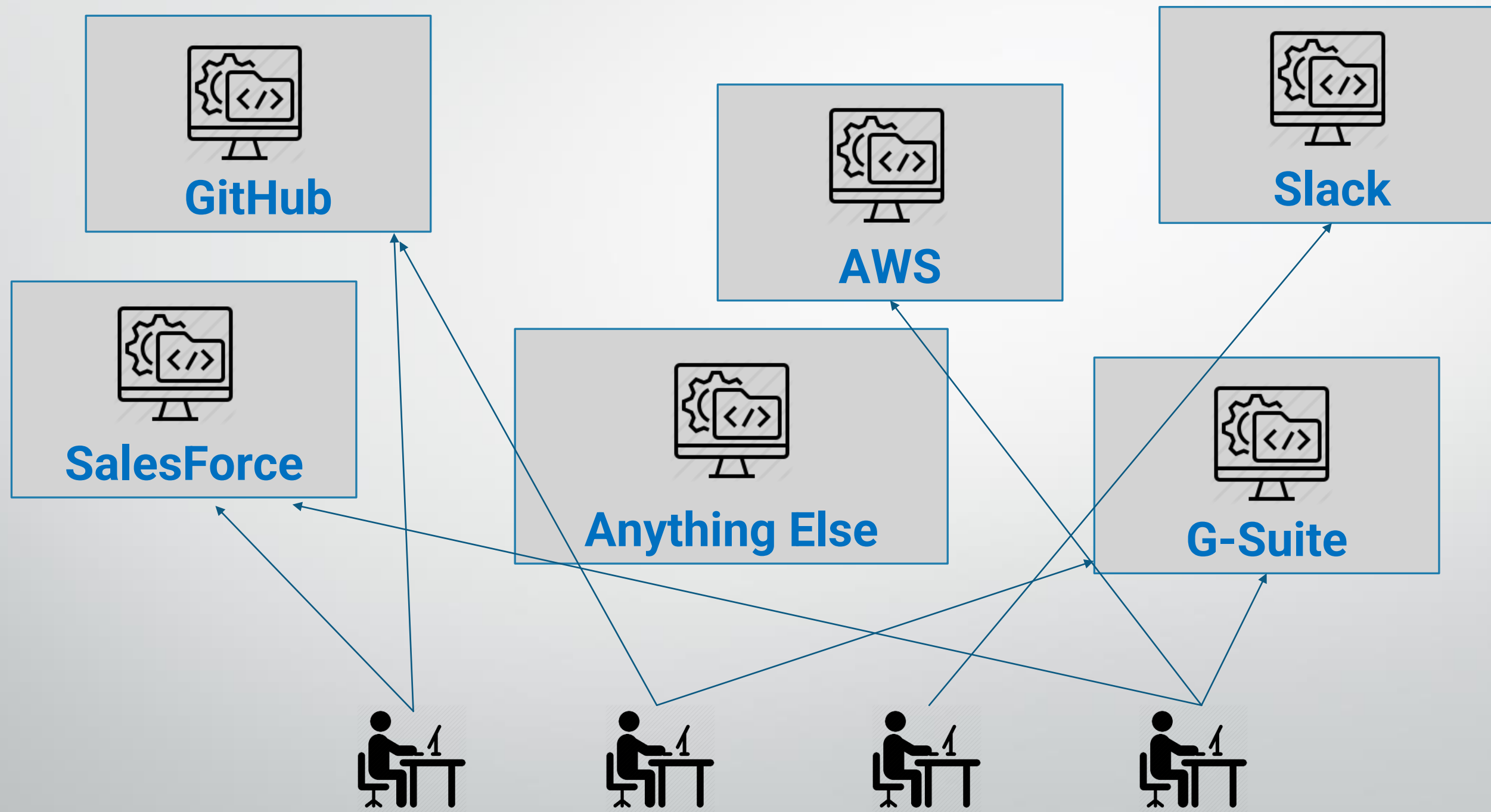


# Standard, perimeter-based security



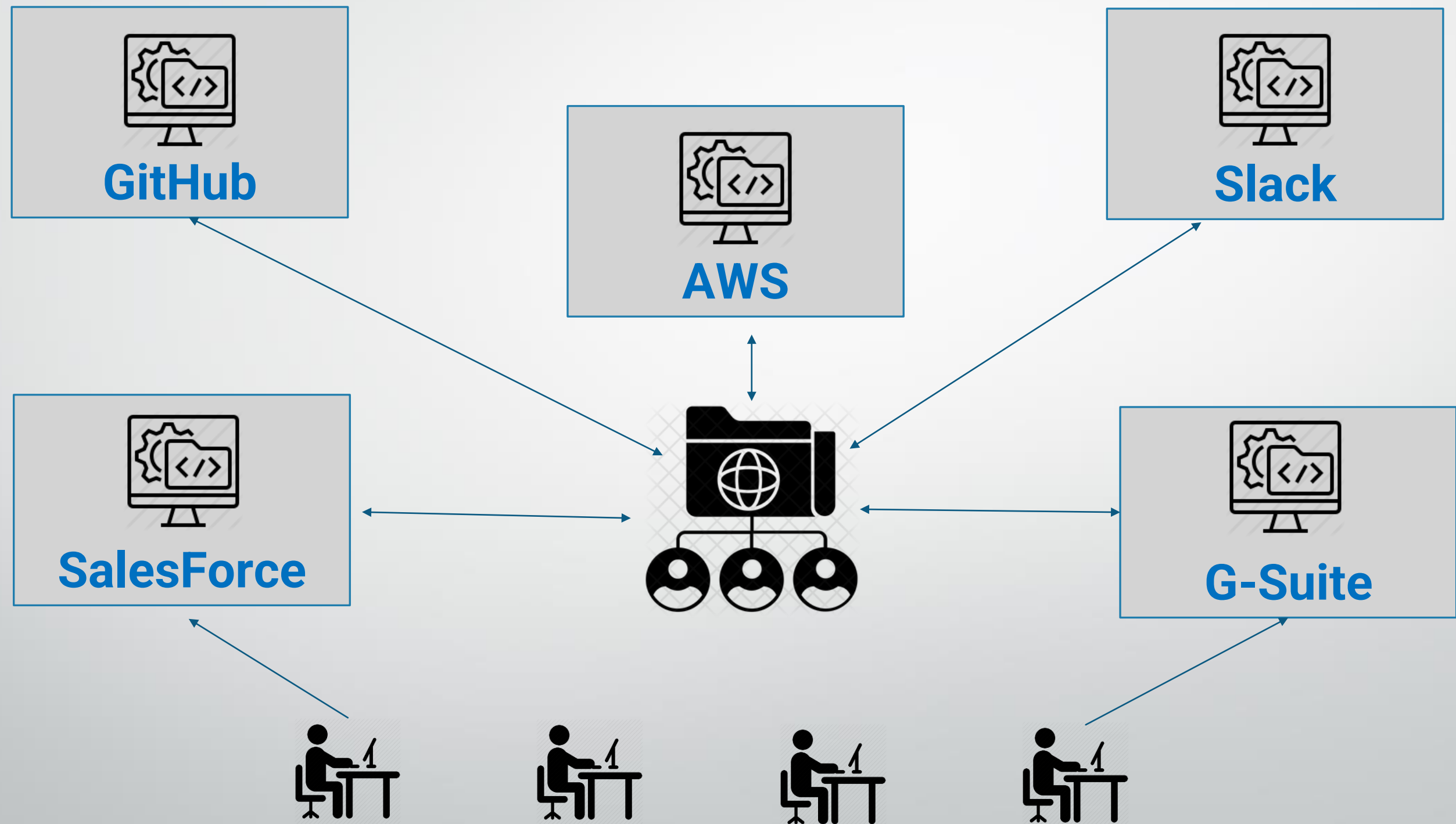


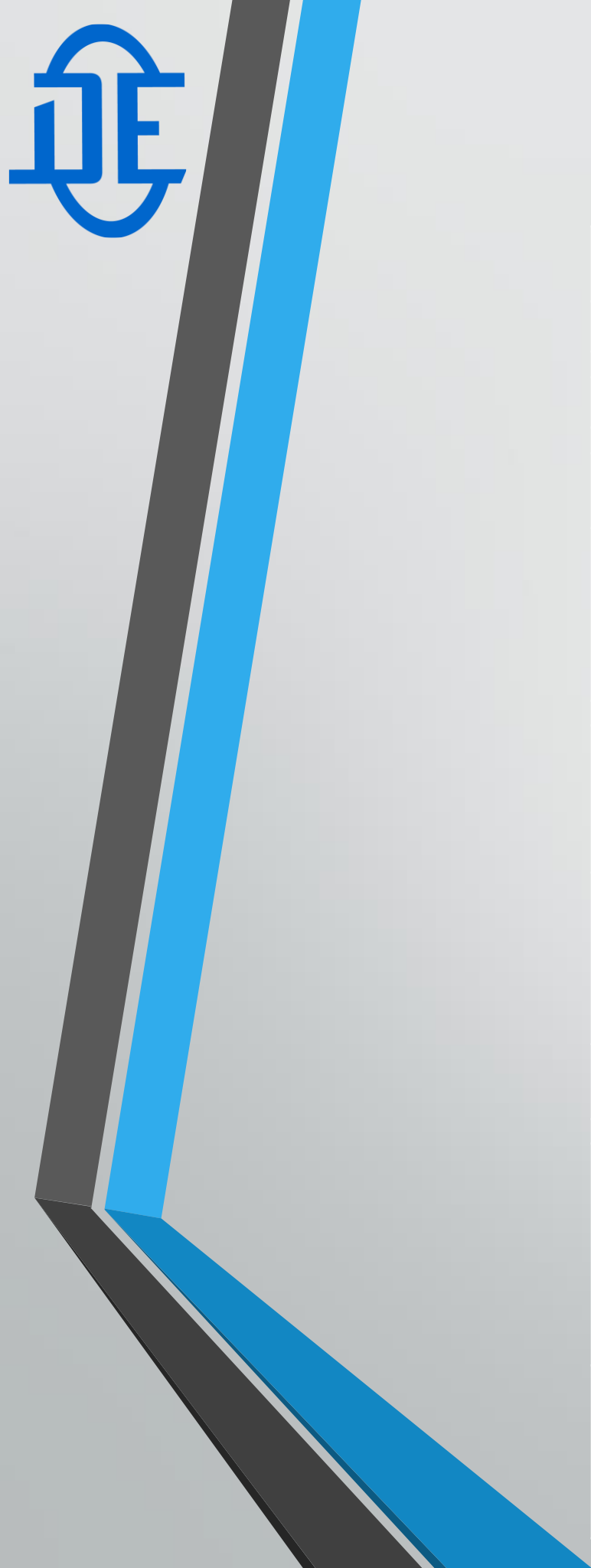
# Zero-trust based





# Zero-trust based





# Zero-trust based

	Microsoft AD	Microsoft AD (AWS Managed Directory)	Google Directory (Google Cloud Identity)	JumpCloud DaaS	OKTA	FreeIPA	OpenLDAP
G-Suite	Yes (GADS)	Yes (GADS)	Yes (native)	Yes	Yes	Yes (SAML or GCDS)	Yes (GCDS)
AWS	Yes (ADC or SAML)	Yes (ADC or SAML)	Yes (SSO-SAML)	Yes (SAML)	Yes (SAML)	Yes (SAML)	Yes (SAML)
DropBox	Yes	Yes		Yes (SSO-SAML)	Yes (Dropbox business)		Yes (LDAP)
Slack	Yes	Yes		Yes (SSO-SAML)	Yes (SSO-SAML)	Yes (SAML)	Yes
GitHub * Assumes GitHub Enterprise Cloud	Yes (SAML)	*limited (full ADFS required)		Yes (SSO-SAML)	Yes (SAML, SCIM)	Yes (SAML)	Yes (LDAP)
Sophos	Yes (LDAP)	Yes (LDAP)	Yes (LDAP - G Suite Enterprise, Cloud Identity Premium, G Suite Enterprise for Education, and G Suite for Education)	Yes (LDAP)	Yes (LDAP)		Yes (LDAP)
Comment							
	Regular EC2 instance, self-managed. Need to consider availability	Managed by AWS, requires additional ec2 instance with windows for AD managment	Secure LDAP only with several plans.	OpenLDAP as backend		Good support with RedHat/CentOS, but installation with other systems is not trivial	Requires Shibboleth IdP for SAML
		Some features are limited (only 5 fine-grained policied, pre-defined object locations, no ADFS)	Requires a lot f manual configuration	Pre-built guides/configurations available		Can run with docker containers	Can run with docker containers
	Limited MacOS support	Limited MacOS support					HIGHEST level of manual work and management
Cost							
	\$288 per month + EC2 instance for management	t2.medium, windows 2019 base * 2x instances = ~\$94 per month	Free edition has no SecureLDAP + has user cap (should be enough for Halo, since Gsuite is purhased, which allows free users cap extension)	Pro tier - \$10 per user per month (billed annually)	SSO + Lifecycle Management = \$2 + \$4 = \$6 per user per month		
		* on-demand pricing	Cloud Identity Premium - \$6 per user per month	Custom: Cloud Directory + Cloud LDAP + SSO(SAML2) = \$2 + \$3 + \$3 = \$8 per user per month billed annually			





# Segmentation – AWS Sample



# The structure of Cybersecurity Compliance





# It is all about 2 things



CONTEXT and SCOPE



# Information Classification

FIPS

<https://csrc.nist.gov/publications/detail/fips/199/final>

CIA factor

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<b><i>Confidentiality</i></b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Integrity</i></b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Availability</i></b> Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.



# Risk

- **Laws, regulations do not expect that all information security incidents will be prevented**
- **Standards do not guarantee that full implementation will protect from all the attacks**
- **BUT they make us responsible for implementing necessary safeguards to prevent harm. This is the essence of “Duty to Care”**
- **Judges use “Duty to Care” to determine liabilities in data breaches.**
- **FTC requires risk assessment to demonstrate reasonability of the controls**
- **GDPR requires protection of privacy based on risk analysis.**



# **Risk**

**Sufficient of safeguards  
Compliance goals  
“Reasonable”**





# Risk problems

- It is very important
- No standardization
  - “Decisions are often made based on individual’s instinct and knowledge of conventional wisdom and typical practices” – NIST.IR 8286*
- System based approach problems
- Likelihood ⇔ Impact ⇔ Rating
- FAIR (<https://www.fairinstitute.org/about>)
  
- Risk appetite. “Email service shall be available during large majority of a 24 hour period.
- Risk tolerance: “Email service shall not be interrupted more than 5 minutes during core hours”
  
- Granularity questions
- Multidimensional questions
- Treatment and residual risk questions
- Likelihood problems
- Dynamic in nature
- KRI/Fair?
- Constantly shifting



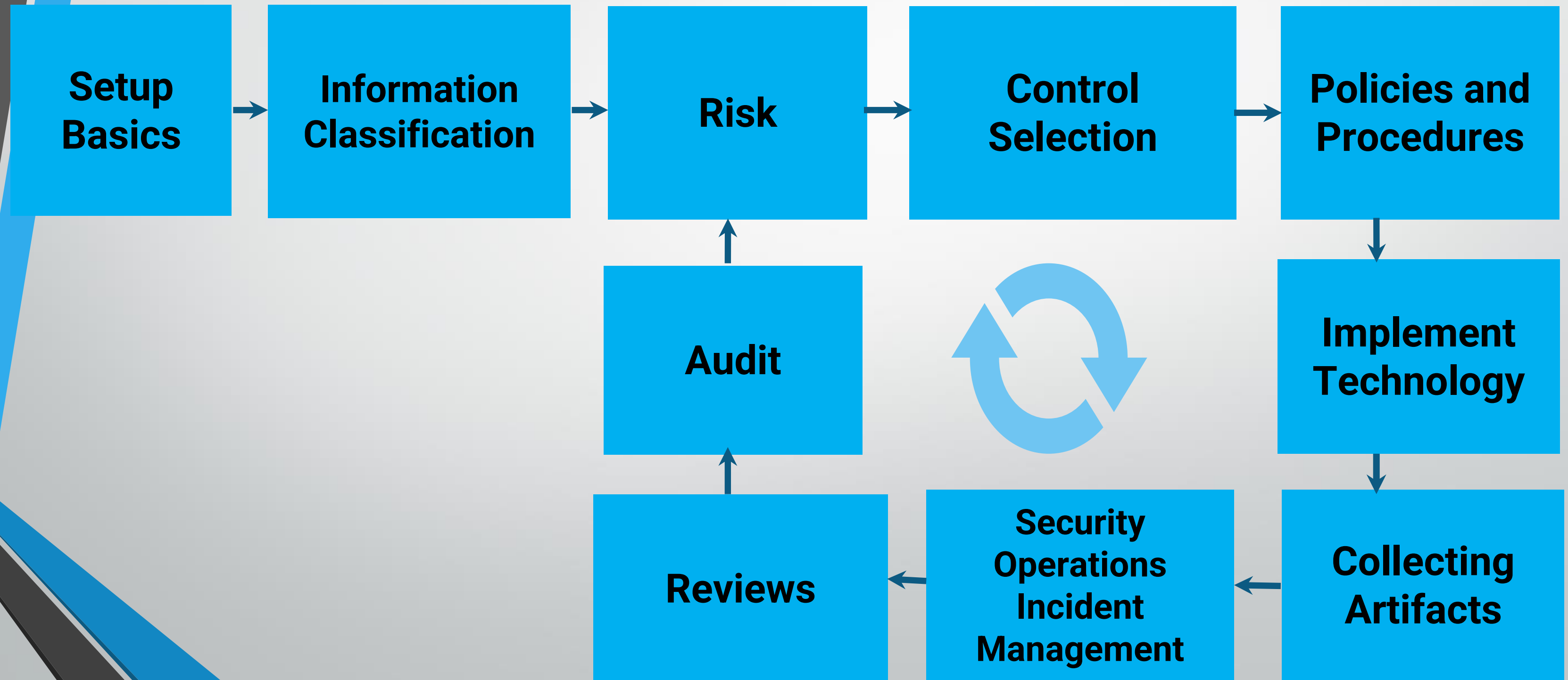
# Risk function

- To select controls
- Awareness of the executives
- To capture historical view
- To measure effectiveness
- To measure and adjust likelihood
- To report to executives
- To adjust control selection
- Budget





# Simplifying standards





# SETUP BASICS

- **Governance**
- **Roles**
- **Scope**
- **Mission**
- **Lines of business**
- **Context**
- **Boundaries**





# Information Classification

- CIA factor
- PII identification
- Informational assets
- Retention
- Deletions rules
- Owner
- Access rules





# RISKS

- Identification
- Classification
- Management
- **Link to incidents**

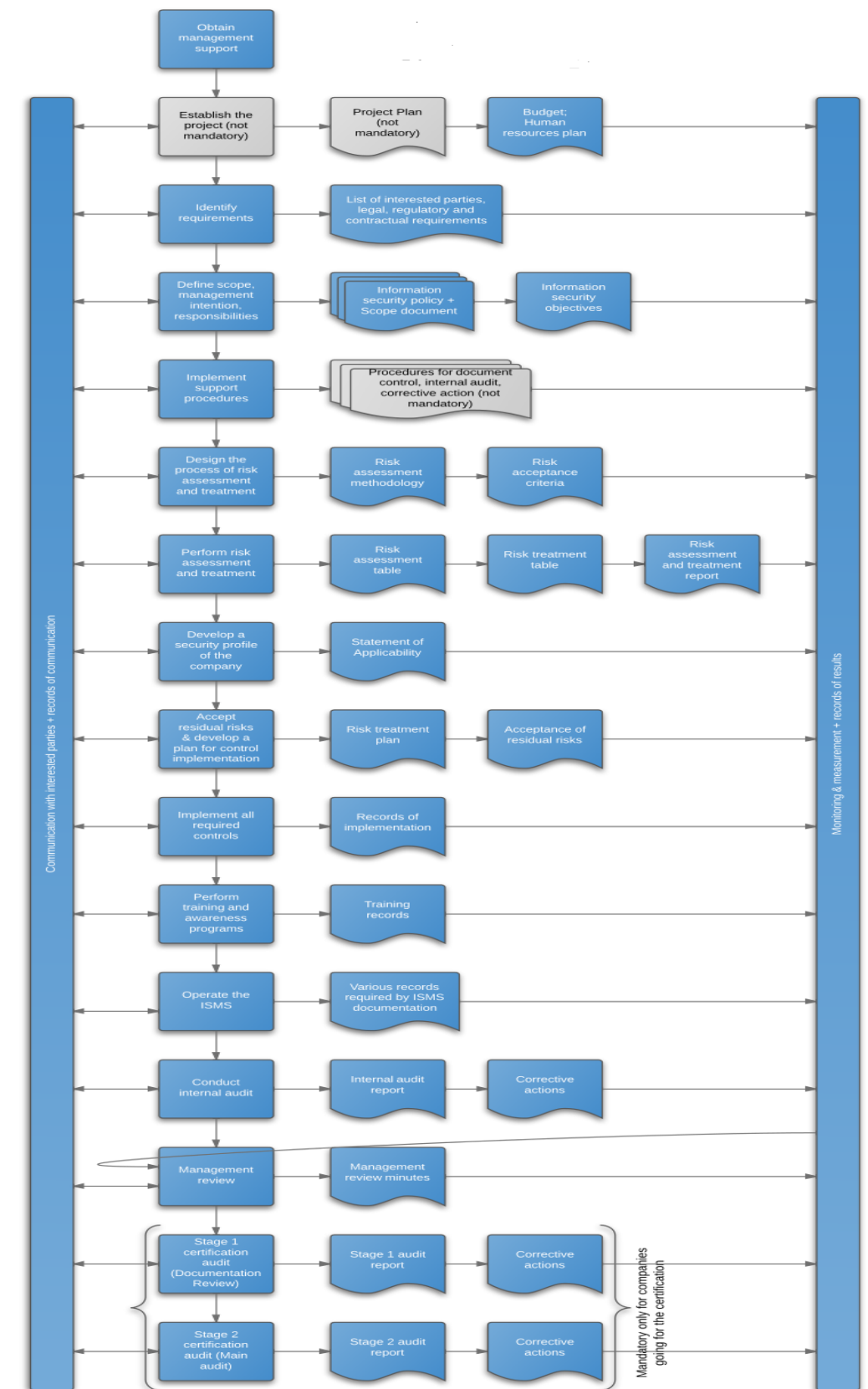




# CONTROL SELECTION

- Select applicable controls from the standard
- Review sufficiency
- Applicability statement

Diagram of ISO 27001:2013 Implementation Process







# POLICIES AND PROCEDURES

- Documentation/Versioning
- Awareness
- Reviews
- Policies
  - **Must/Shall/Will**
- Procedures
  - **Who/When/What/How**





# TECHNOLOGY IMPLEMENTATION

- Review controls and required artifacts
- Additional implementations and compensations
- Monitoring and review
- **Feed to GRC and SOC**
- **Quality/ HITRUST scoring**







# COLLECT ARTIFACTS

- Review controls and required artifacts
- Additional implementations and compensations
- Monitoring and **review**

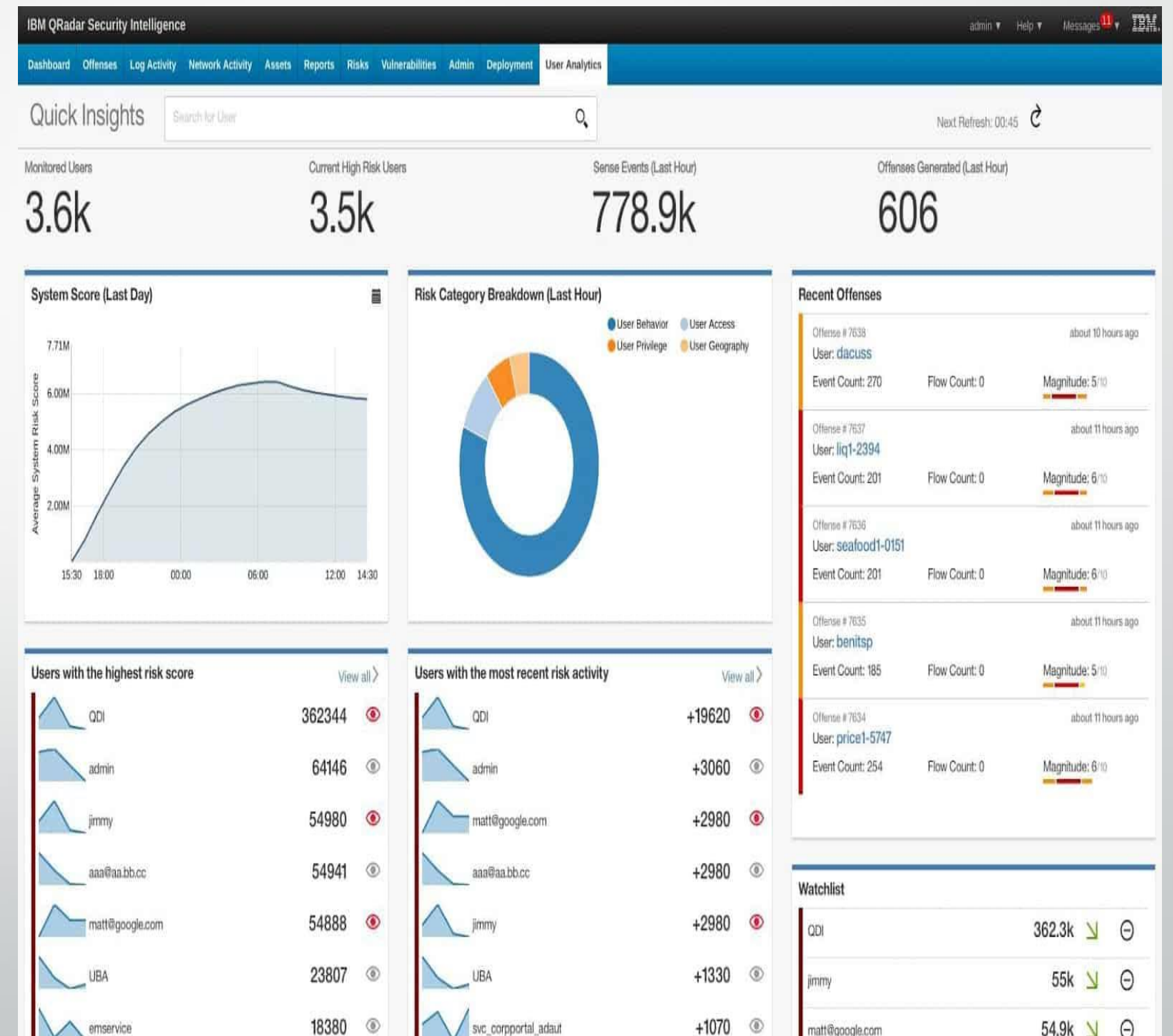
```
[bash-3.2# pwd
/var/db/diagnostics
[bash-3.2# ls -l
total 192584
drwxr-xr-x  2 root  wheel   68 Sep 27 19:03 Events
drwxr-xr-x 31 root  wheel 1054 Nov 13 19:44 FaultsAndErrors
drwxr-xr-x  2 root  wheel   68 Sep 27 19:03 Oversize
drwxr-xr-x  2 root  wheel   68 Sep 27 19:03 SpecialHandling
drwxr-xr-x  2 root  wheel   68 Sep 27 19:03 StateDumps
drwxr-xr-x 16 root  wheel  544 Nov 13 19:44 TTL
-rw-r----- 1 root  wheel 10586976 Nov  6 06:08 logdata.Persistent.20161106T045449.tracev3
-rw-r----- 1 root  wheel 10549904 Nov  6 17:03 logdata.Persistent.20161106T112151.tracev3
-rw-r----- 1 root  wheel 2331488 Nov  6 19:17 logdata.Persistent.20161106T221230.tracev3
-rw-r----- 1 root  wheel 6667976 Nov  7 19:18 logdata.Persistent.20161107T002825.tracev3
-rw-r----- 1 root  wheel 3605360 Nov  7 21:56 logdata.Persistent.20161108T003223.tracev3
-rw-r----- 1 root  wheel 10506760 Nov  9 23:11 logdata.Persistent.20161109T001242.tracev3
-rw-r----- 1 root  wheel 3068952 Nov 10 20:57 logdata.Persistent.20161110T051134.tracev3
-rw-r----- 1 root  wheel 10587272 Nov 11 17:55 logdata.Persistent.20161111T023347.tracev3
-rw-r----- 1 root  wheel 3177928 Nov 11 20:21 logdata.Persistent.20161111T230548.tracev3
-rw-r----- 1 root  wheel 10573896 Nov 12 12:10 logdata.Persistent.20161112T012527.tracev3
-rw-r----- 1 root  wheel 5564952 Nov 12 19:32 logdata.Persistent.20161112T185153.tracev3
-rw-r----- 1 root  wheel 10602712 Nov 13 11:58 logdata.Persistent.20161113T003205.tracev3
-rw-r----- 1 root  wheel 9023072 Nov 13 19:37 logdata.Persistent.20161113T170327.tracev3
-rw-r----- 1 root  wheel 520040 Nov 13 19:59 logdata.Persistent.20161114T004307.tracev3
-rw-r----- 1 root  wheel 1212268 Nov 13 19:43 logdata.statistics.0.txt
```





# SECURITY OPERATIONS

- Security Information and Event Management
- SOC
- Reviews and SOPs
- Escalations





# INCIDENT MANAGEMENT

- CIRT operations
- **Legal aspects**
- Documentation
- Risk correlation and measurements








# INTERNAL AUDIT

- Checkboxes vs self continues Due Diligence process
- Scheduled reviews
- Internal Audits
- Management reviews
- Standardization of DDQs

	AVS Quality Management System	OPM #	Revision 0
Title: AFS-460 Audit Team Leader Checklists		Effective Date:	Page 5 of 6

**Closing Meeting**

A closing meeting, chaired by the team leader, will be held to present the audit findings in such a manner that the audited party understands them. Participants should include the audited party's management and/or those responsible for the audited requirements or procedures.

	Yes	No	N/A
1. Extend appreciation to the audited party for their cooperation and assistance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Reiterate the audit objective and scope	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Describe the verification methods used during the audit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Review results of the audit: <ul style="list-style-type: none"><li>• Positive aspects of the audit</li><li>• Observations and whether they require follow-up</li><li>• Safety critical, safety compliance issues, and other findings</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Inform final report will be distributed to the division manager within 21 calendar-days from the conclusion of the audit <ul style="list-style-type: none"><li>• If additional information is needed, the team leader will notify the branch manager</li><li>• The audit is concluded 7 calendar-days after all data is collected</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Close out any logistics and security matters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Provide the audited party with AFS-460 Audit Process Feedback form (AFS-460-001-T01-F3)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Team Leader: \_\_\_\_\_ Date: \_\_\_\_\_

Audit Project Number: ADT-FY- \_\_\_\_\_ - \_\_\_\_\_ Facility: \_\_\_\_\_

UNCONTROLLED COPY WHEN DOWNLOADED  
Check The Master List To Verify That This Is The Correct Revision Before Use



# OUR ATTITUDE

**Setup  
Basics**

**Information  
Classification**

**Risk**

**Control  
Selection**

**Policies and  
Procedures**

**Audit**

**Reviews**

**Security  
Operations  
Incident  
Management**

**Implement  
Technology**

**Collecting  
Artifacts**





# Vendor Management

- **Standardize audit**
- **SLA definition**
- **Contractual language**



# Education

- General employee awareness
- **Privileged user education**



# Reviews and Audits

- Hard to control
- Need tools
- Automagical artifacts/Manual artifacts
- Define procedure



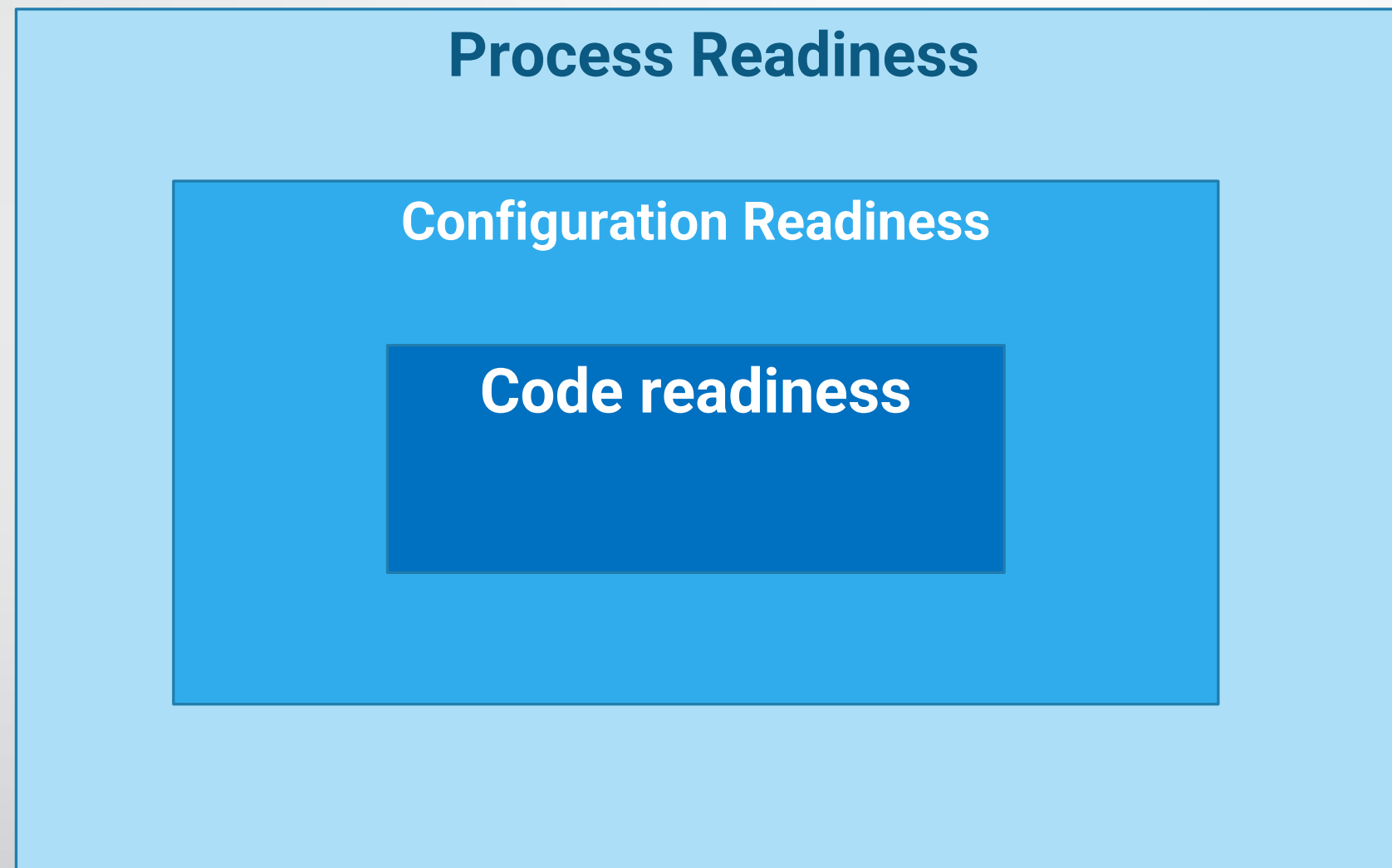
# Compliance in Public Clouds

Essential Rules for  
**Public Cloud**  
Security and Compliance





# Moving to Cloud?





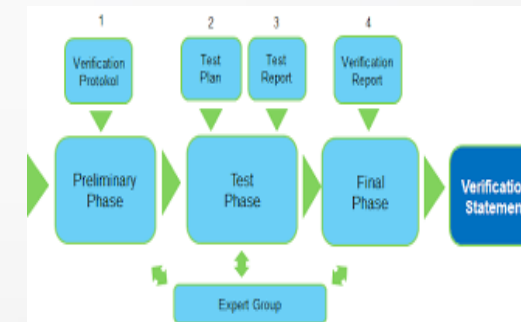
# Moving to Cloud?



Code  
Verification



Configuration  
Verification



Processes  
Verification



# Code Readiness

**OWASP:**

[https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated\\_content](https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content)



# ATTACKS



UP

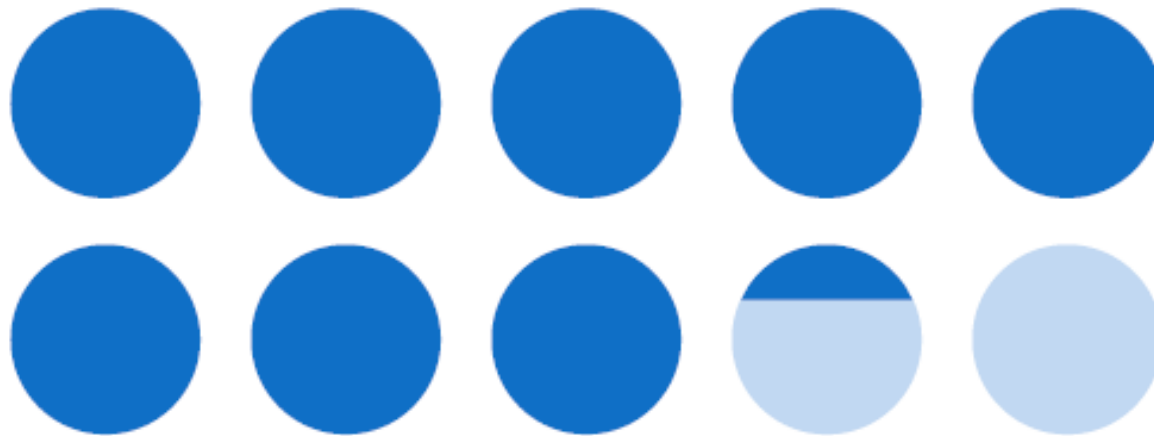
## SECURE CODING



# Code Readiness

## *Concern about open source security*

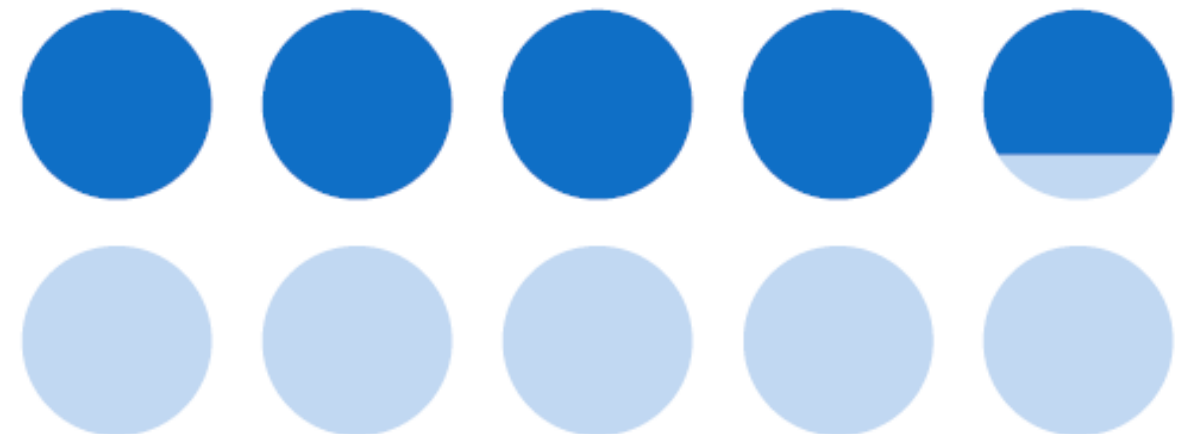
83% of developers are concerned about whether the open source code they use is secure.



Source: Enterprise JavaScript in 2019, npm

## *Security is important, but time is scarce*

48% of developers say they believe security is important but don't have enough time to spend on it.



Source: DevSecOps Community Survey 2019, Sonatype





# Code Readiness

Automated Vulnerability Identification Integrated  
in Your Software Development Life Cycle Automating DevSecOps

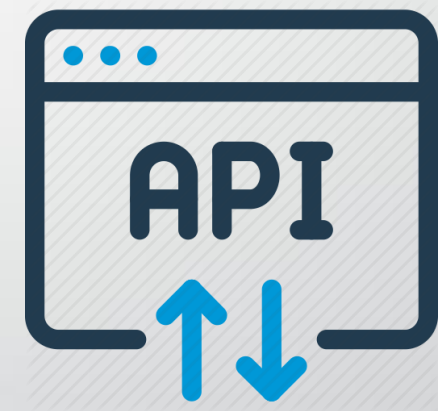


**Jenkins**

1. CI build step  
initialize ZAP proxy



2. Traffic flows through ZAP web proxy  
3. Targeted app sends response through ZAP proxy  
4. Proxy modifies requests to include Security Tasks



Jira

Confluence

5. ZAP outputs scan results as a Security Task List

[https://owasp.org/www-community/Source\\_Code\\_Analysis\\_Tools](https://owasp.org/www-community/Source_Code_Analysis_Tools)



# Code Readiness

## Coders education

### OWASP principals

Input Validation: .....  
Output Encoding: .....  
Authentication and Password Management: .....  
Session Management: .....  
Access Control: .....  
Cryptographic Practices: .....  
Error Handling and Logging: .....  
Data Protection: .....  
Communication Security: .....  
System Configuration: .....  
Database Security: .....  
File Management: .....  
Memory Management: .....  
General Coding Practices: .....



docker



kubernetes

Not a security tools



GitHub

Not a secret store



DevOps => DevSecOps



Security is not guaranteed





# Configuration Readiness

**Through 2025, 99% of cloud security failures will be the customer's fault.**

**Gartner:**

<https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>



# Configuration Readiness

**CIS:**

[https://www.cisecurity.org/benchmark/amazon\\_web\\_services/](https://www.cisecurity.org/benchmark/amazon_web_services/)



# Processes readiness

**ISO**

**NIST**

**PCI**

**HITRUST**

**OSPAR**

**SOC**



# Exercise

**Create a due diligence list for 3<sup>rd</sup> party vendors**

**Develop your dream Cyber Security Program  
Effectiveness report.**



# HAJIME!

(Begin!)





# Yahoo 2014 Breach

**Reason: Spear Phishing**

**Intruder: Russia**

The hack began with a spear-phishing email sent in early 2014 to a Yahoo company employee. It's unclear how many employees were targeted and how many emails were sent, but it only takes one person to click a link.

Once Aleksey Belan, a Latvian hacker hired by Russian agents, started poking around the network, he looked for two prizes: Yahoo's user database and the Account Management Tool, which is used to edit the database. He soon found them.

So he wouldn't lose access, he installed a backdoor on a Yahoo server that would allow him access, and in December he stole a backup copy of Yahoo's user database and transferred it to his own computer.

<https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>

**Yahoo hacker vs Cybersecurity Standard**

**Undecided**



# Marriot 2014 Breach

Reason: Unknown

Intruder: Possibly China

**Rusty Carter, VP, Product Management, Arxan:** *"In this situation, the attackers had access since 2014 which shows that for years they went undetected and were able to access sensitive data about individuals and their travel. This attack sheds light on the fact that many enterprise backend systems and databases are vulnerable because they must trust the application accessing them. Furthermore, the massive size of this breach further highlights the need for regulation to protect consumers. Companies need to protect their applications from tampering and reverse engineering attacks if they want to keep (or rebuild) their customers' trust. Key to minimizing the impact and likelihood of success is developing strategies that include strong detection and reporting of the health and status of applications both inside and outside the company's network."*

**Ian Eyberg, CEO, NanoVMs:** *"This breach happened because the underlying operating systems are completely broken. The underlying systems - be it Windows or Linux, the two most prevalent server-side operating systems today - are broken by design because they predate both wide-scale commercialized virtualization (a la vmware) and the "cloud" (aws). They are inherently designed to run multiple programs on the same server which is what allows attackers to run their programs on them (like connecting to a database and slurping down 500M records). This doesn't have to be the case though - newer operating systems exist that allow you to run only one program on a given virtual machine (server) - the one that was designed to run there - not the attacker's program. Hotels need to start looking at preventive measures such as only using single process systems that limit only running the single program that was designed to run on a given server thus not allowing attackers to run theirs."*

<https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective>

**Marriot hackers vs Cybersecurity Standard**  
**Undecided, would mitigate a lot of issues**





# Equifax 2017 Breach

## Reason: Unpatched Apache

The following day, the Department of Homeland Security contacted Equifax, Experian, and TransUnion to notify them of the vulnerability. On March 9, 2017, an internal email notification was sent to Equifax administrators directing them to apply the Apache patch. Equifax's information security department ran scans on March 15, 2017 that were meant to identify systems that were vulnerable to the Apache Struts issue, but the scans did not identify the vulnerability.

The vulnerability was left unpatched until July 29, 2017 when Equifax's information security department discovered "suspicious network traffic" associated with its online dispute portal and applied the Apache patch. On July 30, 2017, Equifax observed further suspicious activity and took the web application offline. Three days later the company hired cybersecurity firm Mandiant to conduct a forensic investigation of the breach. The investigation revealed that the data of an additional 2.5 million U.S. consumers had been breached, bringing the total number of Americans affected to approximately 145.5 million. Equifax disclosed in the same [announcement](#) that 8,000 Canadians had been impacted and stated that the forensic investigation related to UK consumers had been completed, but did not state the amount of UK consumers affected. A later [announcement](#) from Equifax stated that the data of 693,665 UK citizens were breached.

## Equifax hacker vs Cybersecurity Standard

## Cybersecurity Standard wins



# eBay 2014 Breach

**Reason: Either local disclose or brute force. Employee password compromise**

**Intruder: Syrian Electronic Army**

eBay says the credential theft and database access occurred in late February and early March of 2014. The reason eBay didn't tell anyone before now, is because the company didn't know they had a problem. The unauthorized access was only recently discovered (early May 2014). The time between discovery and disclosure is rather short, which is a good thing.

**Information on eBay was not encrypted.**

[https://www.eecs.yorku.ca/course\\_archive/2014-15/W/3482/Team3\\_presentation.pdf](https://www.eecs.yorku.ca/course_archive/2014-15/W/3482/Team3_presentation.pdf)

**eBay hacker vs Cybersecurity Standard**

**Cybersecurity Standard wins**



# JP Morgan Chase 2014 Breach

**Reason: Remote access to an employee computer/Phishing**  
**Intruders: Russian, Israeli hackers**

"Employees often use software to tap into corporate networks from home through what are known as virtual private networks," the news report states. Chase reportedly has reset passwords used by every technology employee and disabled employee accounts that may have been compromised.

Since discovering the intrusion, some 200 employees across J.P. Morgan's technology and cybersecurity teams have worked to examine data on more than 90 servers that were compromised, sources told *The Journal*. And a core team, led by Chase's chief operating officer, Matt Zames, oversaw the bank's breach-response strategy, the paper reports.

**JP Morgan Chase hacker vs Cybersecurity Standard**

**Cybersecurity Standard wins**



# Capital One 2019 Breach

**Reason: Remote attack through misconfigured Web Application firewall**

**Intruders: Paige A. Thompson**

Court documents showed that Capital One didn't learn about the hack until July 17, 2019, when someone sent a message to the company's responsible disclosure email address with a link to the GitHub page. The page had been up since April 21, with the IP address for a specific server containing the company's sensitive data.

"Capital One quickly alerted law enforcement to the data theft – allowing the FBI to trace the intrusion," US Attorney Brian T. Moran said in a statement.

The GitHub page had Thompson's full name, as well as another page containing her resume. Court documents showed that on the resume, Thompson was listed as a systems engineer and was an employee at Amazon Web Services from 2015 to 2016. In a statement, Amazon said the former employee left the company three years before the hack took place.

<https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/>

**Capital One hacker vs Cybersecurity Standard**

**Cybersecurity Standard lost**



# Conclusion

**We live in a scary world.**

**Is there hope?**

**Maybe!**

**Here are my sources:**

**EDUCATION, KNOWLEDGE, VIGILANCE, CURIOSITY**



# Q&A session

We are here to answer your questions



# Thank you!

You can always reach us at [www.digitaledge.net](http://www.digitaledge.net)  
Find in LinkedIn = Michael Petrov; Digital Edge Ventures.