#MissionBeforeMoney

Class #3 – Chapters 3,4,5

Christophe Foulon

Founder CPF Coaching & vCISO

CISSP® MENTOR PROGRAM – SESSION THREE

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials. (pdf of book)**

CISSP® MENTOR PROGRAM – SESSION THREE

INTRODUCTION

Agenda –

- Welcome
- Introduction
- Questions
- Policies
- Business Continuity
- Personnel
- Third-party / Supply Chain controls
- Risk Management
- Security Awareness

CISSP® MENTOR PROGRAM – LEAD MENTOR INTRO

WHOAMI

Christophe Foulon

Founder CPF Coaching & vCISO

https://www.linkedin.com/in/christophefoulon/

https://substack.cpf-coaching.com/

CISSP® MENTOR PROGRAM – SESSION SIX

WHO I AM?

I love Baby Yoda

Outside of being a security practitioner focused on helping businesses tackle their cybersecurity risks while minimizing friction resulting in increased resiliency and helping to secure people and processes with a solid understanding of the technology involved.

I am a dad, dog dad and career coach. I love helping other to achieve their best. Through this channel, I help veterans with their transitions and others via non-profits like Whole Cyber Human Initiative, Boots2Books and others.

I give back by producing a podcast focused on helping people who are "Breaking into Cybersecurity" by sharing the stories of those who have done it in the past 5 years to inspire those looking to do it now.

Co-authored:
"Develop Your Cybersecurity Career Path: How to Break into Cybersecurity at Any Level"
"Hack the Cybersecurity Interview: A complete interview preparation guide for jumpstarting your cybersecurity career"
And advised on "Understand, Manage, and Measure Cyber Risk"

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Discord Channels
- Exercise or get fresh air in between study sessions

Let's get going!

CISSP® MENTOR PROGRAM – SESSION THREE

QUESTIONS.

The most common questions have been about:

- **About the Discord channel**
- Live session links.
- Instructor slide deck.

Because of the way Discord works and normal communications challenges, the Discord invite you received may have "expired". Email the FRSecure CISSP Mentor List (**cisspmentor@frsecure.com**) for a new invite.

CISSP® MENTOR PROGRAM – SESSION THREE

QUESTIONS.

The most common questions have been about:

- About the Discord channel
- **Live session links.**
- Instructor slide deck.

All LIVE session links will be sent by email on the same day as the LIVE session. If you have not received the live session link it's usually because the email went to your "Junk" folder (or similar).

CISSP® MENTOR PROGRAM – SESSION THREE

QUESTIONS.

The most common questions have been about:

- About the Discord channel
- Live session links.
- **Instructor slide deck.**

The instructor slide decks will be sent as soon as FRSecure receives them from the instructors. Sometimes the decks are not available until they teach. Whenever possible, we will try to send you the slide decks before each class.

CISSP® MENTOR PROGRAM – SESSION THREE

INTRODUCTION

Before we get too deep into this.

What's a hacker's favorite season?

Phishing season.

Yeah, I know. That's dumb.

Let's get to it…

CISSP® MENTOR PROGRAM – SESSION THREE

INTRODUCTION

Cornerstone Information Security Concepts

Definition of "**information security**" (don't forget):

Information security is managing risks to the **confidentiality**, **integrity**, and **availability** of information using **administrative**, **physical** and **technical** controls.

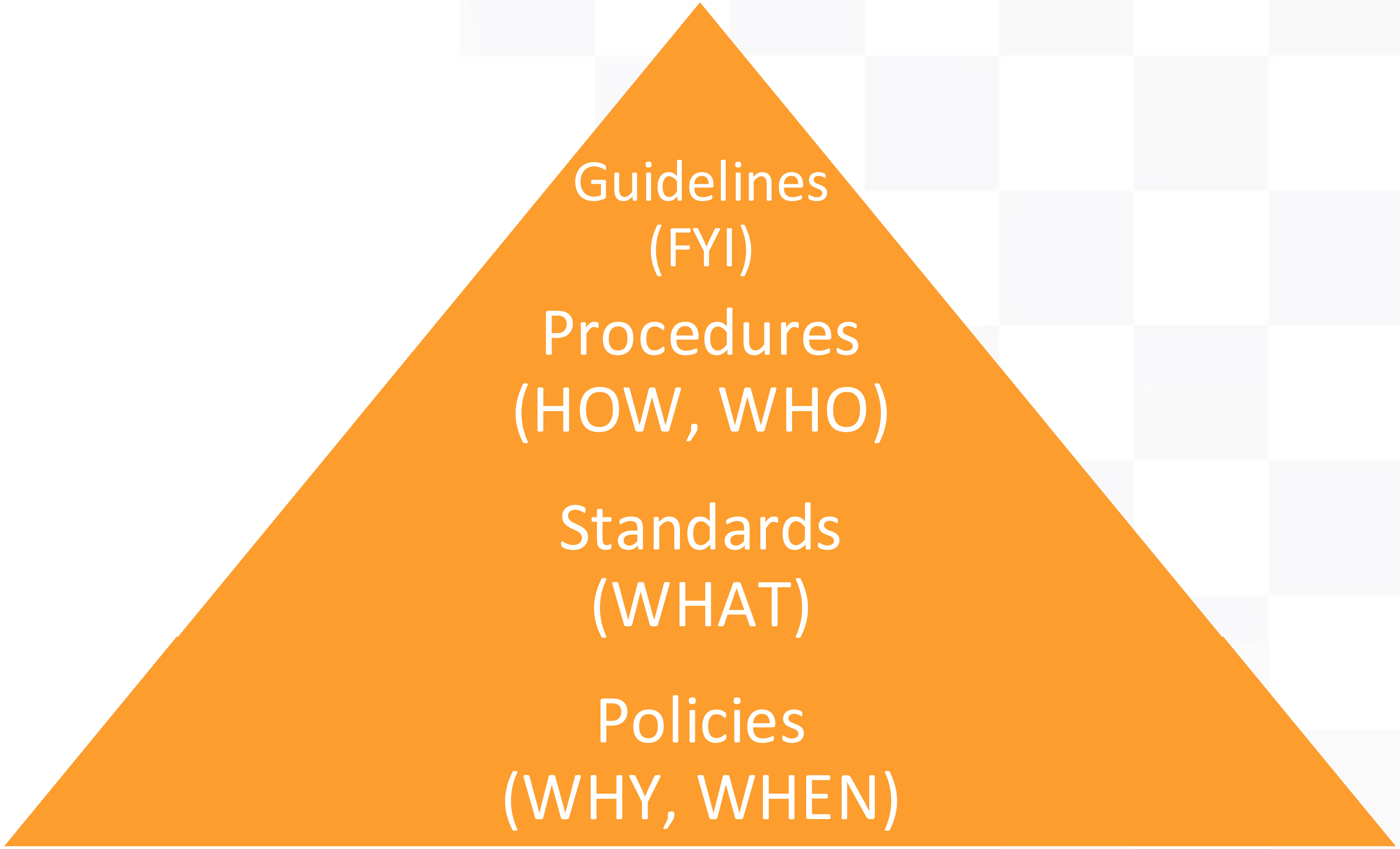
"Most organizations overemphasize technical controls to protect confidentiality and do so at the expense of other critical controls and purposes."

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Identify, Analyze and Prioritize Business Continuity Requirements

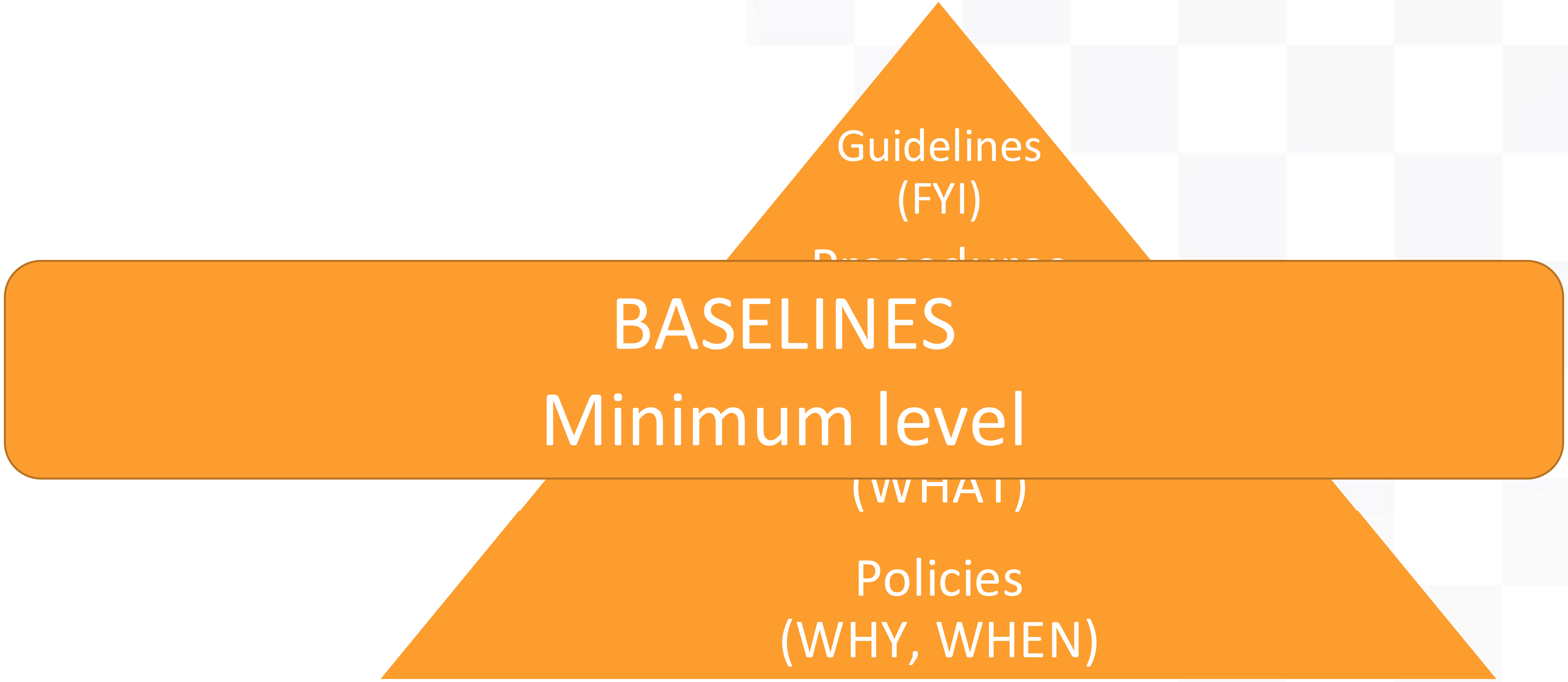


CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Identify, Analyze and Prioritize Business Continuity Requirements



Guidelines
(FYI)

Procedures

BASELINES

Minimum level

(WHAT)

Policies
(WHY, WHEN)

Chapter 3: Business Continuity Planning

Business Impact Analysis

Identify, Analyze and Prioritize Business Continuity Requirements

BCP Overview and Process

Business Continuity Planning and Disaster Recovery Planning are two very distinct disciplines

Business Continuity Planning (BCP)

- Goal of a BCP is for ensuring that the business will continue to operate before, throughout, and after a disaster event is experienced
- Focus of a BCP is on the **business as a whole**
- Business Continuity Planning provides a **long-term** strategy
- Accounting for items such as people, processes and technology in addition to critical systems and data

Chapter 3: Business Continuity Planning

Business Impact Analysis

Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Business Continuity Plan (BCP)—a long-term plan to ensure the continuity of business operations

Continuity of Operations Plan (COOP)—a plan to maintain operations during a disaster.

Disaster—any disruptive event that interrupts normal system operations

Disaster Recovery Plan (DRP)—a short-term plan to recover from a disruptive event (more in chapter 7)

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Critical Business Function (CBF)—Essential functions critical to the business operations

Business Impact Analysis (BIA)—Analyzing impact of an over time disruption

Maximum Tolerable Downtime (MTD)—Total length of time a critical business function can be unavailable

Maximum Acceptable Outage (MAO)—Total length of time a critical business function can be unavailable

Critical business function is anything the absence of would cause business to stop or be severely interrupted

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Recovery Time Objective (RTO)—Maximum time to restoration of minimum service expectations, must be less than or equal to MTD

Recovery Point Objective (RPO)—Tolerable amount of data loss in a time period

*not testable

OMG—The feeling you will have executing the BCP plan

FML—what you shout if you didn't print out the BCP plan

Chapter 3: Business Continuity Planning

Develop and Scope the Plan
Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Recovery Time Objective (RTO)—Maximum time to restoration of minimum service expectations, must be less than or equal to MTD

Recovery Point Objective (RPO)—Tolerable amount of data loss in a time period

*not testable

OMG—The feeling you will have executing the BCP plan

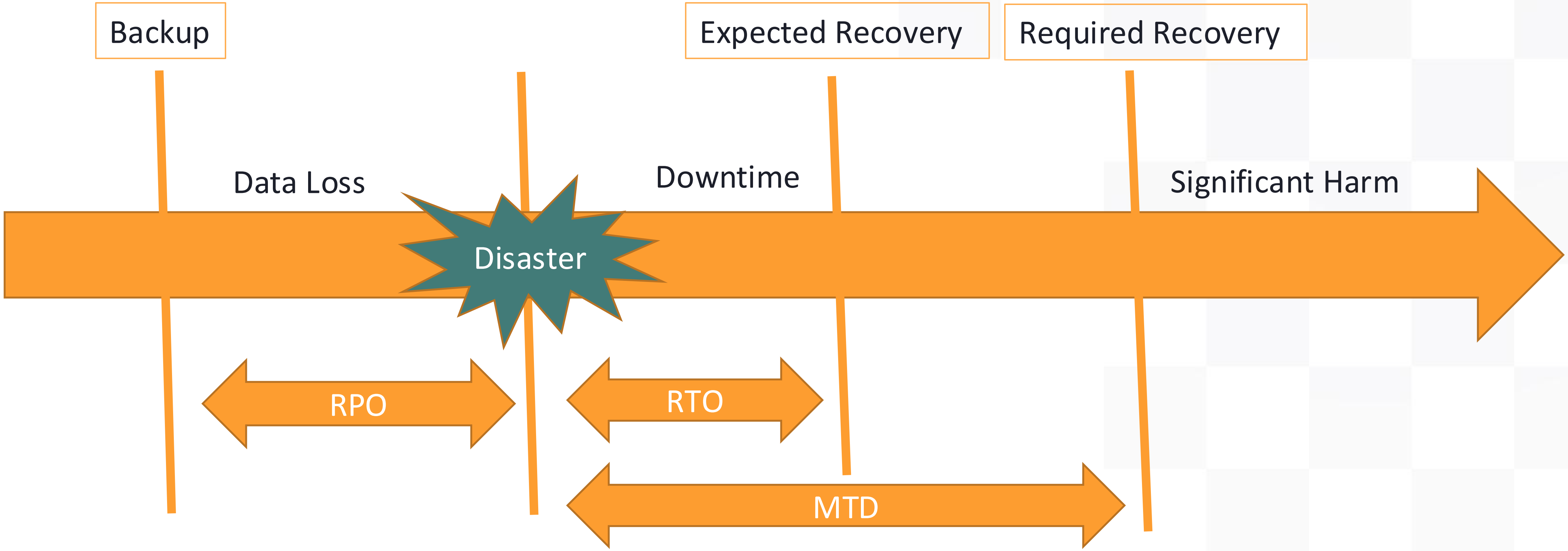
FML—what you shout if you didn’t print out the BCP plan

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements



Chapter 3: Business Continuity Planning

Information Security Governance

Identify, Analyze and Prioritize Business Continuity Requirements

Conduct Business Impact Analysis (BIA)

- Formal method for determining how a disruption to the IT system(s) of an organization will impact the organization
- An analysis to identify and prioritize critical IT systems and components
- Enables the BCP/DRP project manager to fully characterize the IT contingency requirements and priorities

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Management Support

“C”-level managers:

- Must agree to any plan set forth
- Must agree to support the action items listed in the plan if an emergency event occurs
- Refers to people within an organization like the chief executive officer (CEO), the chief operating officer (COO), the chief information officer (CIO), and the chief financial officer (CFO)
- Have enough power and authority to speak for the entire organization when dealing with outside media
- High enough within the organization to commit resources

Chapter 3: Business Continuity Planning

Develop and Scope the Plan
Identify, Analyze and Prioritize Business Continuity Requirements

Develop and Document the Scope and the Plan

- Define exactly what assets are protected by the plan, which emergency events the plan will be able to address, and determining the resources necessary to completely create and implement the plan
- “What is in and out of scope for this plan?”
- After receiving C-level approval and input from the rest of the organization, objectives and deliverables can be determined

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Scoping the Project

- Objectives are usually created as “if/then” statements
  - For example, “If there is a hurricane, then the organization will enact plan H—the Physical Relocation and Employee Safety Plan.” Plan H is unique to the organization but it does encompass all the BCP/DRP subplans required
  - An objective would be to create this plan and have it reviewed by all members of the organization by a specific date.
  - The objective will have a number of deliverables required to create and fully vet this plan: for example, draft documents, exercise planning meetings, table top preliminary exercises, etc.

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Scoping the Project

Executive management must at least ensure that support is given for three BCP/DRP items:

- 1. Executive management support is needed for **initiating** the plan.
- 2. Executive management support is needed for **final approval** of the plan.
- 3. Executive management must demonstrate due care and due diligence and be held liable under applicable laws/regulations.

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Example Scope

Critical business functions

Threats, vulnerabilities, and risks

Data backup and recovery plan

BCP personnel

Communications plan

BCP testing requirements

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

People

- **#1 Most important no exceptions (Life and safety above all else)**
- **Start with human safety then move on**
- **People = Any living human being that may be affected by the event**
- Notifications and communications, using multiple methods
- Resources to keep people working
  - Alternate work locations, food, equipment, internet, etc.
- Regular updates to leadership
- Notifications of external affected parties

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Processes

- What resources need to be available
- Critical supplies (computers, power, internet)
- How do we maintain critical operations
- Logistics
- Continuously available resources
- Recovery site (more in chapter 7)
  - Hot, Warm, Cold
- Testing and updating

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Other Roles

Continuity Planning Project Team (CPPT)

- Comprises those personnel that will have responsibilities if/when an emergency occurs
- Comprised of stakeholders within an organization
- Focuses on identifying who needs to play a role if a specific emergency event were to occur
- Includes people from the human resources section, public relations (PR), IT staff, physical security, line managers, essential personnel for full business effectiveness, and anyone else responsible for essential functions

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Technologies

- **Tech fails plan for it**
- Backups are the #1 way to address this risk
- BCP should account for redundancy (power, water, telco, internet)
- Multiple locations for backups (on-prem and cloud)
- Need to account for external disaster (ISP, Bank, SaaS provider, etc.)
- Testing and updating

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Technologies

- **Tech fails plan for it**
- Backups are the #1 way to address this risk
- BCP should account for redundancy (power, water, telco, internet)
- Multiple locations for backups (on-prem and cloud)
- Need to account for external disaster (ISP, Bank, SaaS provider, etc.)
- Testing and updating

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Technologies

- Why didn't the IT team set up their remote office from the beach?
  - It was too cloudy

Yeah, I know. That's dumb.

Let's get to it…

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Candidate Screening and Hiring

Contribute to and enforce personnel security policies and procedures

Humans are the biggest part of information security

- Clearly defined roles and job descriptions simplify security
- **Need process and procedure for verifying background**
  - Education, Work history, Citizenship, Criminal record, Credit and financial history, social media activity, and references
- More sensitive positions require further background investigation
- Have clear policies on the use of social media and business systems (appropriate use)
- Verify before granting access to sensitive data

Chapter 3: Business Continuity Planning

Employment Agreements and Policies

Contribute to and enforce personnel security policies and procedures

Employment agreements set the stipulations the employee must abide by

- Nondisclosure
- Non compete
- Code of conduct
- Conflict of interest
- Acceptable use
- Employment policies
- Equipment use
- At home expectations (remote worker)

Chapter 3: Business Continuity Planning

Onboarding, Transfers and Termination process

Contribute to and enforce personnel security policies and procedures

Each stage of employment comes with a security component

- Onboarding sets the tone for work behavior
- Processes for training on secure habits (security awareness)
- Additional training for employees who are likely targets of attackers (C-Level, Admins)
- Process for reporting security incidents (IMO #1)
- Roles and responsibility for securing their work area
- Data classification process and training
- Awareness of monitoring controls
- Their actions matter and make the difference (good or bad)

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Onboarding, Transfers and Termination process

Contribute to and enforce personnel security policies and procedures

Transfers

- Clearly defined process for role transfer
- Employee access review (Is current access needed for new role)
- Transition period clearly defined (when is it time to cut off access to previous role)
- Least privilege (enforce)
- Legacy needs (smaller orgs)
- Temporary access (helping out)

Chapter 3: Business Continuity Planning

Onboarding, Transfers and Termination process

Contribute to and enforce personnel security policies and procedures

Termination (Voluntary and Involuntary separation)

- Voluntary separation is a planned event (2 weeks, retire, good terms)
  - Use a standard checklist (equipment, access, keys, badges, changing codes)

- Involuntary separation is usually an unplanned event and **threat must be assumed**
- Moves very fast, being well coordinated with HR / manager is key
- It is **emotional for all involved**, respect that and plan for it
- When possible, recover any equipment and retain for **potential forensics**
- Remaining **staff need to be informed of termination** and loss of access (don't reset the password for Evan)
- Process for reporting attempted access by terminated employee
- *Insider threat program established and adhered to (UEBA can alert to a rage quit)

Chapter 3: Business Continuity Planning

Vendor, Consultant and Contractor Agreements and Controls

Contribute to and enforce personnel security policies and procedures

- Vendor, Consultant and Contractor agreements and controls
  - NDA's and other agreements should be in place to protect sensitive information
  - Policies that support monitoring and auditing of access by 3rd parties
  - Policies that require secure connections with 3rd parties who access sensitive data
- Compliance Policy Requirements
  - Ensure all employees are trained and periodical retrained on policies and regulations they need to comply with in the fulfilment of their job duties.
- Privacy Policy Requirements
  - Privacy policy should include what kind of personal data is collected, how it will or will not be used, how it will be stored, maintained, and secured.
- Review and signature by employee that they understand and will comply with company policies and regulations is common practice

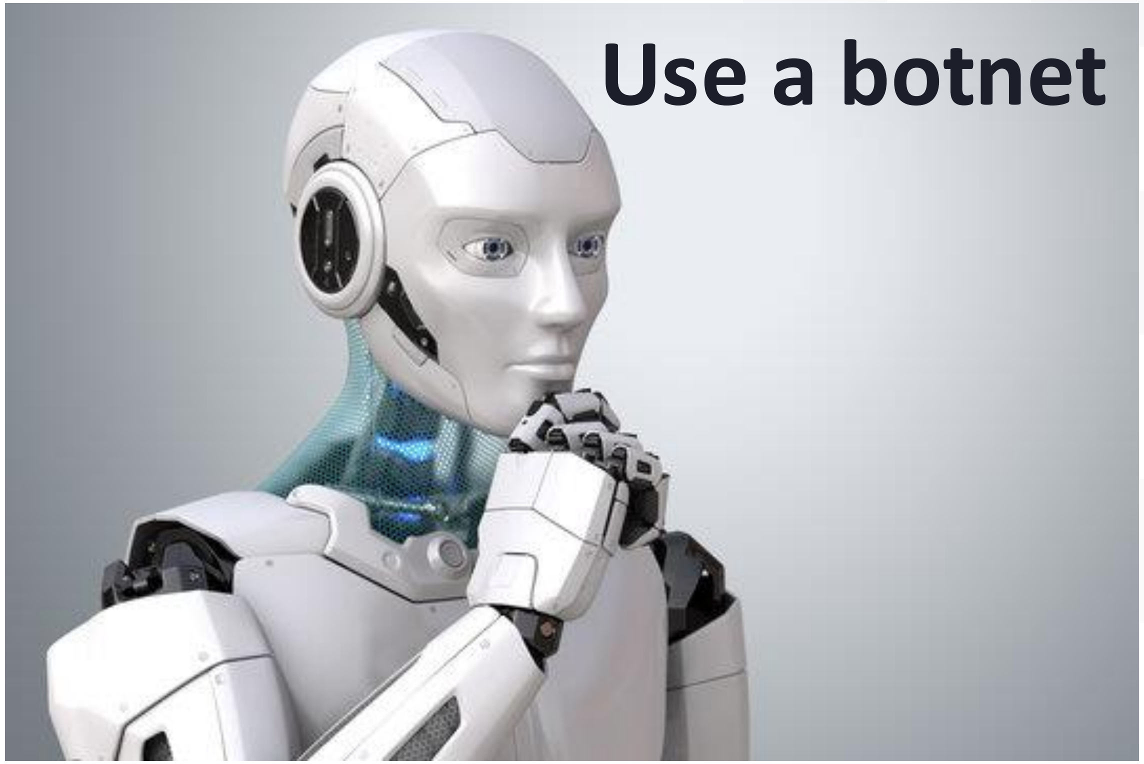
CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKE TIME

Whew that was a lot to take in.

How about a dumb dad joke?

What's the best way to catch a runaway robot?



Yeah, I know.
That's dumb.

Let's get to it…

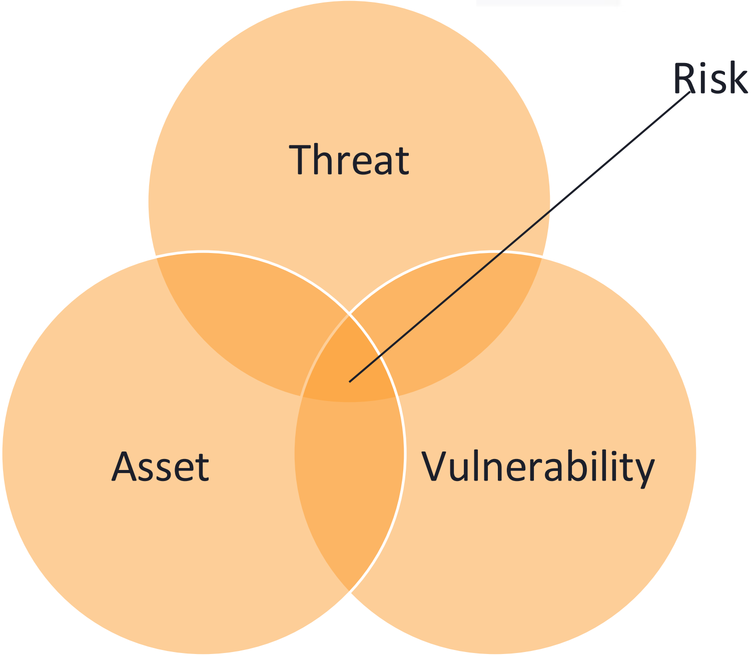
CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

- Risk management provides structure for making security decisions



Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Information Security IS RISK MANAGEMENT!!!

Unique terms and definitions

Risk—expose (someone or something valued) to danger, harm, or loss.

Inherent risk—risk present before any controls are applied.

Residual risk—level of risk that remains after controls are applied.

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Unique terms and definitions

Threats—Negative event leading to a negative outcome.

Examples:

- Fire or natural disaster.
- Disgruntled employee.
- Cybercriminal looking to ransom you.
- Click happy employee

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Unique terms and definitions

Vulnerabilities—Weakness or gap in a system that may be exploited.

Examples:

- Unpatched software applications (#1)
- Weak access control mechanisms (e.g., weak passwords)
- Faulty fire suppression system
- Security unaware employee

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Unique terms and definitions

Vulnerabilities—Weakness or gap in a system that may be exploited.

Examples:

- Unpatched software applications (#1)
- Weak access control mechanisms (e.g., weak passwords)
- Faulty fire suppression system
- Security unaware employee

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Unique terms and definitions

Assets—Anything of value.

- Value can be Quantitative (cost or market value of asset)
- Value can be Qualitative (relative importance to you or the organization)

CISSP® MENTOR PROGRAM – SESSION THREE

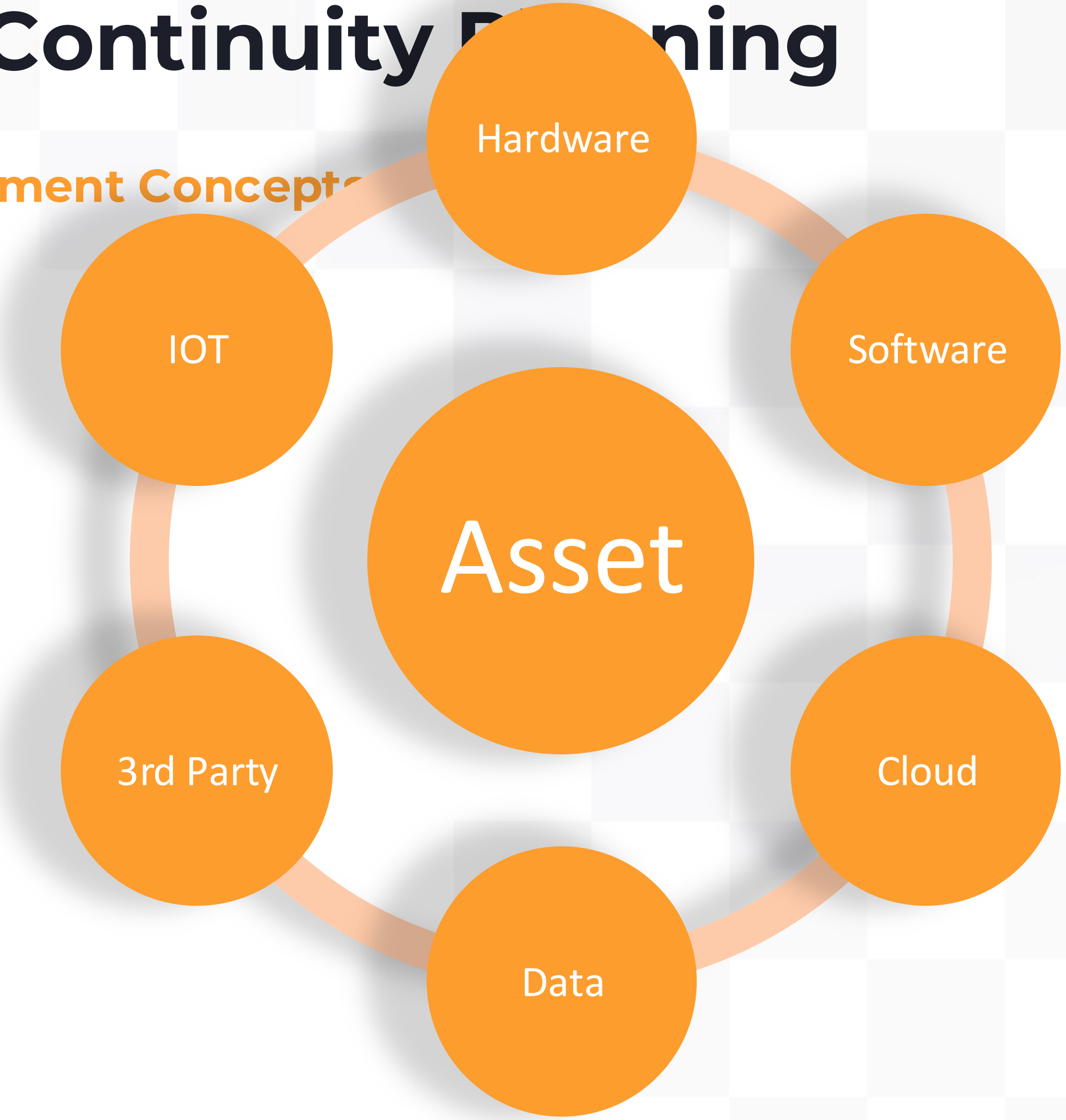
Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Unique terms and definitions

Assets—Anything of value.

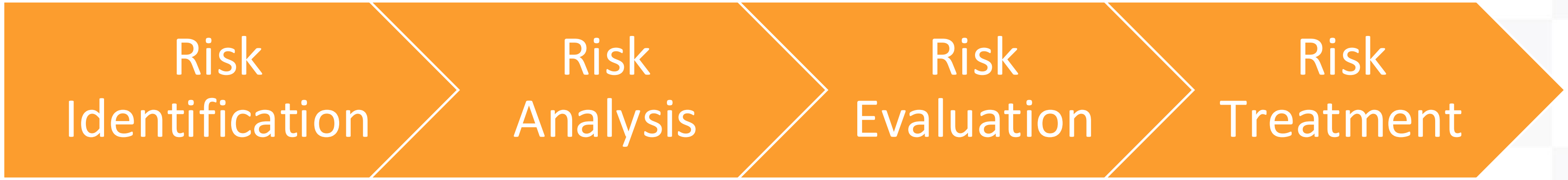


Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk assessments are the gateway to good security



*No such thing as Risk Elimination

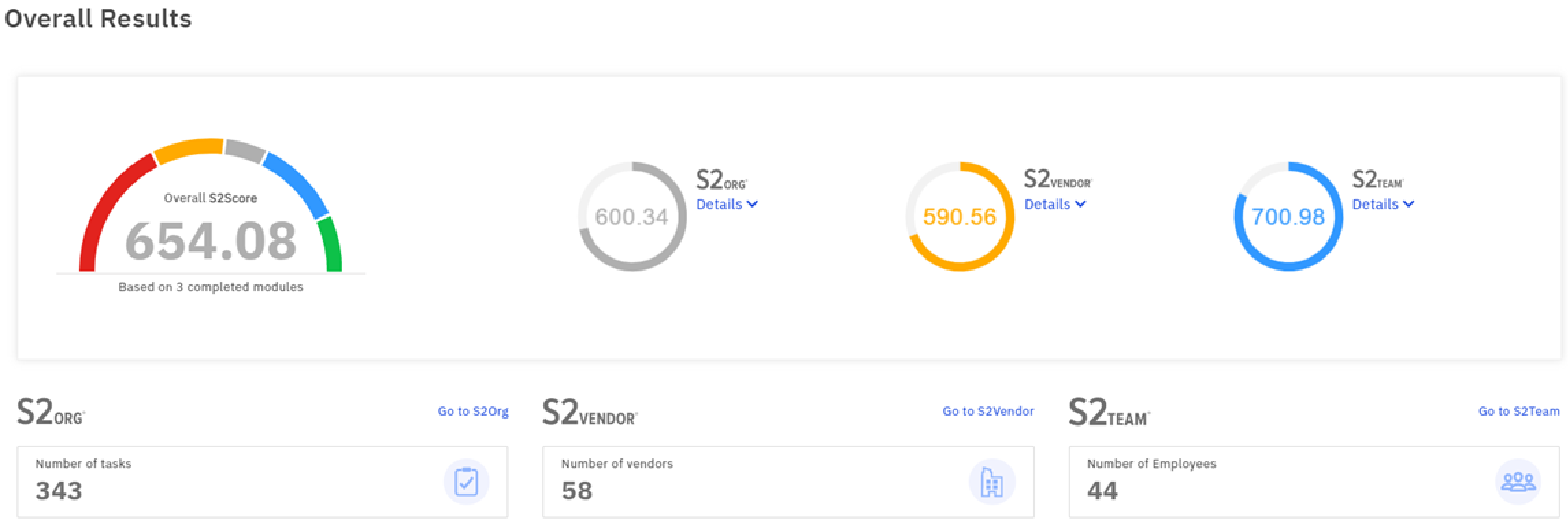
CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk assessments are the gateway to good security



Overall Results

Overall S2Score
654.08
Based on 3 completed modules

600.34 S2ORG Details

590.56 S2VENDOR Details

700.98 S2TEAM Details

S2ORG — Go to S2Org
Number of tasks
343

S2VENDOR — Go to S2Vendor
Number of vendors
58

S2TEAM — Go to S2Team
Number of Employees
44

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Identification

- Asset discovery (hardware, software, network, data, people)
- Asset valuation (business value of asset)
- Classification (how sensitive, how critical)
- Vulnerabilities and Threats to asset

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Analysis

Should begin with a vulnerability assessment (more in chapter 6) and threat analysis (more on this later in this chapter)

The goal of risk analysis is to evaluate how likely identified threats are to exploit weaknesses (i.e., vulnerabilities)

To make this evaluation we need to look at two key factors

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Analysis

Likelihood—Probability that event will occur.

Impact—How disastrous the event would be if it were to happen .

Risk = Threat x Vulnerability (likelihood and impact)

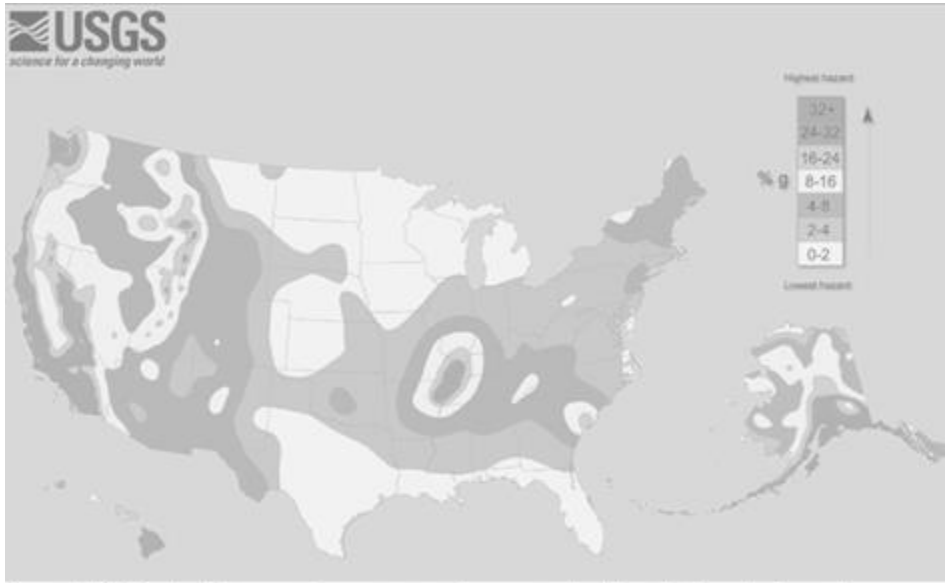
Risk = Threat × Vulnerability × Impact (another way to put it)

Human life trumps everything!

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts



Source: U.S. Geological survey/www.usgs.gov/programs/earthquake-hazards/hazards

USGS Earthquake hazards likelihood map, denoting where has the highest risk of earthquake.

Other times of hazards can also have similar analysis based on large amounts of data previously collected and analyzed, providing a % of change of a hazard happening.

Technology and capabilities change quickly, so attempting to predictions would depend on assumptions of which risk and the impact to the business, so it needs to be much more tailored.

Human life trumps everything!

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Risk Analysis

- **Qualitative** – based upon professional opinion; High, Medium, Low…
- **Quantitative** – based on real values; dollars. Pure quantitative analysis is nearly impossible (lack of data).
- **Risk Analysis Matrix** – Qualitative risk analysis table; likelihood on one side, impact on the other.

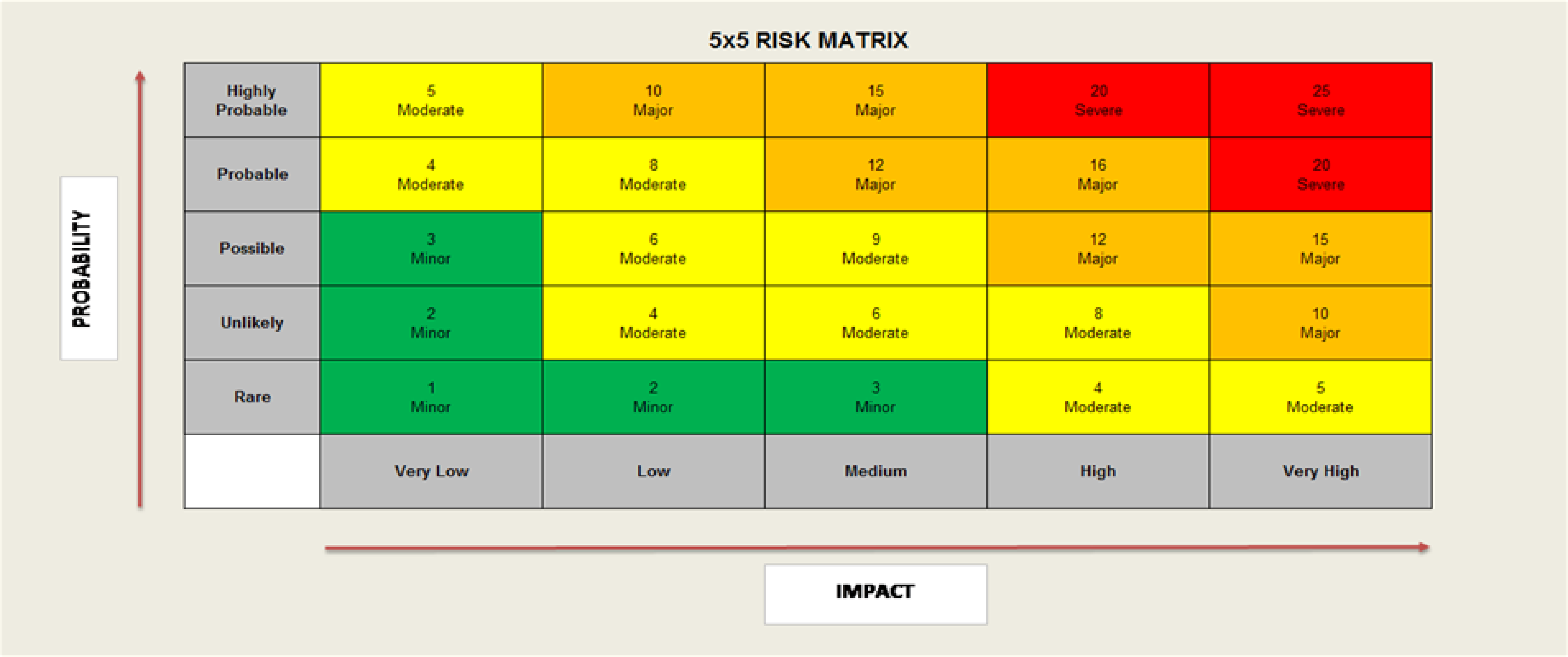
CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Analysis



5x5 RISK MATRIX

Highly Probable	5 Moderate	10 Major	15 Major	20 Severe	25 Severe
Probable	4 Moderate	8 Moderate	12 Major	16 Major	20 Severe
Possible	3 Minor	6 Moderate	9 Moderate	12 Major	15 Major
Unlikely	2 Minor	4 Moderate	6 Moderate	8 Moderate	10 Major
Rare	1 Minor	2 Minor	3 Minor	4 Moderate	5 Moderate
	Very Low	Low	Medium	High	Very High

PROBABILITY
IMPACT

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Qualitative & Quantitative Risk Analysis

- **Quantitative** – based on real values; dollars. Pure **Qualitative** analysis is nearly impossible (lack of data).
- **Asset Value (AV)** – Fair market value for an asset
- **Exposure Factor (EF)** - % of asset lost during an incident (threat occurrence)
- **Single Loss Expectancy (SLE)** – **AV** x **EF**
- **Annual Rate of Occurrence (ARO)** – How many times a bad thing is expected/year.
- **Annualized Loss Expectancy (ALE)** – **SLE** x **ARO**

If ALE exceeds Total Cost of Ownership (TCO), there is a positive Return on Investment (ROI), or Return on Security Investment (ROSI).

CISSP® MENTOR PROGRAM – SESSION THREE

INTRODUCTION

Terms and Definitions to Memorize

- **Risk** – The likelihood of something bad happening and the impact if it did; threats (source) and vulnerabilities (weakness)
- **Annualized Loss Expectancy (or ALE)** - the cost of loss due to a risk over a year
- **Safeguard (or “control”)** - a measure taken to reduce risk
- **Total Cost of Ownership (or TCO)** – total cost of a safeguard/control
- **Return on Investment (or ROI)** - money saved by deploying a safeguard

Another term is Return on Security Investment or “ROSI”.

CISSP® MENTOR PROGRAM – SESSION THREE

INTRODUCTION

Terms and Definitions to Memorize

- **Risk** – The likelihood of something bad happening and the impact if it did; threats (sour ness)
- **Annualized Loss** st of loss due to a risk over a year
- **Safeguard (or “c** reduce risk
- **Total Cost of Ow** t of a safeg
- **Return on Invest** by deployi

Another term is ent or “R

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Risk Response / Treatment

Understand and Apply Risk Management Concepts

Unique terms and definitions

Risk Tolerance—How much risk the organization is willing to take on.

Risk Profile—How much risk the organization is willing to take on.

Risk Treatment—Best way to address the risk.

Risk Response—Best way to address the risk.

Chapter 3: Business Continuity Planning

Risk Response / Treatment

There are only four; risk acceptance criteria should be documented. Risk decisions should **ALWAYS** be made by management, **NOT** information security.

- **Accept** – the risk is acceptable without additional control or change.
- **Mitigate** – the risk is unacceptable (to high) and requires remediation. *(Most common)*
- **Transfer** – the risk can be transferred to someone else; 3rd-party provider, insurance.
- **Avoid** – the risk will be avoided by discontinuing the action(s) that led to the risk.

Chapter 3: Business Continuity Planning

Countermeasure Selection and Implementation (Security Controls)

Risk mitigation involves ONE or MORE countermeasures with the goal of reducing the likelihood of an adverse event.

- **Personnel-related** – Hiring, Roles, Awareness training.
  - People are the #1 Security risk and #1 Security control
- **Process-related** – Policy, procedure, and workflow-based
  - Separation of duties, dual control
- **Technology-related** – Most of the attention.
  - Encryption, configuration settings, hardware, software, change detection.

Chapter 3: Business Continuity Planning

Personnel Security Considerations

- Security Awareness and Training
  - Actually two different things
  - Training teaches specific skills
  - Awareness activities are reminders
- Background Checks
  - Criminal history, driving records, credit checks, employment verification, references, professional claims, etc.
  - More sensitive roles require more thorough checks; one-time and ongoing
- Employee Termination
  - Formalized disciplinary process (progressive)
  - Exit interviews, rights revocation, account reviews, etc.
- Dealing with Vendors, Contractors, 3rd Parties
- Outsourcing and Offshoring

Information security isn't about information or security…

As much as it is about people.

1. If people didn't suffer when things go wrong, nobody would (or should) care.

2. People are the most significant risk

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Risk Response / Treatment

Understand and Apply Risk Management Concepts

Unique terms and definitions

Security-Effectiveness—How effective are the controls selected in addressing the specific risk, and are the controls inline with the kind of security risk your addressing (prevent, detect, or correct)

Cost-Effectiveness—is calculated by performing a cost benefit analysis comparing cost of countermeasure(s) to the cost the would be realized by a compromise of the risks the countermeasures are intended to mitigate.

Chapter 3: Business Continuity Planning

Risk Response / Treatment

Understand and Apply Risk Management Concepts

ALE from ransomware event = $200,000

Countermeasure of backups = $50,000

Value added to organization = $150,000

*Countermeasures generally have ongoing costs to factor

Chapter 3: Business Continuity Planning

Operational Impact

Understand and Apply Risk Management Concepts

- Determine organizational objective, denoting statements of importance and priorities.
- Countermeasures must be evaluated for impact to the organization
- Difficult to implement or use countermeasures increases risk
- People will circumvent difficult countermeasures
- Understanding culture and strategy is important to selecting countermeasures that don't have a negative operational impact

*Culture and strategy alignment, are a countermeasures best friend

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 3: Business Continuity Planning

Applicable Types of Controls

- Categories
  - Administrative Controls
  - Technical Controls
  - Physical Controls
- Types
  - Preventive
  - Detective
  - Corrective
  - Recovery
  - Deterrent
  - Compensating

See! Also in our definition.

VERY TESTABLE: you may be given a scenario or control description and need to provide the category and type.

In order to be sure of the control type, you need to clearly understand context.

Chapter 3: Business Continuity Planning

Applicable Types of Controls

- Types
  - **Preventive** – First line controls (firewall, validation, training)
  - **Detective** – Identify negative security event (alarm, IDS, audit)
  - **Corrective** – Minimize and repair damage
    (patching, config management, new or updated policies)
  - **Recovery** – Return to normal ASAP (backups, DR plans)
  - **Deterrent** – Discourage (generally policy, and physical measures)

  - ***Compensating** – Put in place to satisfy a security requirement deemed to difficult or impractical to implement at the present time.
    Not a full mitigation of risk (**encourage vs enforce**)

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKE TIME

Whew that was a lot to take in.

How about a dumb dad joke?

Yeah, I know. That's dumb.

Let's get to it…

We all know about Murphy's Law: anything that can go wrong will go wrong.

But have you heard of Cole's Law?

It's thinly sliced cabbage

Chapter 4: Laws, Regulations, and Compliance

Foundation: This area establishes the legal and ethical bedrock for all security activities.

"Rules of the Game": It encompasses laws, regulations, industry standards, and internal policies that govern information protection.

Beyond Technical: It's not solely about technology; it's about the legal and organizational context of security.

Risk of Ignoring: Neglecting compliance creates significant legal, financial, and reputational risks.

Key Objective: Understanding and adhering to these mandates ensures lawful, ethical, and responsible security practices.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Criminal Law: Deals with actions considered harmful to society as a whole. Violations can lead to prosecution by the state and penalties like fines or imprisonment. Examples in cybersecurity include laws against hacking (like the Computer Fraud and Abuse Act - CFAA in the US) and data theft.

Civil Law: Concerns disputes between individuals or organizations where one party claims harm caused by another. Remedies often involve monetary compensation. In cybersecurity, this could relate to data breaches leading to lawsuits for damages.

Administrative Law: Governs the activities of administrative agencies of the government. These agencies create and enforce regulations. Examples include data protection authorities enforcing privacy regulations like GDPR or the Federal Trade Commission (FTC) in the US issuing rules related to data security.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Regulatory Laws/Regulations: These are specific rules or requirements established by governmental bodies or industry organizations to ensure compliance in particular sectors. Examples include HIPAA for healthcare, GLBA for financial institutions, and PCI DSS for organizations handling credit card information.

Privacy Laws: Focus on protecting the rights of individuals regarding their personal information. These laws dictate how organizations can collect, use, store, and disclose personal data. Examples include **GDPR**, **CCPA** (California Consumer Privacy Act),and various national privacy laws.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Intellectual Property (IP) Laws: Protect creations of the mind. In cybersecurity, this includes:

- **Copyright:** Protects original works of authorship (e.g., software code, documentation). Digital Millennium Copyright Act of 1998.
- **Patents:** Protect inventions (e.g., algorithms, security mechanisms).
- **Trademarks:** Protect brand names and logos.
- **Trade Secrets:** Protect confidential information that provides a business competitive edge.

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Contract Law: Governs agreements between parties. Security requirements are often included in contracts with vendors, customers, and employees (e.g., Non-Disclosure Agreements - NDAs).

International Laws and Treaties: Address legal matters that transcend national borders, including data transfer agreements and cybercrime conventions.

Industry-Specific Regulations: Certain industries have their own specific compliance requirements beyond general laws (e.g., NERC CIP for the energy sector).

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Cybercrime refers to any illegal activity that involves a computer, computer system, or a computer network. It encompasses a wide range of malicious activities conducted in the digital space, often with the intent to harm individuals, organizations, or even nations. Understanding the different facets of cybercrime is crucial for developing effective security strategies and ensuring compliance with relevant laws.

Definition and Scope:

- There isn't one single, universally agreed-upon definition, but generally, it includes crimes where a computer is the tool (used to commit traditional crimes) or the target (of the criminal activity itself).
- It can range from individual acts to highly organized criminal enterprises and even state-sponsored activities.
- The borderless nature of the internet makes cybercrime particularly challenging to investigate and prosecute, often requiring international cooperation

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Motivations Behind Cybercrime:

- **Financial Gain:** This is a primary driver, including theft of money, financial data (credit card information, bank account details), and intellectual property for resale.
- **Espionage:** Nation-states or organizations may engage in cyber espionage to gather sensitive information for political, economic, or military advantage.
- **Disruption and Damage:** Some cybercriminals aim to disrupt services, damage critical infrastructure, or destroy data for ideological reasons, revenge, or simply to cause chaos.
- **Political Activism (Hacktivism):** Individuals or groups may use cyberattacks to promote a political agenda or protest against certain entities.
- **Personal Gain:** This can include cyberstalking, harassment, or the theft of personal information for identity theft.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Common Types of Cybercrime:

- **Hacking (Unauthorized Access):** Gaining unauthorized entry into computer systems or networks to steal data, disrupt operations, or install malware. Laws like the **Computer Fraud and Abuse Act (CFAA)** in the US address this.
- **Malware Attacks:** Using malicious software (viruses, worms, Trojans, ransomware, spyware) to damage systems, steal data, or extort money. Ransomware, which encrypts data and demands payment for its release, is a significant threat.
- **Phishing and Social Engineering:** Deceiving individuals into revealing sensitive information (passwords, financial details) through fraudulent emails, websites, or other communication methods.
- **Denial-of-Service (DoS)** and **Distributed Denial-of-Service (DDoS) Attacks:** Overwhelming a target system with traffic to make it unavailable to legitimate users, often used for extortion or disruption.

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

- **Identity Theft:** Stealing and using someone else's personal information for fraudulent purposes. The Identity Theft and Assumption Deterrence Act in the US addresses this.
- **Intellectual Property Theft and Piracy:** Illegally copying and distributing copyrighted material (software, music, movies) or stealing trade secrets.
- **Online Fraud and Scams:** A wide range of deceptive practices conducted online, including e-commerce fraud, investment scams, and advance-fee schemes.
- **Cyberstalking and Harassment:** Using electronic communication to harass, threaten, or intimidate individuals.
- **Child Sexual Abuse Material (CSAM) and Online Grooming:** The creation, distribution, and possession of CSAM, as well as online communication aimed at exploiting children.
- **Cryptojacking:** Secretly using someone else's computing resources to mine cryptocurrency.
- **Business Email Compromise (BEC):** Sophisticated scams targeting businesses to fraudulently transfer funds.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

- **Export Controls:** Regulations on transferring specific tech/data internationally for national security.
  - **ITAR:** State Dept. controls defense articles (USML) - impacts military cybersecurity. Strict.
  - **EAR:** Commerce Dept. controls dual-use items (CCL) - broader impact on commercial security tech.
  - **DFARS:** DoD rules for contractors handling defense info (CDI) - mandates specific security.
  - **Countries of Concern:** Nations with restrictions due to security/policy risks - stricter export rules apply.
    - https://www.pillsburylaw.com/en/news-and-insights/doj-data-security-program-compliance-guide.html

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Privacy laws & Regulations

- **Privacy Act of 1974:** Governs how federal agencies collect, use, and disclose individuals' personal information; establishes rights for individuals to access and amend their records.
- **Electronic Communications Privacy Act (ECPA) of 1986:** Extends wiretap laws to electronic communications (email, data); restricts government interception of these communications.
- **Communications Assistance For Law Enforcement Act (CALEA) of 1994:** Requires telecommunications carriers and equipment manufacturers to build in capabilities for law enforcement to conduct surveillance.
- **Economic Espionage Act of 1996:** Criminalizes the theft of trade secrets for the benefit of foreign powers or for commercial advantage.
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996:** Protects the privacy and security of Protected Health Information (PHI) for healthcare providers, insurers, and related entities.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Privacy laws & Regulations

- **Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009:** Strengthened HIPAA rules, increased penalties for violations, and promoted the adoption of electronic health records.
- **Children's Online Privacy Protection Act (COPPA) of 1998:** Requires websites and online services to obtain verifiable parental consent before collecting personal information from children under 13.
- **Gramm-Leach-Bliley Act (GLBA) of 1999:** Requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data.
- **USA PATRIOT Act of 2001:** Expanded government surveillance powers in response to terrorism; some provisions have raised privacy concerns.
- **Clarifying Lawful Overseas Use of Data (CLOUD) Act:** Allows US law enforcement to compel US-based providers to disclose electronic communications data, even if stored on servers outside the US.

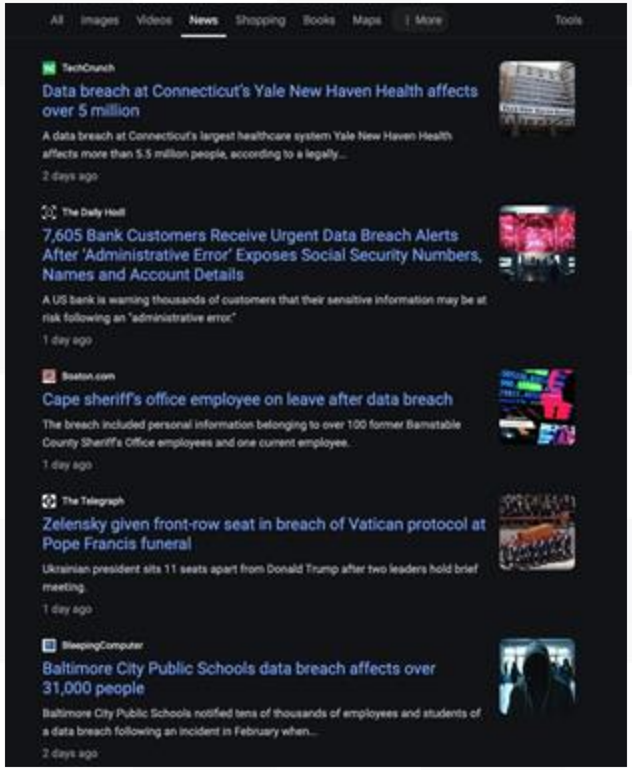
Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Privacy laws & Regulations

- **Family Educational Rights and Privacy Act (FERPA):** Protects the privacy of student educational records; gives parents and eligible students certain rights regarding these records.
- **Identity Theft and Assumption Deterrence Act:** Makes identity theft a federal crime and strengthens penalties for those who steal and misuse personal information.

Data Breaches: Security incidents that result in the unauthorized access and disclosure of sensitive information. This can lead to legal liabilities under privacy laws.



TechCrunch
Data breach at Connecticut's Yale New Haven Health affects over 5 million
A data breach at Connecticut's largest healthcare system Yale New Haven Health affects more than 5.5 million people, according to a legally...
2 days ago

The Daily Hodl
7,605 Bank Customers Receive Urgent Data Breach Alerts After 'Administrative Error' Exposes Social Security Numbers, Names and Account Details
A US bank is warning thousands of customers that their sensitive information may be at risk following an "administrative error."
1 day ago

Boston.com
Cape sheriff's office employee on leave after data breach
The breach included personal information belonging to over 100 former Barnstable County Sheriff's Office employees and one current employee.
1 day ago

The Telegraph
Zelensky given front-row seat in breach of Vatican protocol at Pope Francis funeral
Ukrainian president sits 11 seats apart from Donald Trump after two leaders hold brief meeting.
1 day ago

BleepingComputer
Baltimore City Public Schools data breach affects over 31,000 people
Baltimore City Public Schools notified tens of thousands of employees and students of a data breach following an incident in February when...
2 days ago

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Privacy laws & Regulations

- GDPR: General Data Protection Regulation
  - Broad European Union scope, strong individual rights, strict consent, data minimization, security, accountability, breach notification, high fines.
  - Cross-border: Adequacy decisions or safeguards (Standard Contractual Clauses, Binding Corporate Rules[BCD]) needed for transfers.
  - BCRs: Internal rules for multinational data transfers within their group.
- PIPEDA: Personal Information Protection and Electronic Documents Act (Canada)
  - Focused on Private sector in Canada (commercial activities).
  - Ten fair information principles, generally requires consent. Accountability for transferred data.

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Privacy laws & Regulations

PIPL: Personal Information Protection Law (China)

- Processing personal info in China (and some extraterritorial).
- Strong consent (especially for sensitive data and transfers), individual rights, data localization/transfer rules, Data Protection Impact Assessments, Data Protection Officer may be required, significant penalties, state control.

South Africa's Protection of Personal Information Act (POPIA)

- POPIA establishes eight conditions that organizations must adhere to when processing personal information. These include accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation.

Chapter 4: Laws, Regulations, and Compliance

Control Assessments

Understand and Apply Risk Management Concepts

Examine – Inspecting, reviewing, observing, studying or analyzing assessment objects.(specifications, mechanisms or activities)

Interview – Talking to people for clarity and obtaining evidence provided during the examine phase.

Test – Comparing actual with expected behavior of the security control, confirming security controls are implemented as they are documented and operating effectively as intended.

Monitoring and Measurement –periodic measuring of security control effectiveness and health (ongoing, annual or quarterly)

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Common Types of Software licenses:

Proprietary/Commercial Licenses: Software owned by a specific company or individual. Users typically pay a fee for the right to use it, often with restrictions on modification, distribution, and reverse engineering. Examples include Microsoft Windows and Adobe Photoshop. These licenses often come with End-User License Agreements (EULAs) that detail permitted uses.

Open Source Licenses: Grant users the freedom to run, study, distribute, and modify the software. These licenses vary in their specific terms, particularly regarding the requirement to share modifications (copyleft vs. permissive). Examples include the GNU General Public License (GPL), MIT License, and Apache License 2.0. Open source fosters collaboration and transparency.

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 4: Laws, Regulations, and Compliance

Types of Laws & Regulations

Common Types of Software licenses:

Freeware Licenses: Software provided free of charge, but often with restrictions on modification, distribution, and commercial use. The copyright is usually retained by the developer. While free to use, it's not necessarily open source. Examples include some utilities or older software versions.

Shareware Licenses: Software provided for free for a trial period. After the trial, users are typically required to pay a fee to continue using it. It's a "try before you buy" model. Restrictions on full functionality may apply during the trial.

Public Domain: Software where the copyright has been explicitly waived by the author, or has expired. It can be used, modified, and distributed by anyone for any purpose without restrictions. This is the most permissive type of software licensing.

Chapter 4: Laws, Regulations, and Compliance

Control Assessments

Understand and Apply Risk Management Concepts

Examine – Inspecting, reviewing, observing, studying or analyzing assessment objects.(specifications, mechanisms or activities)

Interview – Talking to people for clarity and obtaining evidence provided during the examine phase.

Test – Comparing actual with expected behavior of the security control, confirming security controls are implemented as they are documented and operating effectively as intended.

Monitoring and Measurement –periodic measuring of security control effectiveness and health (ongoing, annual or quarterly)

Chapter 4: Laws, Regulations, and Compliance

Reporting

Understand and Apply Risk Management Concepts

- Process to report to leadership, regulators, and other stakeholders – Important discoveries or metrics
- Specific reporting requirements (DHS, Legal, Regulatory, Industry specific)
- A well managed risk-based security program has reporting on
- Internal audits (self assessment)
- External audits (regulators or any other third-party audits)
- Significant changes to organization's risk posture
- Significant changes to security or privacy controls
- Suspected or confirmed security incidents (or breaches)

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 4: Laws, Regulations, and Compliance

Continuous Improvement

Understand and Apply Risk Management Concepts

Strive to improve efficiency of security management program. Seek to continuously improve the ROI associated with security.

Risk maturity modeling assess strength of security program. and informs plans for continuous improvement.

Using a predefined scale helps with focus on specific behavior to improve vs getting caught up in individual security gaps.

S2 Scoring…

S2SCORE

SEASON 2

Loki

82% TOMATOMETER 140 Reviews

74% AUDIENCE SCORE 1,000+ Ratings

Not secure enough
Too much risk

Too much security
Burdensome

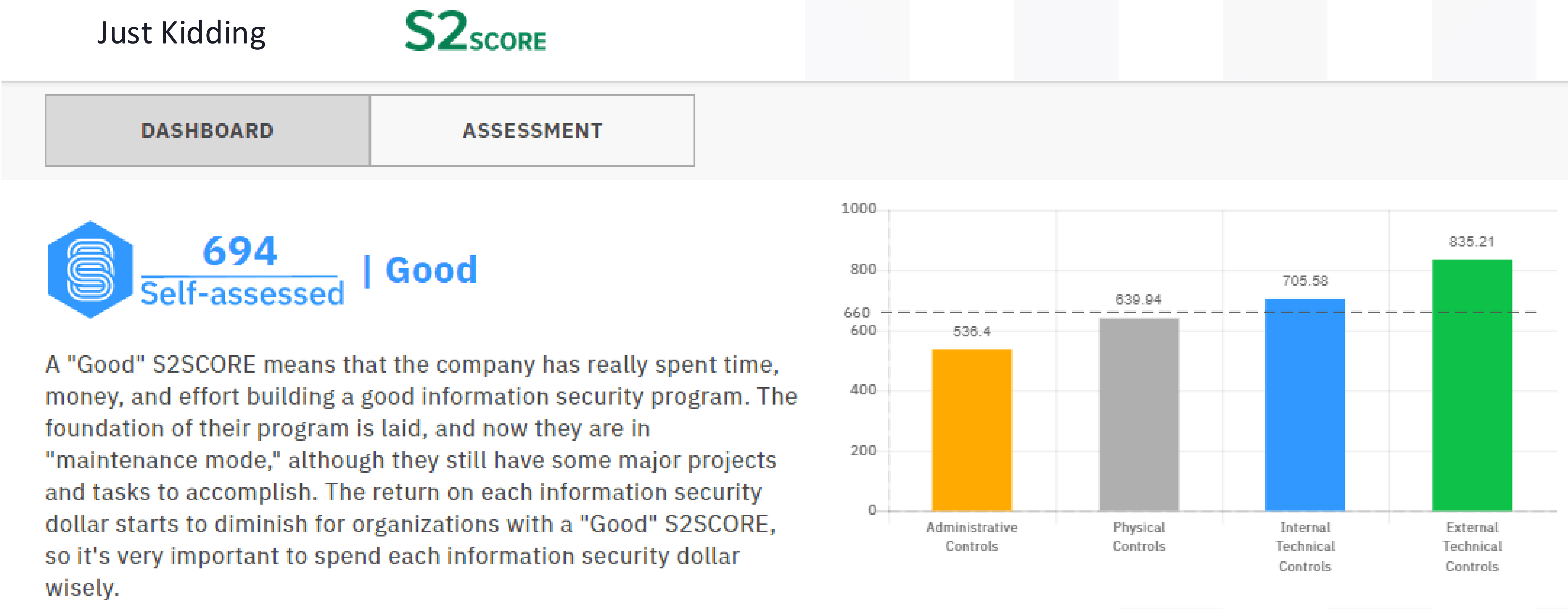
CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 4: Laws, Regulations, and Compliance

Continuous Improvement

Understand and Apply Risk Management Concepts

Just Kidding



A "Good" S2SCORE means that the company has really spent time, money, and effort building a good information security program. The foundation of their program is laid, and now they are in "maintenance mode," although they still have some major projects and tasks to accomplish. The return on each information security dollar starts to diminish for organizations with a "Good" S2SCORE, so it's very important to spend each information security dollar wisely.

Chapter 4: Laws, Regulations, and Compliance

Risk frameworks governance considerations

Understand and Apply Risk Management Concepts

- **Consistent** (same way)
- **Measurable** (progress and goals)
- **Standardized** (meaningful comparisons)
- **Comprehensive** (cover the minimum and be extensible)
- **Modular** (withstand change, only modify what you need)

CISSP® MENTOR PROGRAM – SESSION THREE

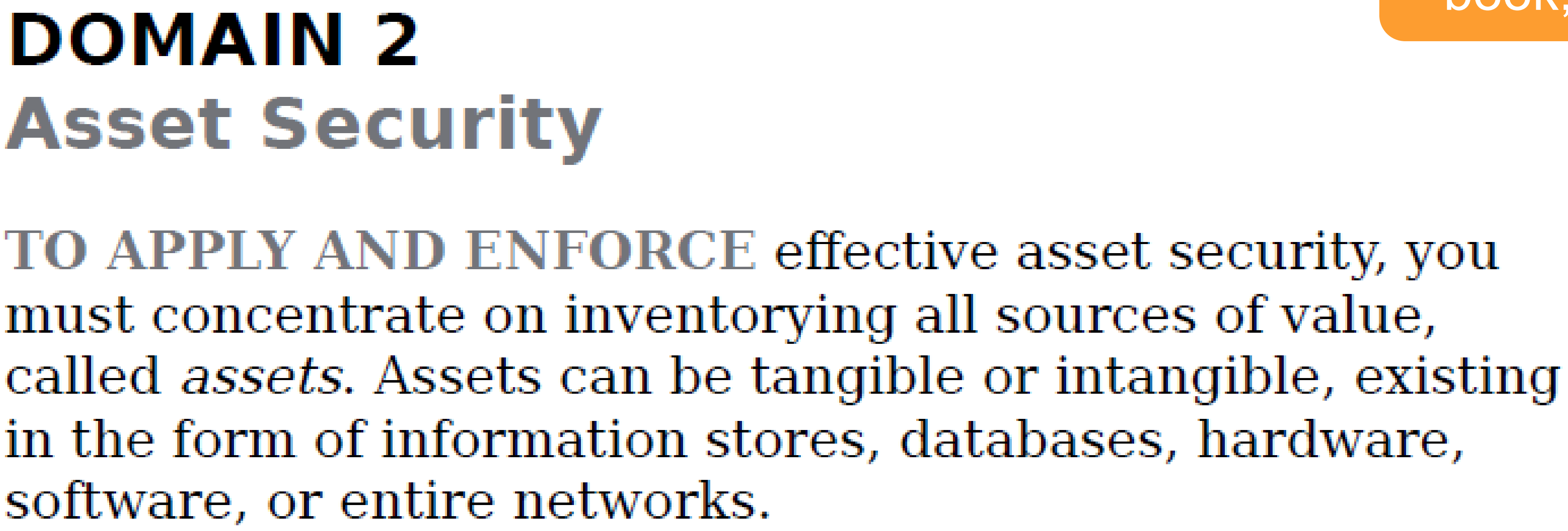
Chapter 4: Laws, Regulations, and Compliance

Risk frameworks

Understand and Apply Risk Management Concepts

Chapter 5: Protecting Security of Assets

You read the book, right?



DOMAIN 2
Asset Security

TO APPLY AND ENFORCE effective asset security, you must concentrate on inventorying all sources of value, called *assets*. Assets can be tangible or intangible, existing in the form of information stores, databases, hardware, software, or entire networks.

Chapter 5: Protecting Security of Assets

Risk frameworks

Understand and Apply Risk Management Concepts

- International Standards Organization
  - ISO 31000:2018 is intended to be applicable to all
  - There are eight principals
  - ISO 31004 guidance on implementing ISO 31000:2018
  - ISO 31000 series address general risk, information security practices are addressed in ISO 27000 series
  - ISO 27005 does not provide a risk assessment practice
    - ISO 27005 provides Inputs to, and outputs from the risk assessment practice used by the organization

IDENTIFY and CLASSIFY INFORMATION and ASSETS

- A mature security program begins with **asset identification and classification**
- Allows you to **locate** and **categorize your assets** and
- **Differentiate** the **security approaches** for each of them.
- *Having a current and complete inventory is the absolute bedrock for implementing and monitoring technical security controls.*

ASSET INVENTORY

More about this later

- WHAT
  - **Hardware** (Servers, Equipment, Devices, Endpoints, etc.)
  - **Software** (Applications)
  - **Data** ** Hardest…
- WHERE
  - **Location**(s) – Physical and virtual
  - Document - **Network Diagrams** and **Data Maps**
- WHO
  - **Responsibilities** (Business & IT)

Chapter 5: Protecting Security of Assets

Data Lifecycle

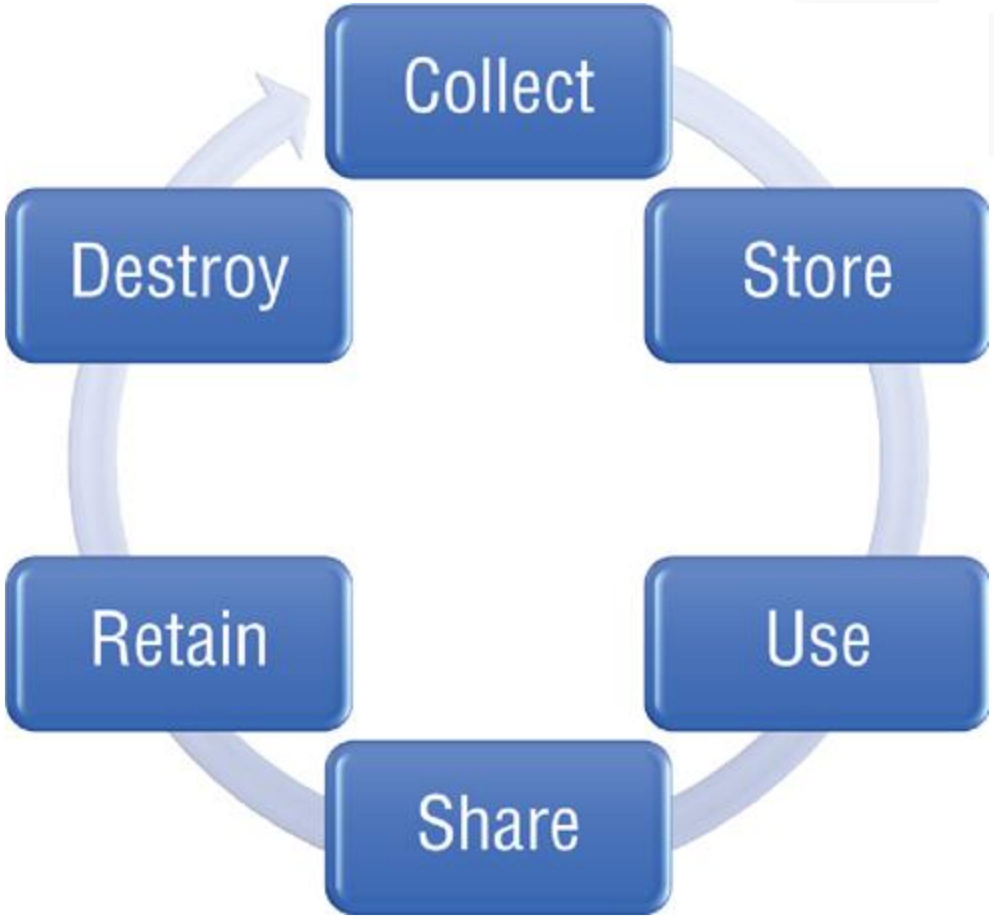
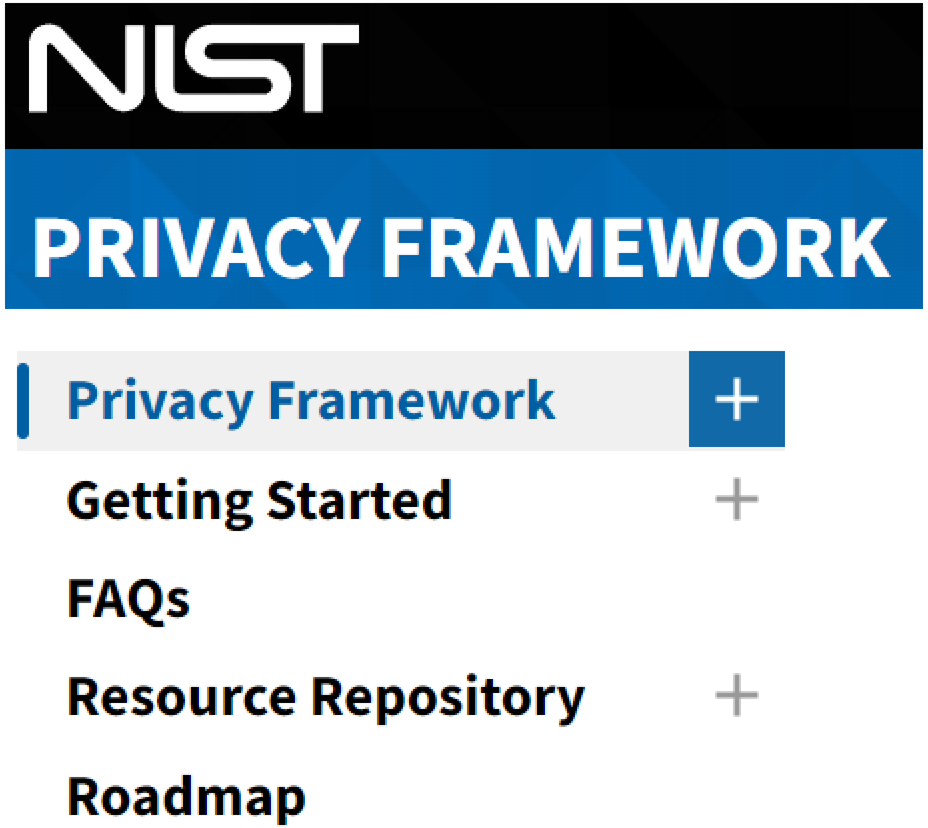


FIGURE 2.5 Secure data lifecycle

Before we talk about Data Classification…

Chapter 5: Protecting Security of Assets

Another **supplemental reference**



NIST

PRIVACY FRAMEWORK

Privacy Framework +

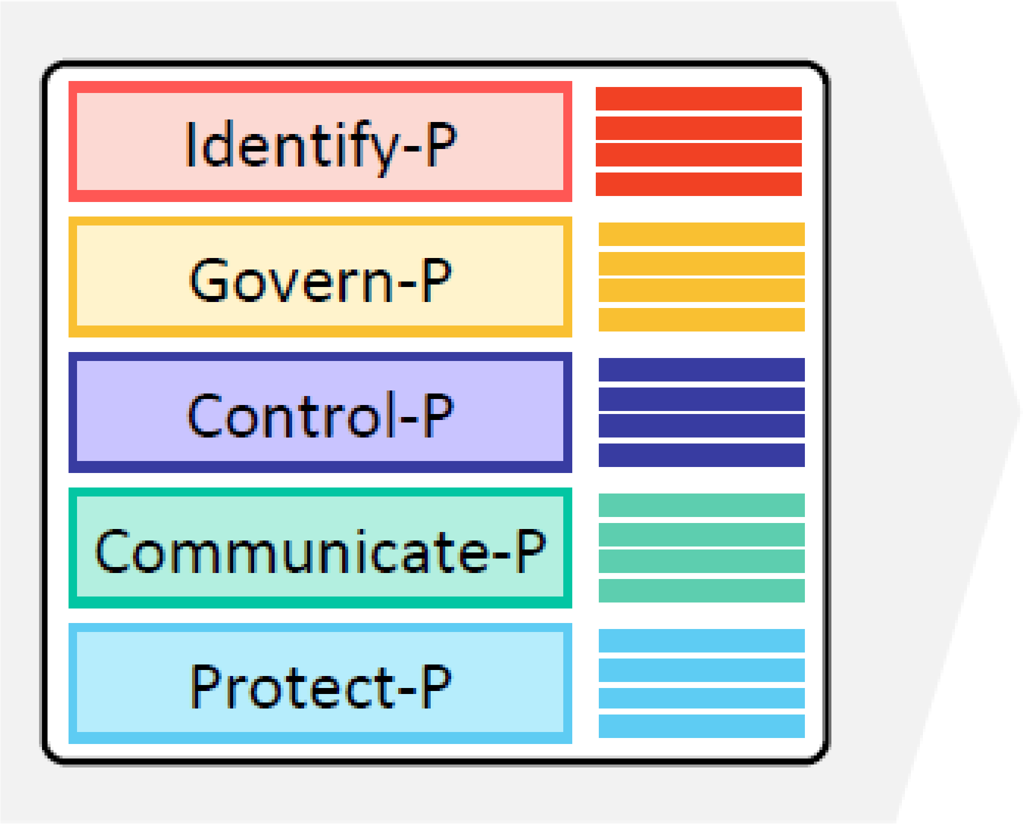
Getting Started +

FAQs

Resource Repository +

Roadmap

CORE



https://www.nist.gov/privacy-framework

Chapter 5: Protecting Security of Assets

Data Classification

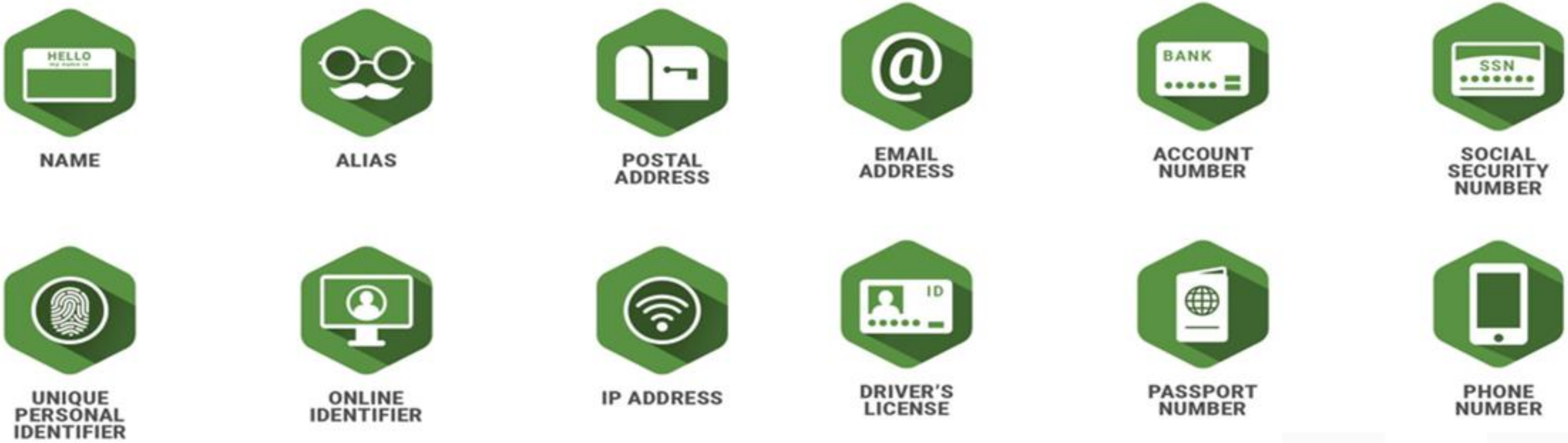
- Needed for **DATA PRIVACY**
- The **process** of **organizing data** into groups or categories that describe the data's **sensitivity, criticality, or value**.
- Determines the data’s CIA Security controls.

- Three Types:
  - Content-based (e.g., PII, PHI, CHD)
  - Context-based (e.g., Web browsing)
  - User-based

Chapter 5: Protecting Security of Assets

Personal Information

- Who you are
- Where you are
- What you are doing



Chapter 5: Protecting Security of Assets

Classification Schema Example

- Confidential
- Sensitive
- Private
- Proprietary
- Public

US Government Classification Labels

- Top Secret
- Secret
- Confidential
- Unclassified
  - For Official Use Only (FOUO)
  - Sensitive by Unclassified (SBU)
  - Controlled Unclassified Information (CUI)

- *Many other classification are possible*
- Documented in the organization’s **Data Classification Policy**
- Asset classification often based on data classification

Chapter 5: Protecting Security of Asse

More about this later (*Provisioning Resources*)

Classifying Data

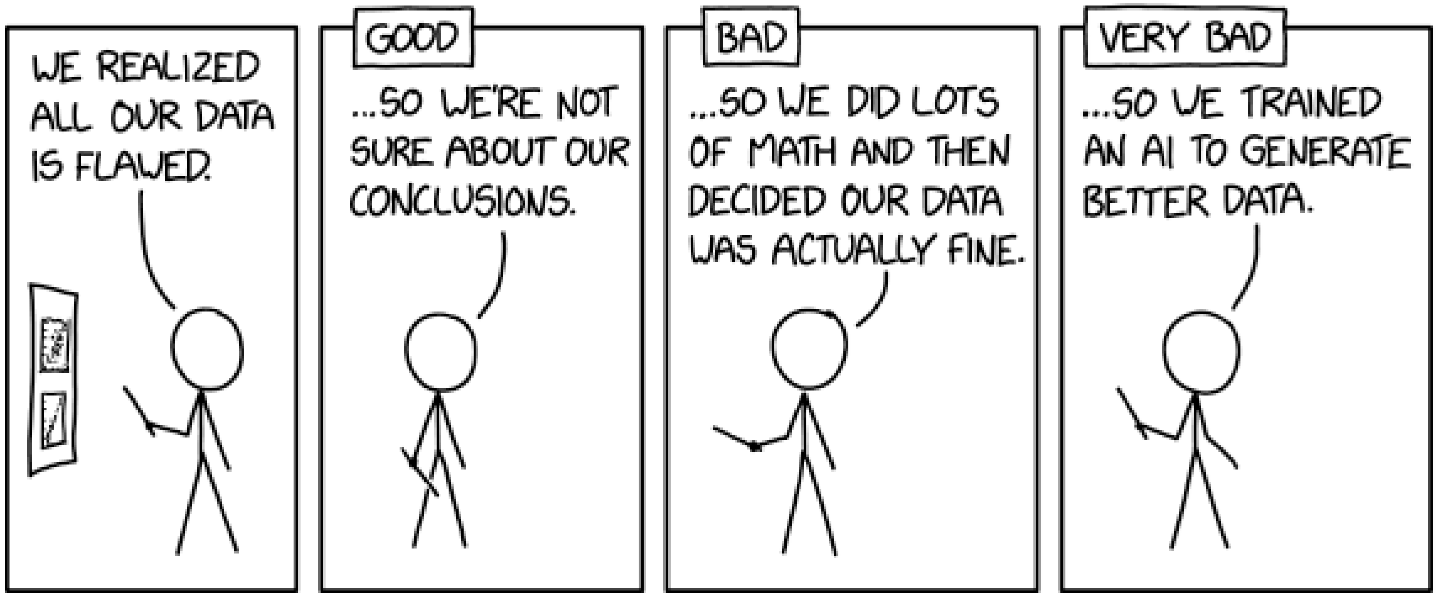
Formal Process for Access Approval

- Documented
- Access requests **approved by the owner**, not the manager and certainly not the custodian (more to follow).
- Approves **subject** access to certain **objects**.
- Subject must understand **rules** and **requirements** for access.
- Best practice is that all access requests and access approvals are **auditable**.
  [Remember – **Repudiation**]

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKE - DATA

Flawed Data


WE REALIZED ALL OUR DATA IS FLAWED.
GOOD
...SO WE'RE NOT SURE ABOUT OUR CONCLUSIONS.
BAD
...SO WE DID LOTS OF MATH AND THEN DECIDED OUR DATA WAS ACTUALLY FINE.
VERY BAD
...SO WE TRAINED AN AI TO GENERATE BETTER DATA.

Title text: We trained it to produce data that looked convincing, and we have to admit, the results look convincing!

https://www.explainxkcd.com/wiki/index.php/2494:_Flawed_Data

Chapter 5: Protecting Security of Assets

Data Categorization

- The process of grouping types of data with comparable "sensitivity labels" (classifications).
- Information is categorized according to its information type.
- Apply similar security controls to assets with similar sensitivities

Chapter 5: Protecting Security of Assets

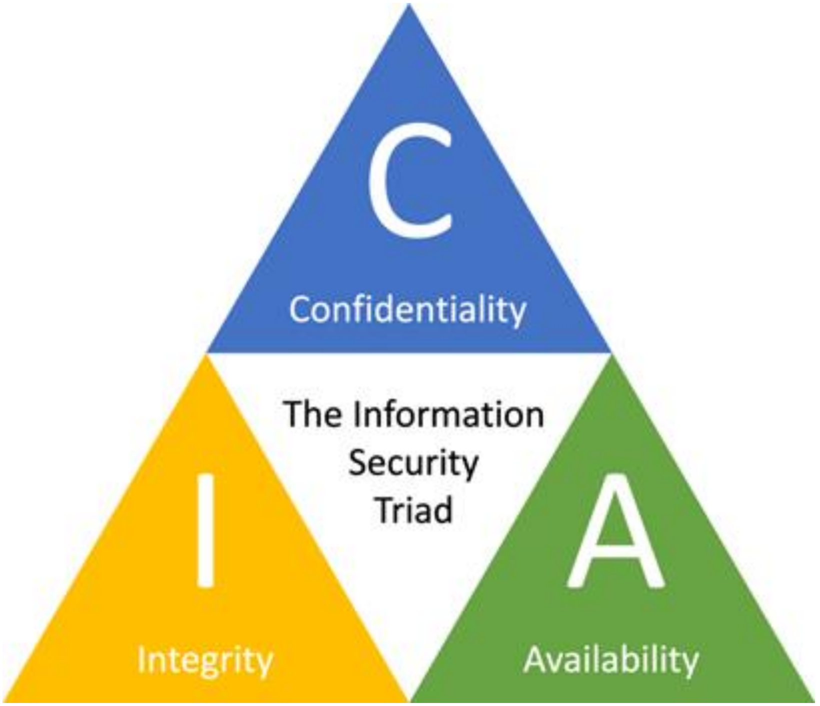
Asset Classification

- Identifying the sensitivity, criticality, and value of information systems.
- Asset types:
  - Data
  - Hardware
  - Media (electronic & physical)
- Grouping assets based on their relative level of sensitivity and the impact to the organization should the assets be compromised.

Chapter 5: Protecting Security of Assets

Identify and Classify Information and Assets

Consider CIA when classifying / categorizing data and assets.

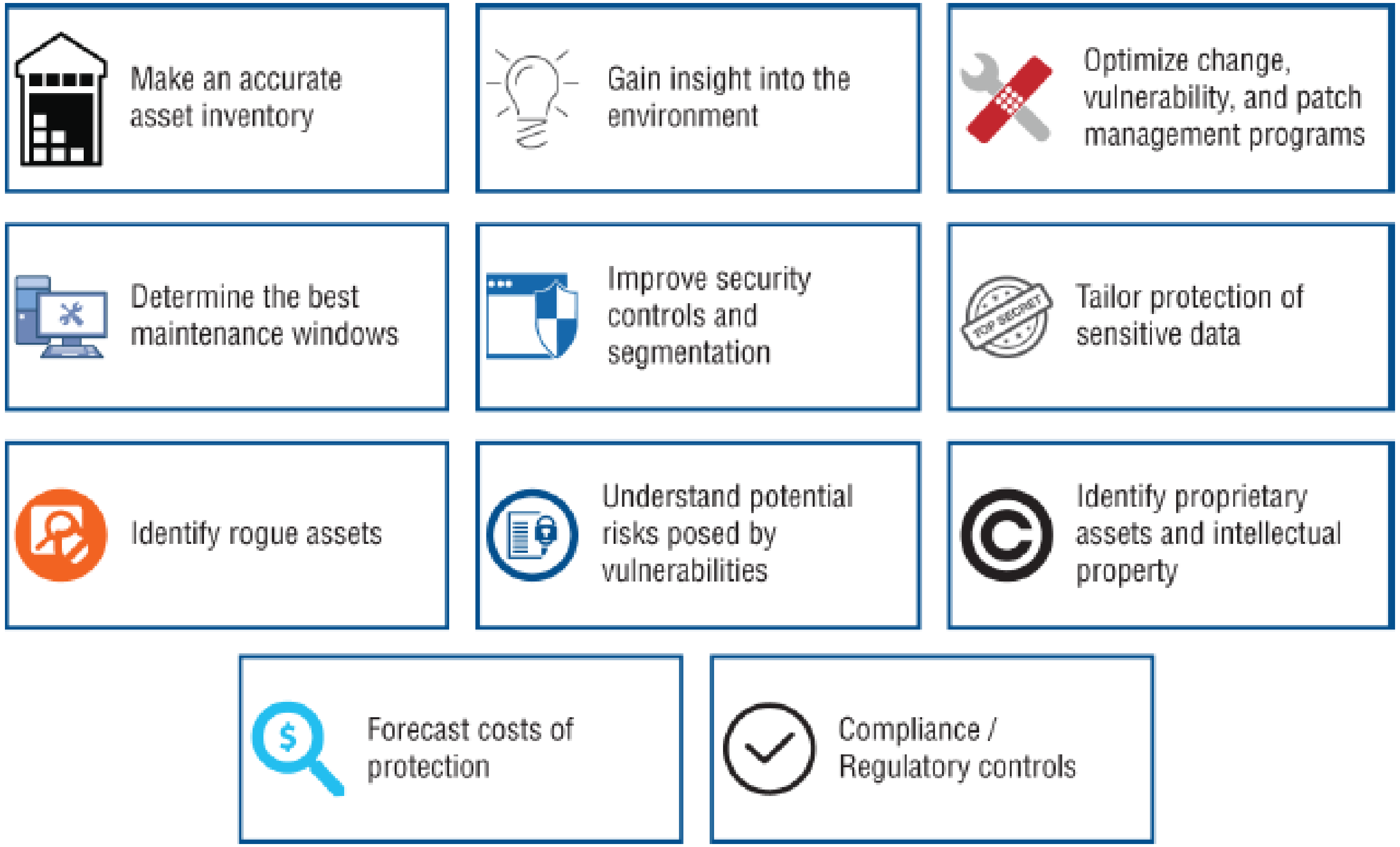


Example:

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 5: Protecting Security of Assets

Classification Benefits



Make an accurate asset inventory

Gain insight into the environment

Optimize change, vulnerability, and patch management programs

Determine the best maintenance windows

Improve security controls and segmentation

Tailor protection of sensitive data

Identify rogue assets

Understand potential risks posed by vulnerabilities

Identify proprietary assets and intellectual property

Forecast costs of protection

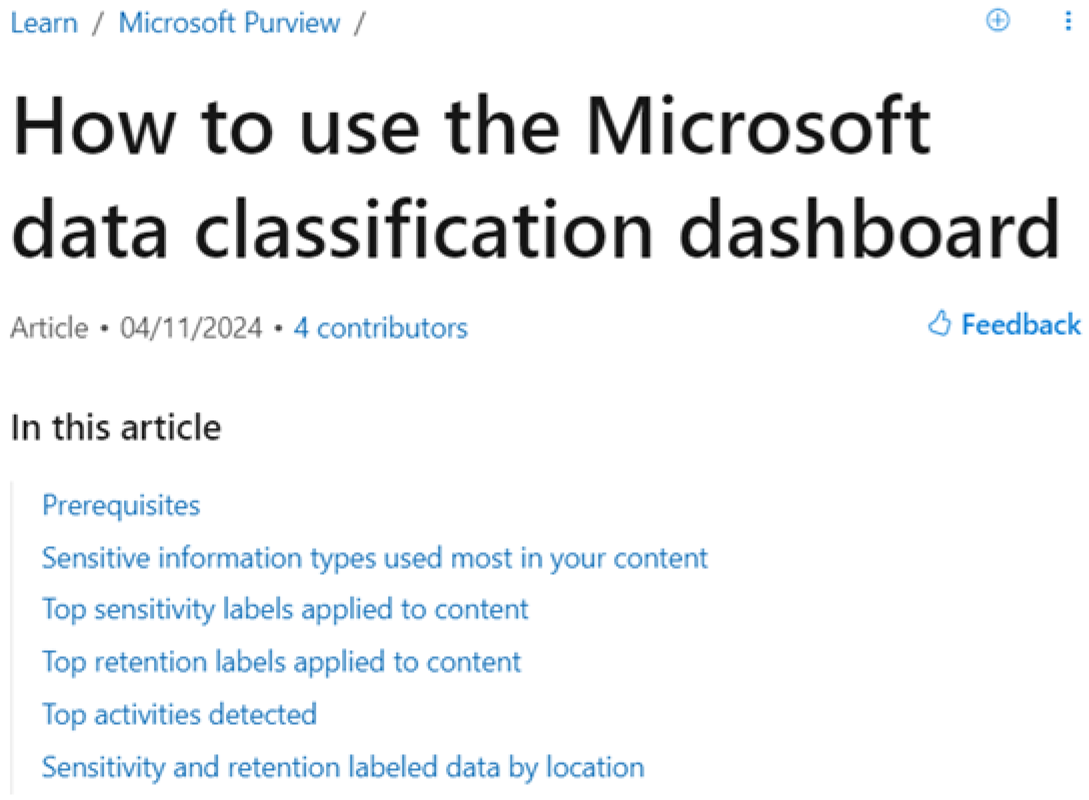
Compliance / Regulatory controls

FIGURE 2.1 General benefits of asset classification

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 5: Protecting Security of Assets

Classification with Microsoft / Office 365 products



Learn / Microsoft Purview /

How to use the Microsoft data classification dashboard

Article • 04/11/2024 • 4 contributors

Feedback

In this article

- Prerequisites
- Sensitive information types used most in your content
- Top sensitivity labels applied to content
- Top retention labels applied to content
- Top activities detected
- Sensitivity and retention labeled data by location

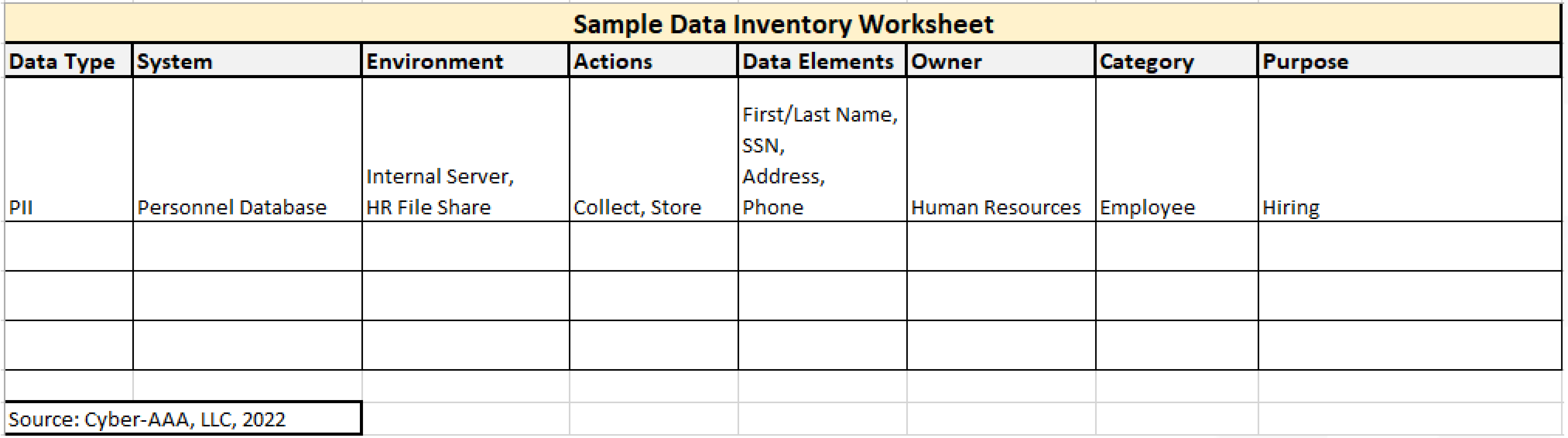
- Get started with sensitivity labels
- Get started with records-management
- Sensitive information type entity definitions

https://learn.microsoft.com/en-us/purview/data-classification-overview

Chapter 5: Protecting Security of Assets

Asset Inventory

- Important systems, devices, software, services or data
- Tangible (hardware) and Intangible (software)
- Start with the items of highest value.



Sample Data Inventory Worksheet

Data Type	System	Environment	Actions	Data Elements	Owner	Category	Purpose
PII	Personnel Database	Internal Server, HR File Share	Collect, Store	First/Last Name, SSN, Address, Phone	Human Resources	Employee	Hiring

Source: Cyber-AAA, LLC, 2022

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 5: Protecting Security of Assets

IDENTIFY AND CLASSIFY INFORMATION AND ASSETS

Best **practices**, **policies**, and **methods** to properly **assure** the **CIA** of **organizational** information and technology **assets**.

You gotta know what you got to keep it secure…
And how important it is…

Questions?
Pls put in YouTube chat or Discord.

DOMAIN 2: PRACTICE QUESTION

Which data type is *not* considered Protected or Private Information?

A. Public WiFi hotspot
B. Protected Health Information (PHI)
C. Credit Card Data
D. Website browsing and cookies

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: PRACTICE QUESTION

Which data type is *not* considered Protected or Private Information?

A. Public WiFi hotspot

B. Protected Health Information (PHI)

C. Credit Card Data

D. Website browsing and cookies

Because it's *Public*

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKES – DATA MINING

Chapter 5: Protecting Security of Assets

New Topic!

ESTABLISH INFORMATION AND ASSET HANDLING REQUIREMENTS

How do you know the data or asset is important?

See the US National Archives for there implementations of labels and markings for CUI - https://www.archives.gov/cui/registry/category-marking-list

Marking and Labeling

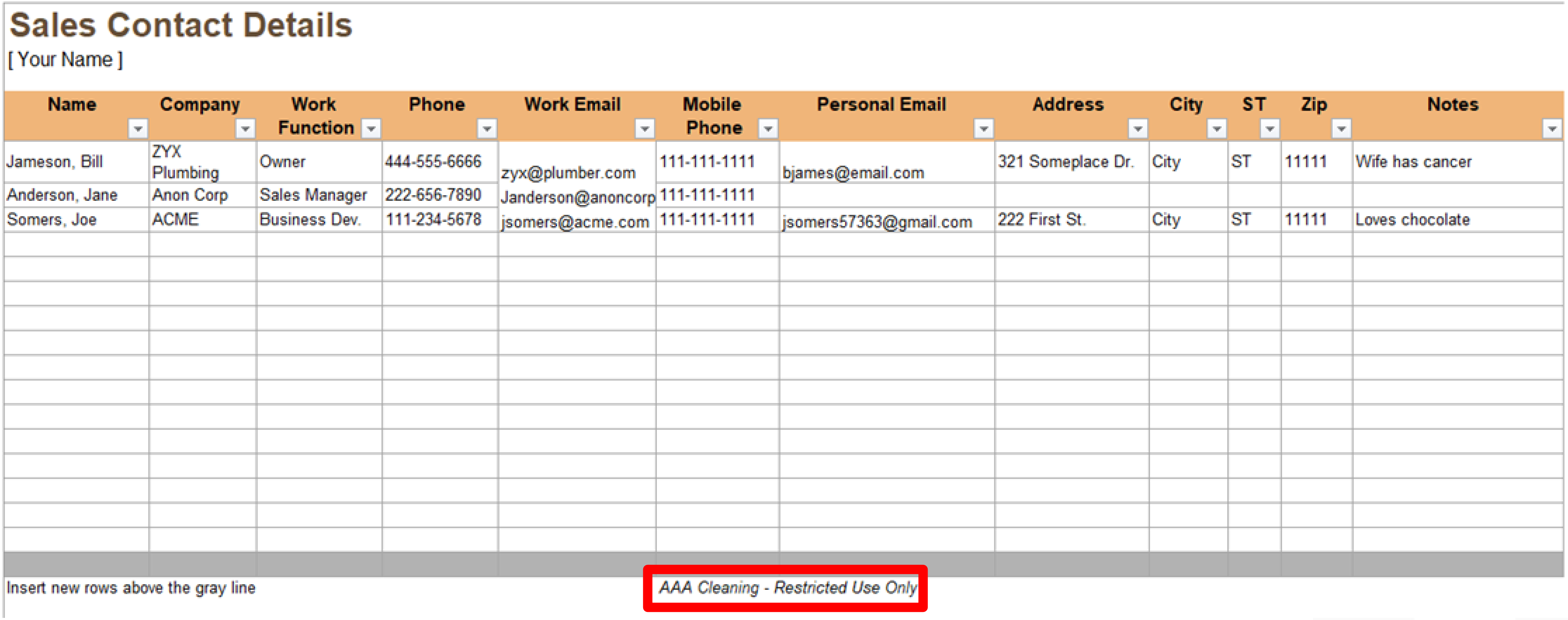
Mark or label assets based on its classification.

Best practice - apply the highest level of security until the data can be determined as not sensitive

Chapter 5: Protecting Security of A

Information and Asset Labeling & Handling

PRIVATE DATA
HANDLE WITH CARE



Sales Contact Details

[Your Name]

Name	Company	Work Function	Phone	Work Email	Mobile Phone	Personal Email	Address	City	ST	Zip	Notes
Jameson, Bill	ZYX Plumbing	Owner	444-555-6666	zyx@plumber.com	111-111-1111	bjames@email.com	321 Someplace Dr.	City	ST	11111	Wife has cancer
Anderson, Jane	Anon Corp	Sales Manager	222-656-7890	Janderson@anoncorp	111-111-1111						
Somers, Joe	ACME	Business Dev.	111-234-5678	jsomers@acme.com	111-111-1111	jsomers57363@gmail.com	222 First St.	City	ST	11111	Loves chocolate

Insert new rows above the gray line

AAA Cleaning - Restricted Use Only

Chapter 5: Protecting Security of Assets

Information and Asset Handling – Storage

Secure Asset Storage

Physical Security

Encryption

Only store data that’s needed.

Backups

Chapter 5: Protecting Security of Assets

Information and Asset Handling – Declassification

- Process of **modifying** the assigned classification of an asset to a **lower level** of sensitivity.
- Used throughout the **Data Lifecycle**.
- *When / Where would you declassify data?*
- Declassification **changes security requirements**. Leads to over-securing assets.
- Manual vs. Automated.
- Part of **data governance** process. (See Domain 1)

Chapter 5: Protecting Security of Assets

Data Declassification Methods

Data De-identification

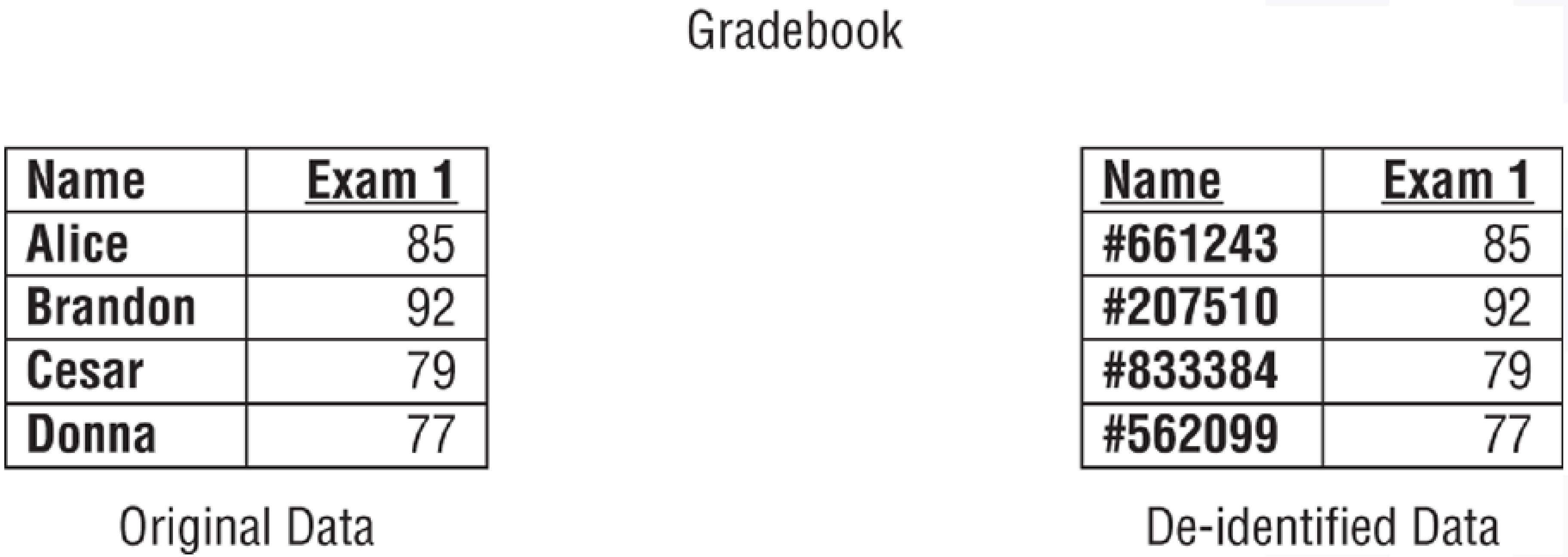
- Process of removing information that can be used to identify an individual.
- Quiz: *Is this used for C, I, or A (or none of the above)?* **Confidentiality**
- Takes PI data fields and converts them to **masked**, **obfuscated**, **encrypted**, or **tokenized** data fields.
- Keeps the data from being easily re-identified.

Chapter 5: Protecting Security of Assets

Data Declassification Methods

Data De-identification via *anonymization*

(Figure 2.2)



Gradebook

Name	Exam 1
Alice	85
Brandon	92
Cesar	79
Donna	77

Original Data

Name	Exam 1
#661243	85
#207510	92
#833384	79
#562099	77

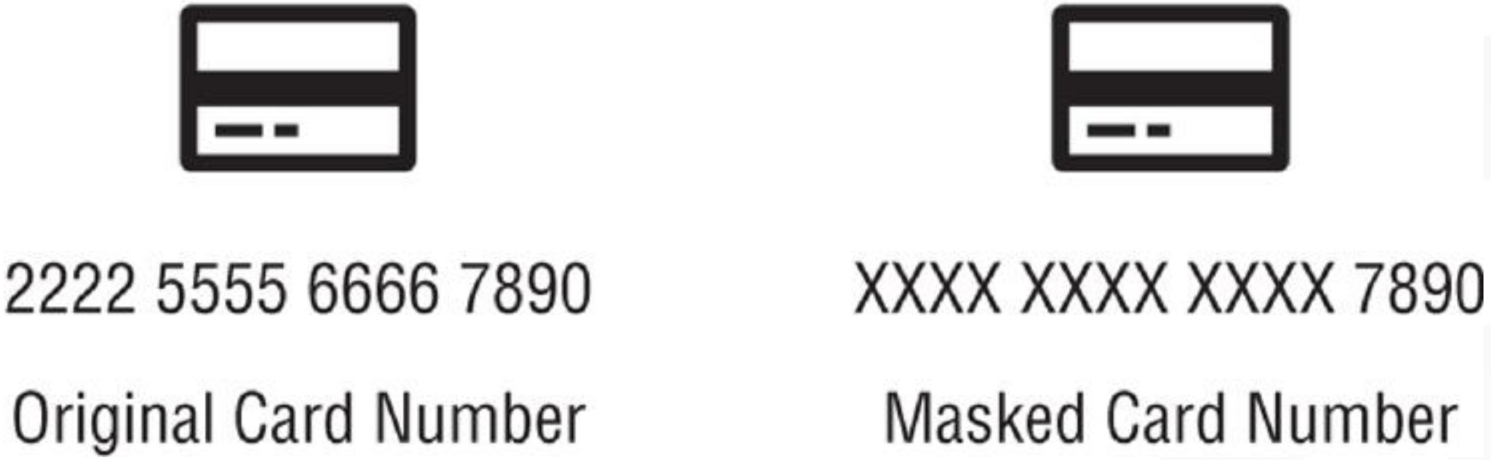
De-identified Data

Chapter 5: Protecting Security of Assets

Data Declassification Methods

Data De-identification via *masking*

(Figure 2.3)



Chapter 5: Protecting Security of Assets

Data Declassification Methods

Data Tokenization

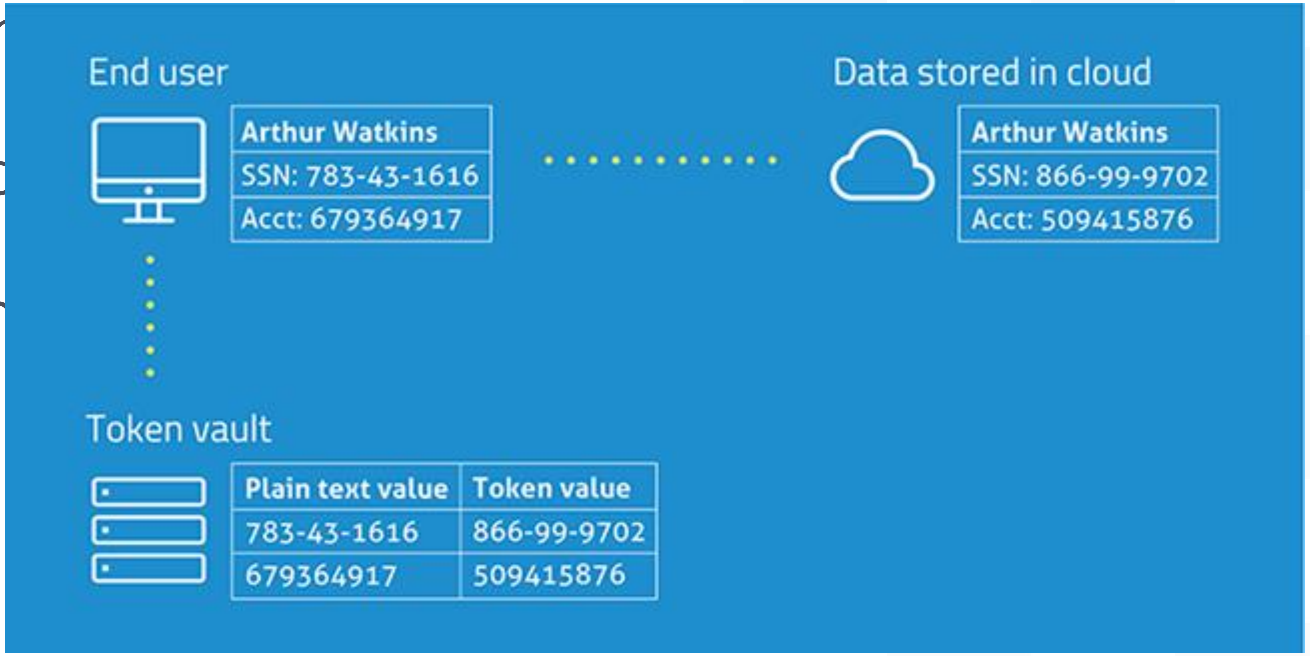
- Substituting personal data with a random token
- Link between token and PI
- Random numbers or one-way functions
- Can’t be reverse-engineered / deciphered

Chapter 5: Protecting Security of Assets

Data Declassification Methods

Data Tokenization

- Substituting personal data with a random token
- Link between token ar
- Random numbers or c
- Can’t be reverse-engir

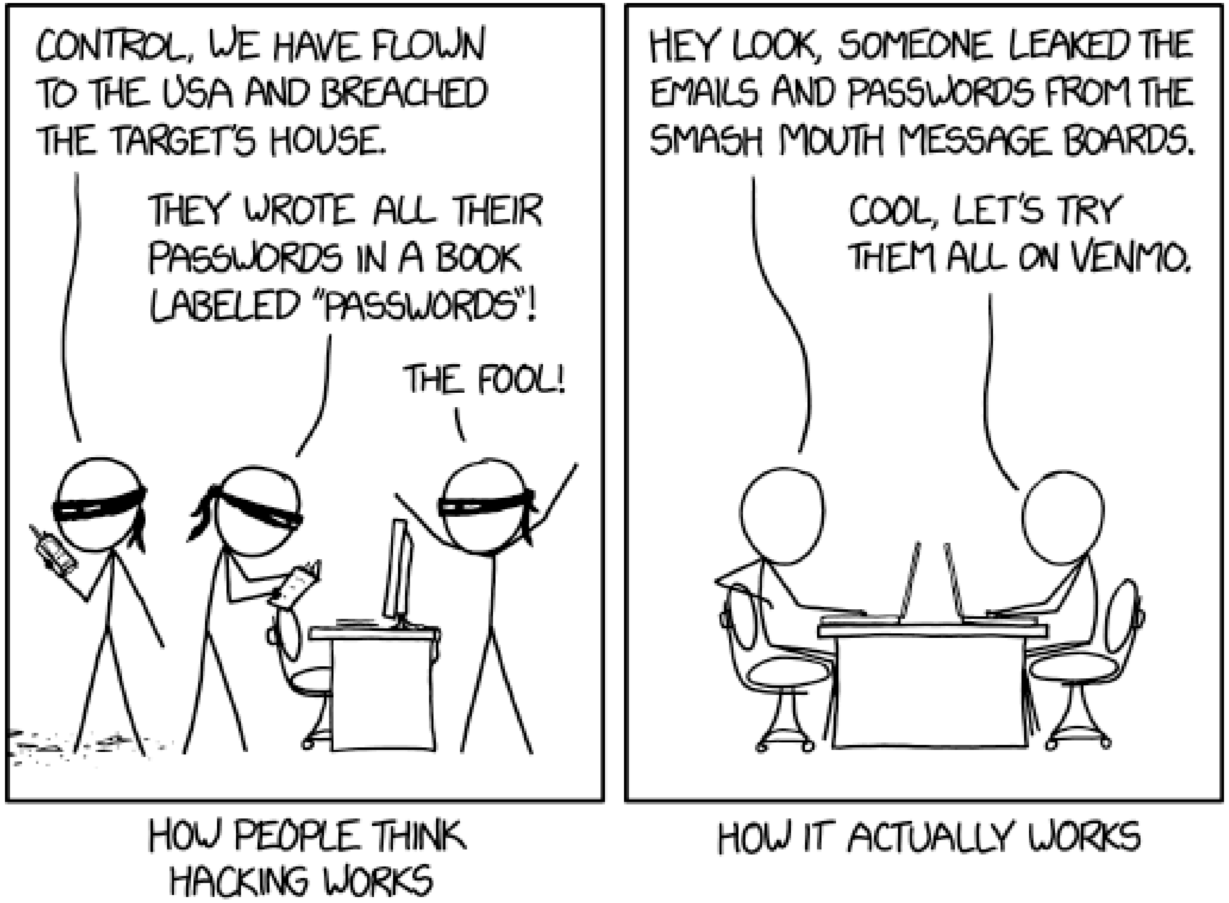


Plain text value	Token value
783-43-1616	866-99-9702
679364917	509415876

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKES - HACKING

How Hacking Works


CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.
THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!
THE FOOL!
HOW PEOPLE THINK HACKING WORKS
HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.
COOL, LET'S TRY THEM ALL ON VENMO.
HOW IT ACTUALLY WORKS

Title text: If only somebody had warned them that the world would roll them like this.

https://www.explainxkcd.com/wiki/index.php/2176:_How_Hacking_Works

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 5: Protecting Security of Ass

New Topic!

PROVISION RESOURCES SECURELY

Topics:

- Information and Asset Ownership
- Asset Inventory
  - Inventory Tool / System of Record
  - Process Considerations
- Asset Management
  - Configuration Management
  - Change Management

Honestly, this domain is a little all over the place. Reminder: Jump around.

Chapter 5: Protecting Security of Assets

Information / Asset Ownership

Assigning responsibility, oversight, and guidelines for asset and data management.
[Part of Governance / Policies]

Dr. Eugene Spafford's first principal of security administration:

> *If you have responsibility for security, but have no authority to set rules or punish violators, your role is to take the blame when something goes wrong.**

* Garfinkle & Spafford, *Practical Unix & Internet Security*, O'Reilly & Associates, Inc, 1996, p.39.

Chapter 5: Protecting Security of Ass

New Topic!

Information / Asset Ownership

Asset Owner Responsibilities:

- Governance / Compliance
- Asset classification
- Asset inventory
- Access oversight (Zero Trust)
- Acceptable use
- Defining, monitoring, & prioritizing safeguards (based on risk)

Lots of Responsibilities!

Rarely formalized… 😑

Chapter 5: Protecting Security of Assets

Asset Inventory

*Having a **current and complete inventory** is the absolute bedrock for implementing and monitoring technical security controls.* (repeated)

Inventory Tool

- System enumeration and endpoint management
- Distinguishes authorized & unauthorized assets (Shadow IT)
- Collect and track individual asset details
- For reporting, audits, risk management, and incident management

System of Record

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 5: Protecting Security of Assets

Repeat Slide 32cccc

ASSET INVENTORY

- WHAT
  - **Hardware** (Servers, Equipment, Devices, Endpoints, etc.)
  - **Software** (Applications)
  - **Data** ** Hardest…
- WHERE
  - **Location**(s) – Physical and virtual
  - Document - **Network Diagrams** and **Data Maps**
- WHO
  - **Responsibilities** (Business & IT)

See book Pages 205-206

Chapter 5: Protecting Security of Assets

Asset Inventory Tools

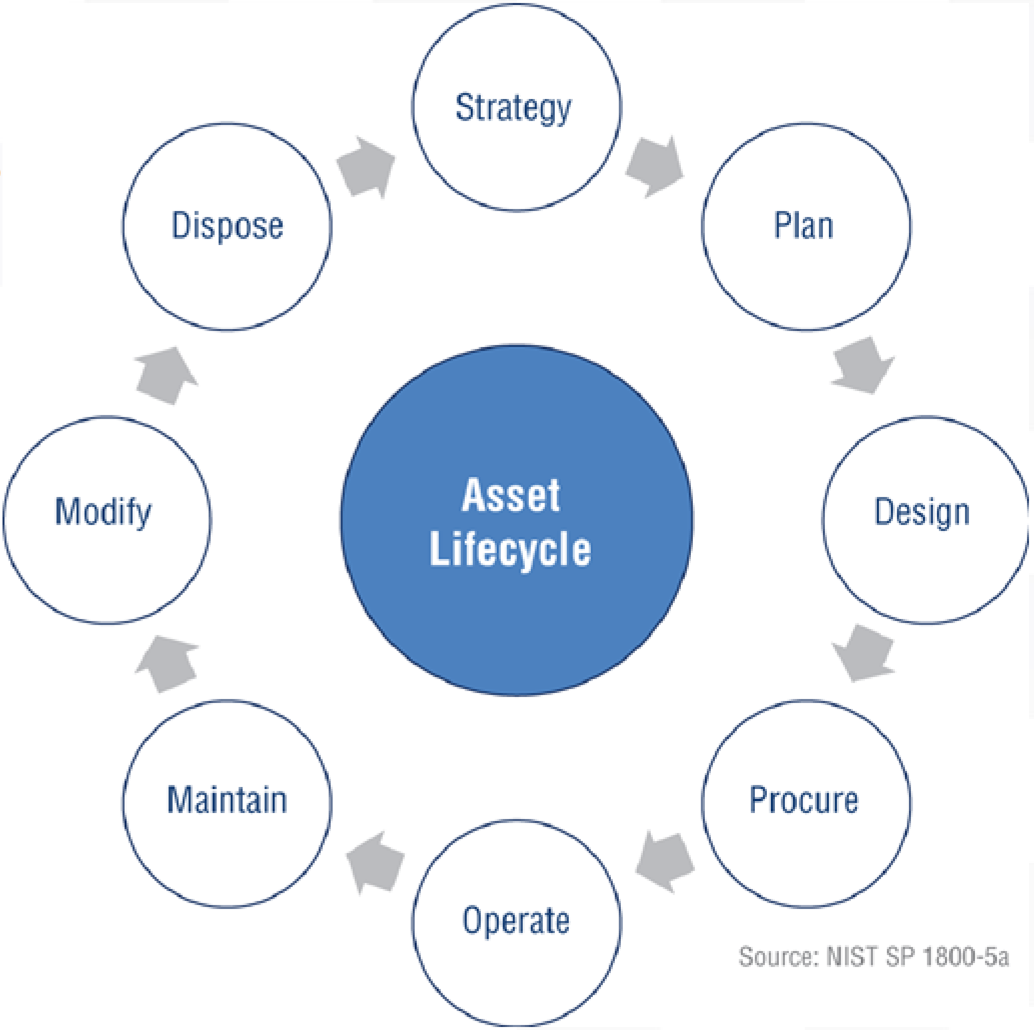
- Active Directory (AD) and
  Lightweight Directory Access Protocol (LDAP) server
- Vulnerability scanners, configuration scanners, and network mapping tools (nmap)
- Software Licenses
- Data Loss Prevention (DLP)

Automate as much as possible!

Chapter 5: Protecting Security of Assets

Asset Management

Typical asset management lifecycle



Source: NIST SP 1800-5a

**Questions?
Pls put in YouTube chat or Discord.**

Chapter 5: Protecting Security of Assets

Implementing Asset Management

Information Technology Asset Management (ITAM)

- Tracking and efficiently using tangible and intangible IT Assets

ISO/IEC 19770 Family

- Assist organizations with managing risks and costs associated with IT assets

Chapter 5: Protecting Security of Assets

More in Domain 7

Implementing Asset Management

Configuration Management

- Maintaining asset inventory by controlling system and software configurations
- Configuration Management Database (CMDB)

Baselines

- System – product versions & settings
- Security – patches

NIST SP800-70 [National Checklist Program (NCP)]

Automate as much as possible!

Security Content Automation Protocol (SCAP)

DAD JOKES – DATA MINING

[redacted]

CISSP® MENTOR PROGRAM – SESSION THREE

Chapter 5: Protecting Security of Ass

New Topic!

MANAGE *DATA* LIFECYCLE

Topics:

- Data Roles
  - Owners
  - Controllers
  - Custodians
  - Processors
  - Users
  - Subjects
- Data Collection
- Data Location
- Data Maintenance
- Data Retention
- Data Destruction
- Data Remanence

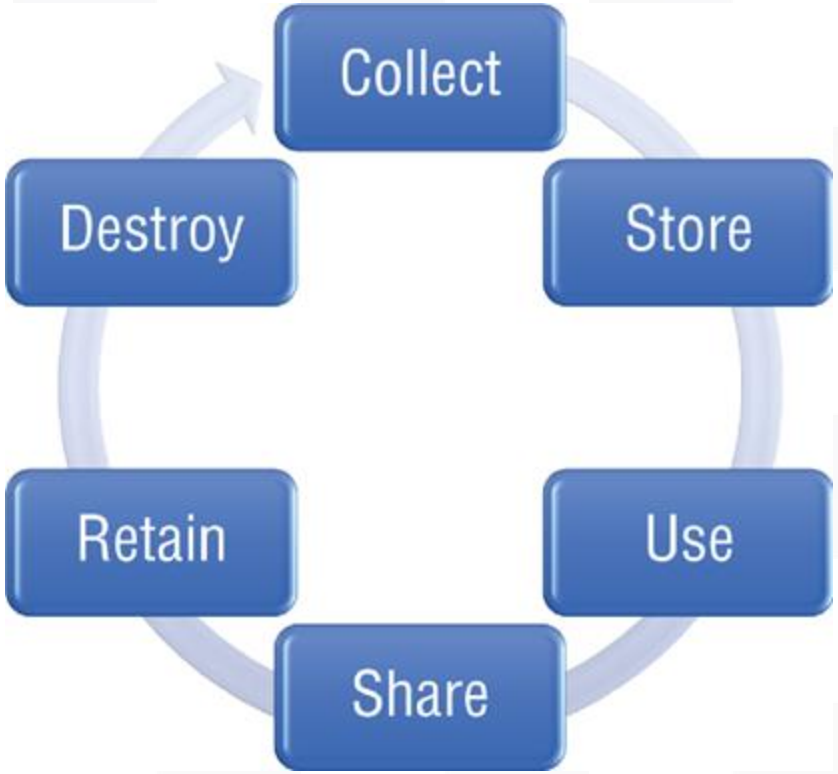


FIGURE 2.5 Secure data lifecycle

Chapter 5: Protecting Security of Assets

Data Lifecycle

Review

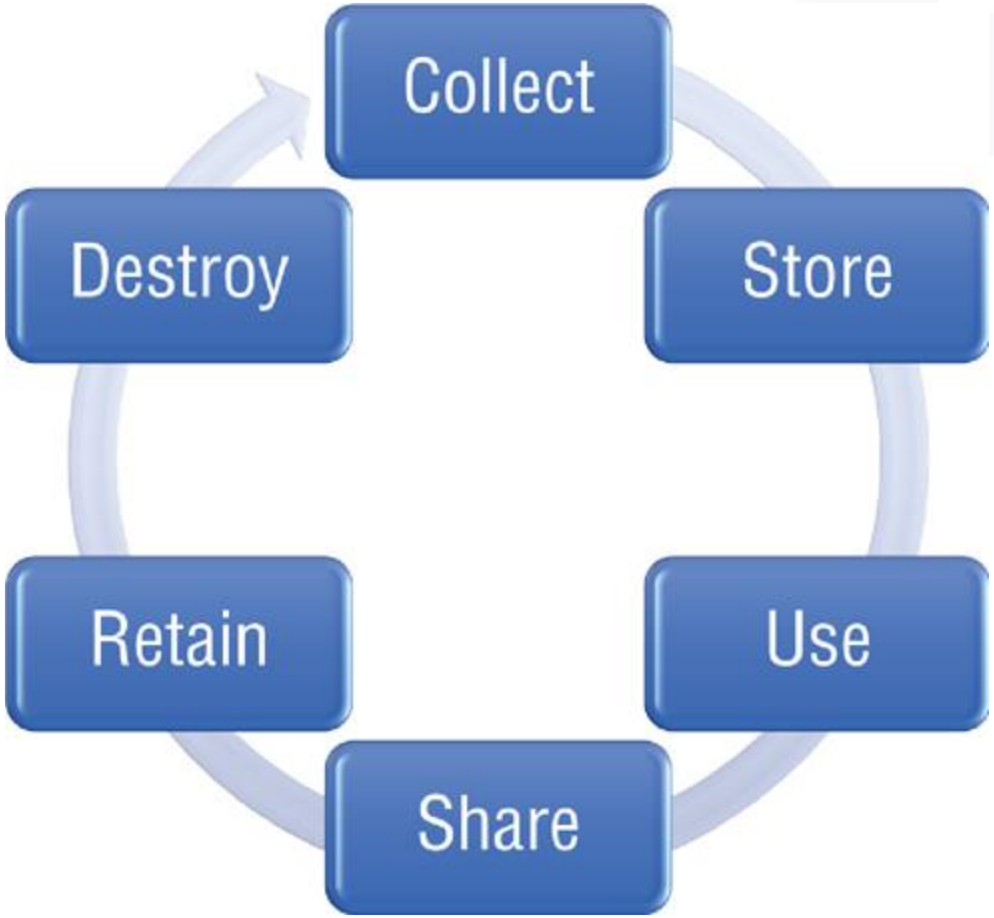


FIGURE 2.5 Secure data lifecycle

Chapter 5: Protecting Security of Assets

Due Care
Due Diligence

Data Oversight Roles

Data Owner

- An individual or group of individuals responsible for dictating how and why data should be used;
- Determines how the data must be secured (risk treatment);
- Knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed;
- Determines the appropriate value and classification of information generated by the owner or department;
- Communicates Data Classification.

Chapter 5: Protecting Security of Assets

Data Oversight Roles

Data Controller

- The person, agency, company, or other body that, alone or jointly with others, determines the purposes and means of data processing.
- Responsible for adhering to all principles relating to processing personal data.
- Negotiate privacy protections / *data processing agreements*
- EU GDPR

Chapter 5: Protecting Security of Assets

Data Oversight Roles

Data Custodians

- Maintains the protection of data according to the information classification.
- Delegated by the Data Owner and is usually IT personnel.

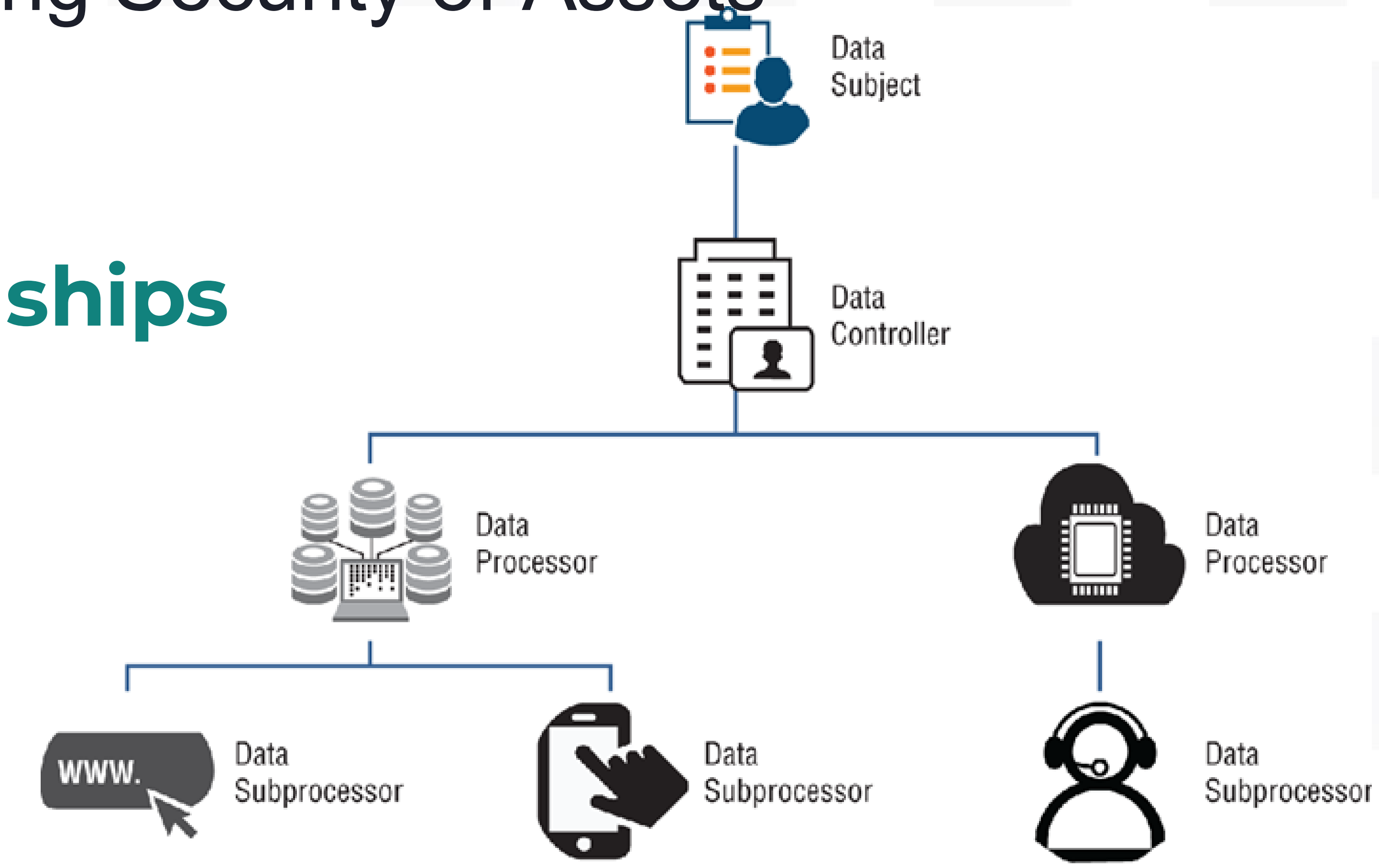
Data Processors

- The party responsible for transferring, transmitting, or otherwise handling data on behalf of a *data owner*.
- Role in the protection of data.
- Examples: Healthcare, Banking, Credit Processing

Chapter 5: Protecting Security of Assets

Data Oversight Roles / Relationships

Figure 2.6



- *Data controller determines the need and how the data will be processed.*
- *Data processor is a separate legal entity processing data for the controller.*
  - *Cloud providers are generally considered data processors, as are market research firms, payroll companies, accountants.*

Chapter 5: Protecting Security of Assets

Data Oversight Roles

Know the Difference

Data Users

- Party that consumes the data.
- May hold data processors accountable for SLAs and protection.

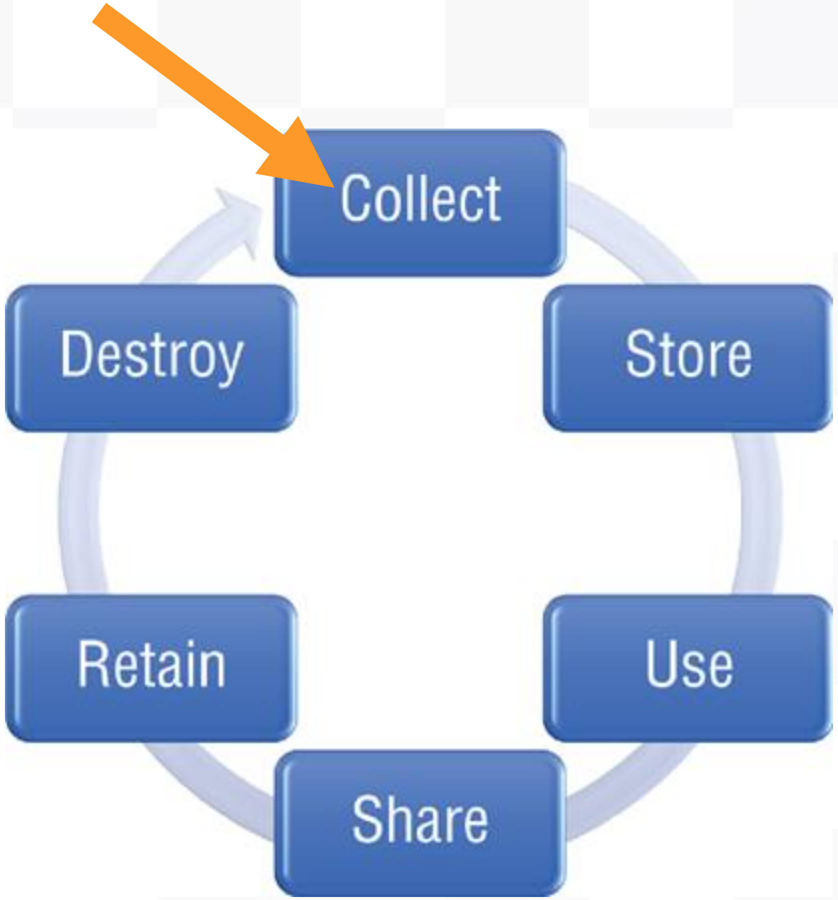
Data Subjects

- Defined by GDPR, are "identified or identifiable natural people" — or just human beings,
- From whom or about whom information is collected

Chapter 5: Protecting Security of Assets

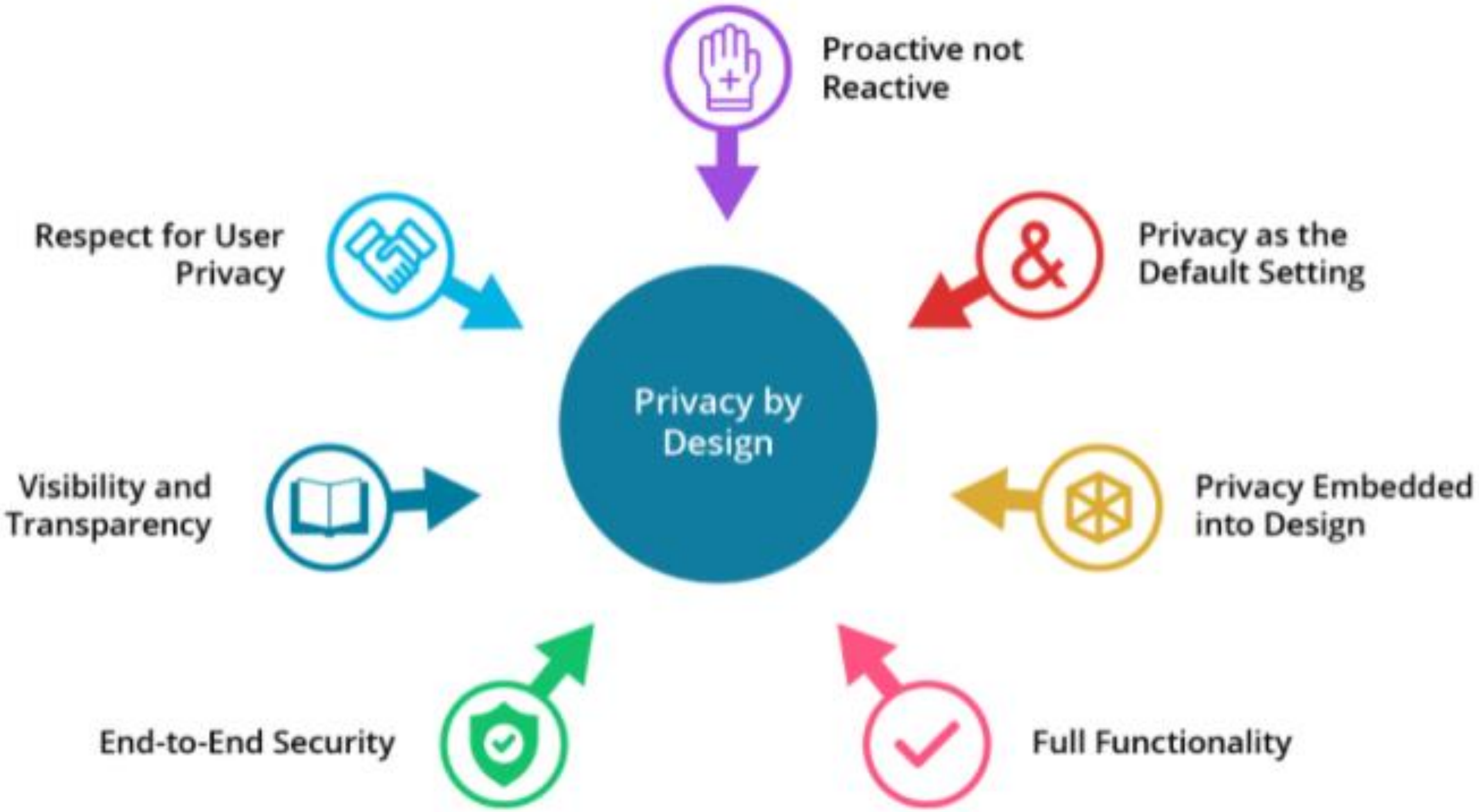
Data Collection

- Data creation, acquisition, aggregation, or any circumstance where data is “new” to your system
- Build Security / Privacy In …
- Organizations should **collect the minimum amount of sensitive information necessary**;
- Collection Limitation Principle – GDPR Individual Rights



Chapter 5: Protecting Security of Assets

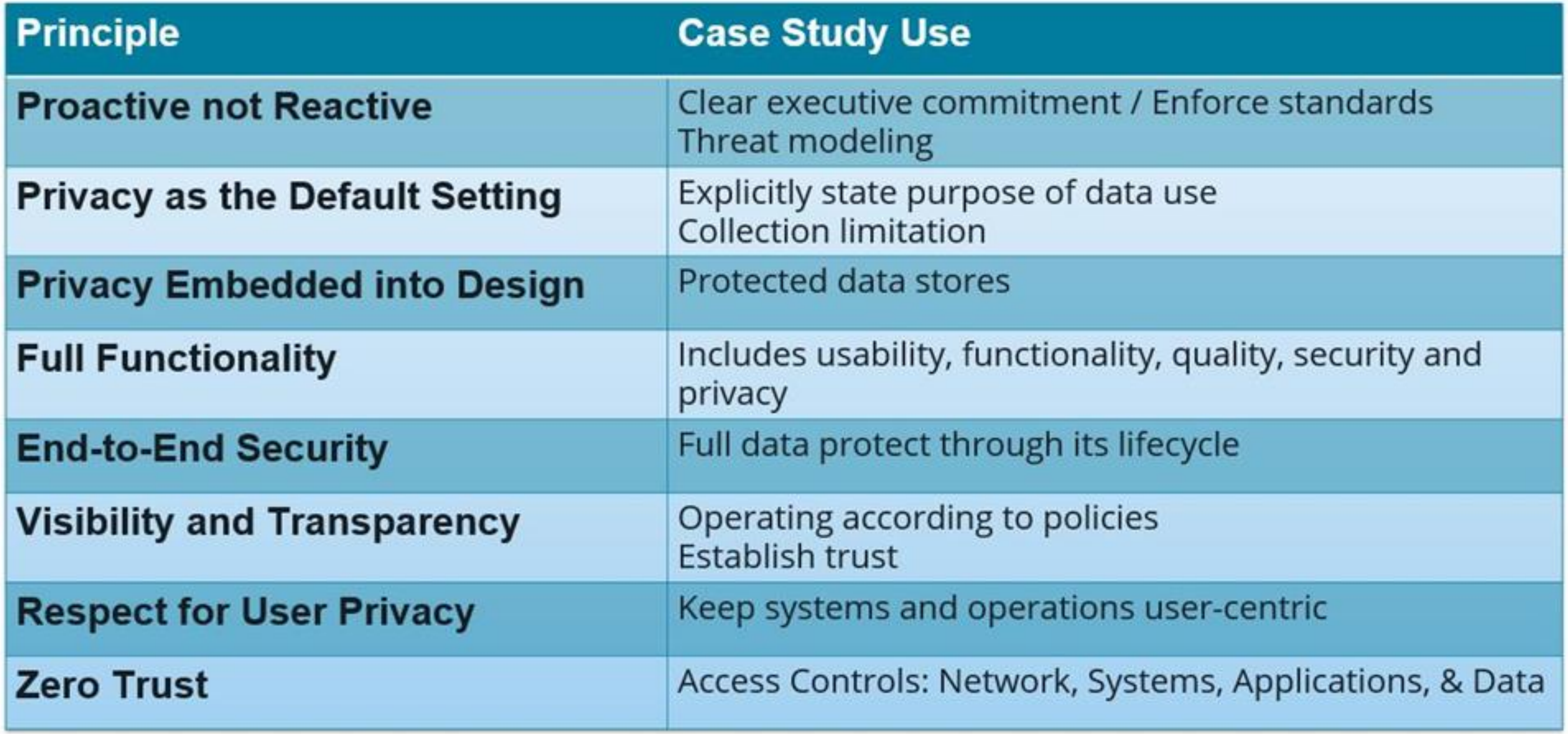
Privacy by Design – 7 Foundational Principles



Source: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Chapter 5: Protecting Security of Assets

Privacy by Design – 7 Foundational Principles



Principle	Case Study Use
Proactive not Reactive	Clear executive commitment / Enforce standards Threat modeling
Privacy as the Default Setting	Explicitly state purpose of data use Collection limitation
Privacy Embedded into Design	Protected data stores
Full Functionality	Includes usability, functionality, quality, security and privacy
End-to-End Security	Full data protect through its lifecycle
Visibility and Transparency	Operating according to policies Establish trust
Respect for User Privacy	Keep systems and operations user-centric
Zero Trust	Access Controls: Network, Systems, Applications, & Data

Source: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Chapter 5: Protecting Security of Assets

Privacy and Security

May 31, 2023

From Silo to Synergy Between Cybersecurity and Privacy in the U.S.

Source: https://www.isc2.org/Insights/2023/05/from-silo-to-synergy-between-cybersecurity-and-privacy-in-the-us

Chapter 5: Protecting Security of Assets

Privacy Principles

Data Management

Data Use / Purpose

- Why is the data collected? (Documenting data purpost)
- User notification of intent.

Data Location

- Where is the data? (Physical & Logical)
- Data Localization

**Questions?
Pls put in YouTube chat or Discord.**

Chapter 5: Protecting Security of Assets

Data Management

Data Maintenance

- Applying appropriate security controls through the “use” phase
- Balance between functionality and security
- Part of *Zero Trust* principles
  (Least Privilege and Defense in Depth)

Data Retention

- Time period for keeping data before destruction
- Determined by policy (often legal)

TIP The less data you have, the less damaging a security breach will be.

Chapter 5: Protecting Security of Assets

TIP: *If you don't need data, securely destroy it.*

Data Management

Data Destruction / Remanence

- Logically or physically destroying unneeded data, you can both reduce your risk exposure and decrease your storage and data maintenance costs.
- Data that is left over is called ***remnant data*** - occurs when data destruction efforts were insufficient to prevent the reconstruction of the data.
- d/or formatting a h thod for destroying on.
- d temporary files (c media.

Certificate of Destruction

ISSUE: Cloud Service Providers

Chapter 5: Protecting Security of Assets

Data Management

Data Destruction Regulations & Frameworks

US

- GLBA
- HIPAA
- Fair Credit Reporting

European standard BS EN 15713, “Secure Destruction of Confidential Information”

Chapter 5: Protecting Security of Assets

See the 2023 Class 3 Slides & Video

Data Management

Data Destruction Methods

Often determined by law

Methods:

1. Render the object useless

- Destruction (Physical) – Shredding, Incineration, Disintegration

2. Cleansing / Sanitizing

- Overwriting / Clearing / Zeroing
- Degaussing / Purging
- Destroying encryption keys

Chapter 5: Protecting Security of Assets – Quiz

What is the best way to protect data?

[✓ A. Don’t collect it.]

B. AES-1024 encryption.

C. Data tokenization.

D. Destroy it based on the organization’s retention policy

DOMAIN 2: PRACTICE QUESTION

Which of the following describes a duty of the Data Owner:

A. Patch systems
B. Report suspicious activity
C. Ensure their files are backed up
D. Ensure data has proper security labels

DOMAIN 2: PRACTICE QUESTION

Which of the following describes a duty of the Data Owner:

A. Patch systems

B. Report suspicious activity

C. Ensure their files are backed up

D. Ensure data has proper security labels

DAD JOKE - DATA

Chapter 5: Protecting Security of Assets

New Topic!

ENSURE ASSET RETENTION

Topics:

- Determining Appropriate Records Retention
- Records Retention Best Practices

Chapter 5: Protecting Security of Assets

ENSURE ASSET RETENTION

Why Retention:

- Preserve Intellectual Property (IP)
- Support institutional memory
- Legal / Regulatory requirements
- Evidence of actions
- Forensics investigations

You answer first…
Why do organizations need to retain data?

Chapter 5: Protecting Security of Assets

Book intermingles data and asset retention…

Data / Asset Retention

Data Retention Policy

Don't forget IT audit logs!

Part of Data Protection Policy

- Assign Responsibility: Data Protection Officer (DPO) and/or Chief Security Officer (CSO)
- See p. 234 for more on building a Data Use Policy
- Appropriately manages and protects data & assets throughout the lifecycle.
- Data should be assigned a retention limit based on regulatory / organizational requirements.

Chapter 5: Protecting Security of Assets

Data / Asset Retention

Determining Appropriate Records Retention

- EU GDPR's Article 17, "*The Right to Erasure*," commonly called the *right to be forgotten*.
- Organizations need procedures to erase data.
- Note exceptions
- Consult legal

Originally from 1890's Louis Brandeis...

Chapter 5: Protecting Security of Assets

Consult Legal

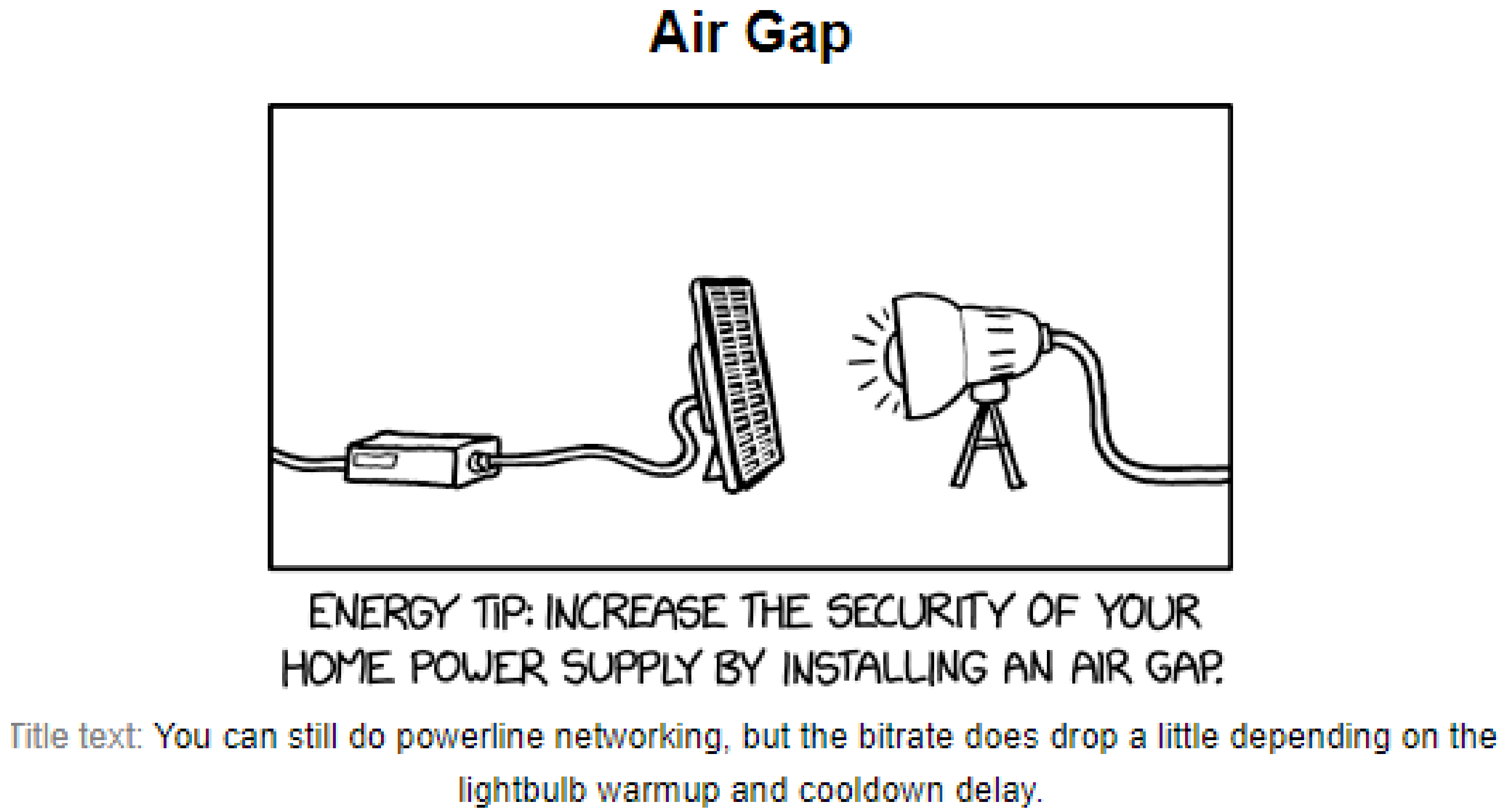
Data / Asset Retention

Records Retention Best Practices

- Handle and retain records in accordance with applicable laws, directives, policies, regulations, standards, and operational requirements.
- Maintain records according to the organization's record retention schedule.
- *Don't keep it if you don't need it.*
- Contained in the **Data Protection / Retention Policy & Procedures**.

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKES – POWER AIR GAP



Air Gap

ENERGY TIP: INCREASE THE SECURITY OF YOUR HOME POWER SUPPLY BY INSTALLING AN AIR GAP.

Title text: You can still do powerline networking, but the bitrate does drop a little depending on the lightbulb warmup and cooldown delay.

https://www.explainxkcd.com/wiki/index.php/2651:_Air_Gap

Chapter 5: Protecting Security of Asse

New Topic!

DETERMINE DATA SECURITY CONTROLS AND COMPLIANCE REQUIREMENTS

Topics:

- Data States
  - Data at Rest
  - Data in Motion
  - Data in Use
- Scoping and Tailoring
  - Common Controls
  - Compensating Security Controls
- Standards Selection
  - Leading Security Frameworks
  - Security Standards
- Data Protection Methods
  - Digital Rights Management
  - Data Loss Prevention (DLP)
  - Cloud Access Security Broker

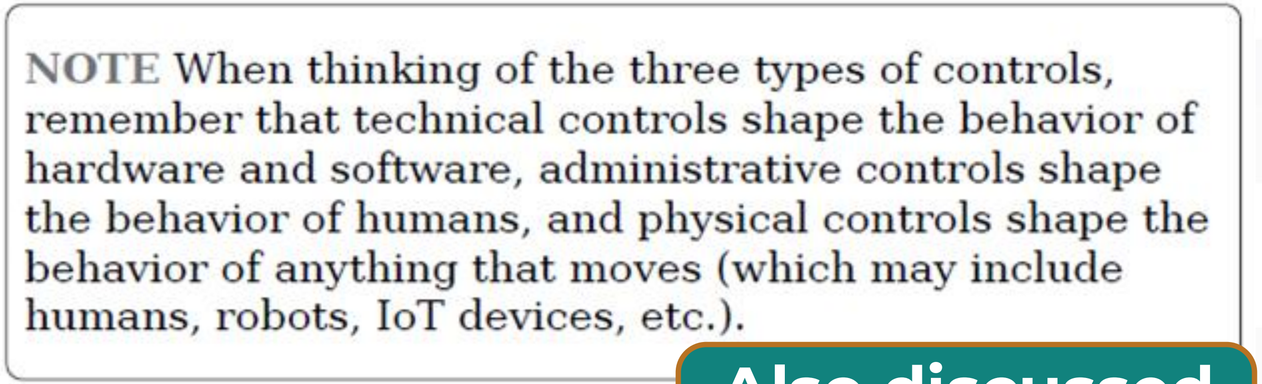
Chapter 5: Protecting Security of Assets

People, Process, & Technology

Data Security Controls

Control Types

- Security controls will vary based on the classification of each asset, the data state (discussed next), and any compliance requirements or industry standards.
- Technical Controls
- Administrative Controls
- Physical Controls



NOTE When thinking of the three types of controls, remember that technical controls shape the behavior of hardware and software, administrative controls shape the behavior of humans, and physical controls shape the behavior of anything that moves (which may include humans, robots, IoT devices, etc.).

P. 247 – Common Controls

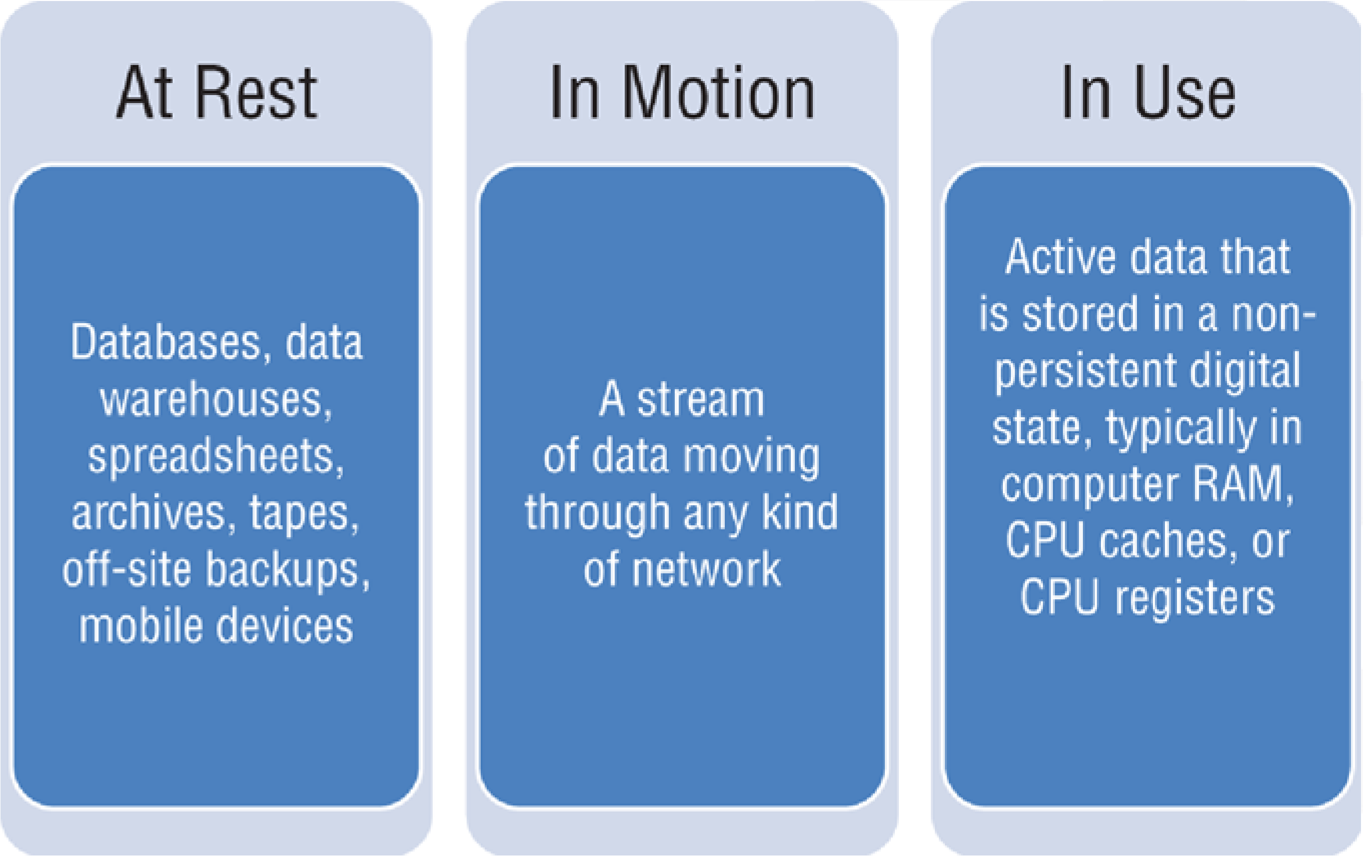
Also discussed Chapter 1

Chapter 5: Protecting Security of Assets

Data Security Controls

Data States

Figure 2.7 Data States and Examples



At Rest

Databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices

In Motion

A stream of data moving through any kind of network

In Use

Active data that is stored in a non-persistent digital state, typically in computer RAM, CPU caches, or CPU registers

Chapter 5: Protecting Security of Assets

Data Security Controls

Data Protection – *Data at Rest*

- Access Controls
- Disk / Data Encryption
    - Trusted Platform Module (TPM)
    - Self-encrypting drive (SED)
    - File-level encryption

Encryption is your friend. Covered in Domain 3.

Chapter 5: Protecting Security of Assets

Encryption is your friend. Covered in Domain 3.

Data Security Controls

Data Protection – *Data in Transit*

- Transport Layer Security (TLS) (including HTTPS)
- VPNs
- Link encryption – Traffic is encrypted and decrypted at each network routing point (e.g., network switch)
- End-to-end encryption – Only sender & receiver can read data

Chapter 5: Protecting Security of Assets

Data Security Controls

Data Protection – ***Data in Use***

Covered in Domain 3.

- Often forgotten
- Protecting Data being processed
  - Applications (RAM, CPU, Caches, etc.)
  - End users
- Encryption may not be relevant
- Access Control is…

Chapter 5: Protecting Security of Assets

Data Security Controls

Scoping & Tailoring

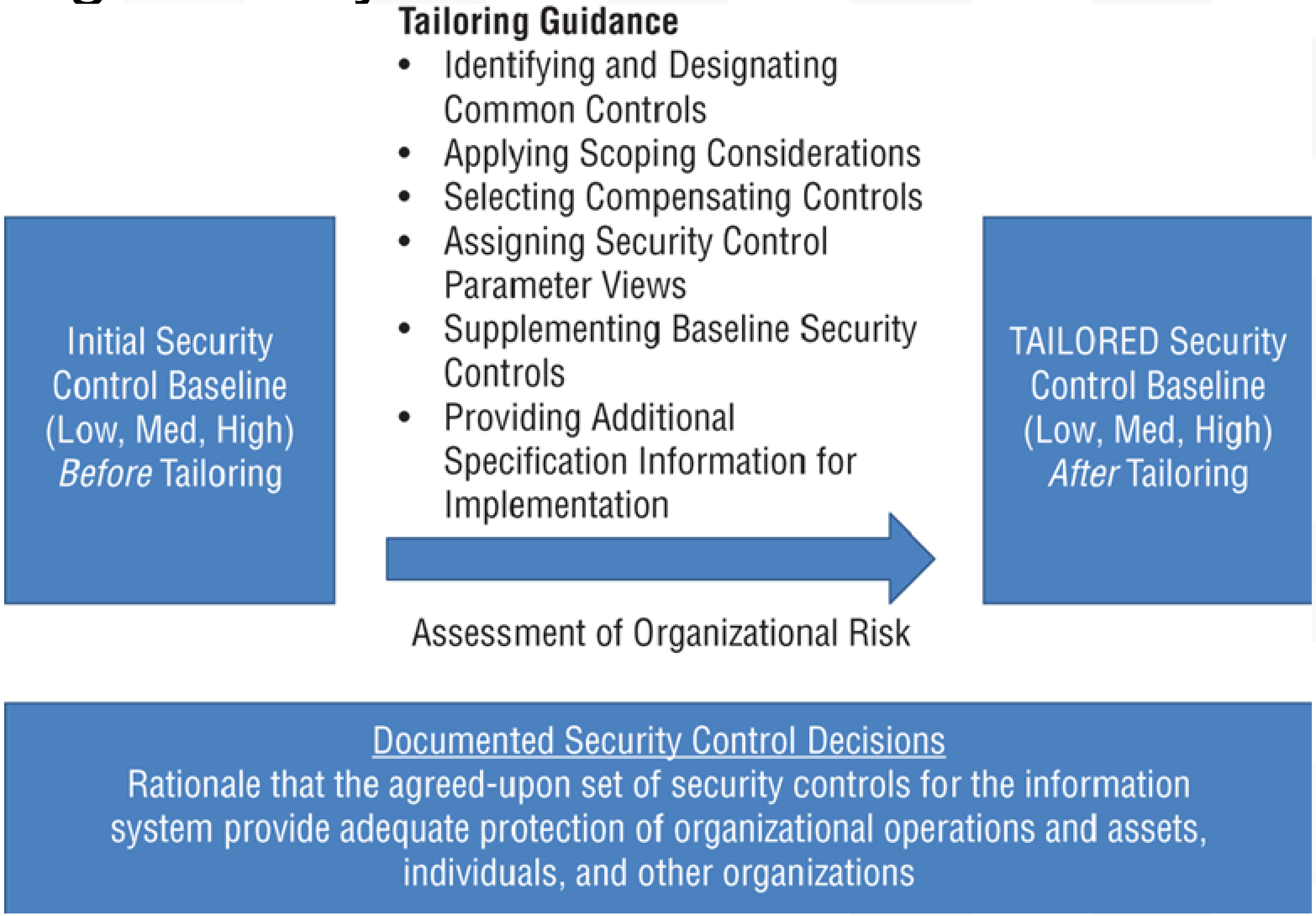
- Not synonymous
- Work together to build the configuration baseline.
- ***Scoping*** is the process the organization undertakes to consider which security controls apply and what assets they need to protect.
- ***Tailoring*** is the process of modifying the set of controls to meet the specific characteristics and requirements of the organization.

Chapter 5: Protecting Security of Assets

Data Security Controls

Tailoring Process

Figure 2.8
from NIST SP800-53



Tailoring Guidance

- Identifying and Designating Common Controls
- Applying Scoping Considerations
- Selecting Compensating Controls
- Assigning Security Control Parameter Views
- Supplementing Baseline Security Controls
- Providing Additional Specification Information for Implementation

Initial Security Control Baseline (Low, Med, High) *Before* Tailoring

TAILORED Security Control Baseline (Low, Med, High) *After* Tailoring

Assessment of Organizational Risk

Documented Security Control Decisions

Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, and other organizations

Convenience is not a factor for removing or altering security controls. Make sure any changes to baseline requirements are rationalized against operational requirements and are analyzed for impact to risk

Chapter 5: Protecting Security of Assets

John is unable to apply a vendor update to a critical vulnerability. What could he use in lieu of a patch?

A. Role-based access controls.

B. Security Event and Information Systems (SIEM).

C. CIS Baselines.

[✓ D. Compensating Security Controls]

Chapter 5: Protecting Security of Assets

Data Security Controls

Scoping & Tailoring – *Compensation Security Controls*

- The entity uses an alternative method to achieve the same result.
- NIST Definition: The security and privacy controls implemented in lieu of the controls in the baselines that provide equivalent or comparable protection for a system or organization.
- PCI: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other control

Chapter 5: Protecting Security of Assets

Data Security Controls

Scoping & Tailoring – *Compensation Security Controls*

PCI: Compensating controls must:

- Meet the intent and rigor of the originally stated PCI DSS requirement
- Provide a similar level of defense as the original PCI DSS requirement
- Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
- Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement."

Chapter 5: Protecting Security of Assets

Data Security Controls & Compliance Requirements

Standards Selection – *Security Frameworks*

- U.S. Department of Defense Instruction (DoDI): DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" (www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf)
- NIST SP 800-37, "Risk Management Framework" (csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)
- NIST Cybersecurity Framework (CSF) (www.nist.gov/cyberframework)
- UK 10 Steps to Cyber Security (www.ncsc.gov.uk/collection/10-steps)

Chapter 5: Protecting Security of Assets

Data Security Controls & Compliance Requirements

Standards Selection – *Security Standards*

In addition to frameworks and industry-specific standards (PCI DSS, HIPAA, GDPR)

- NIST SP 800-53 rev 5, "Security and Privacy Controls for Federal Information Systems and Organizations"
  (csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)
  SP800-53A rev5 (csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final)
  SP800-53B (https://csrc.nist.gov/publications/detail/sp/800-53b/final)
- FIPS Pub 199 "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS Pub 200 "Minimum Security Requirements for Federal Information and Information Systems"

Chapter 5: Protecting Security of Assets

Data Security Controls & Compliance Requirements

Standards Selection – *Security Standards*

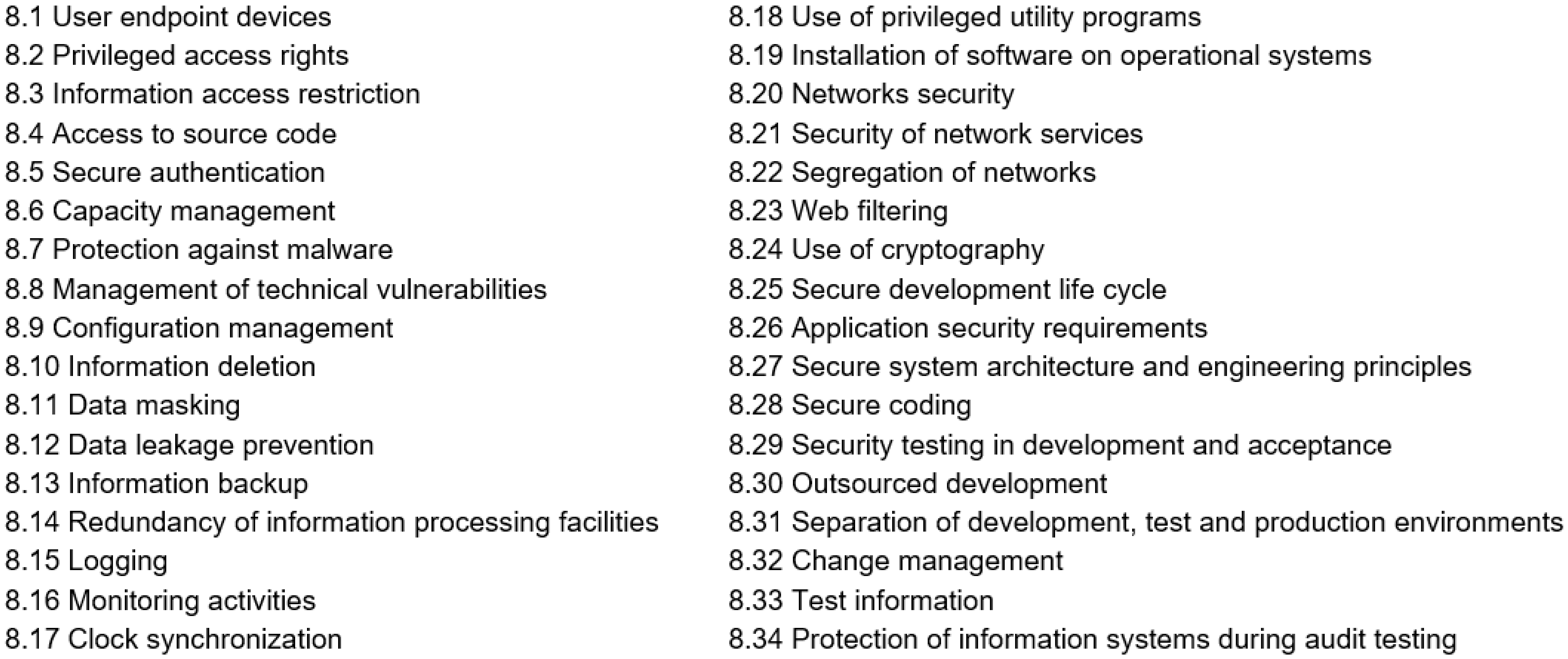
ISO 2700X Family

- ISO 27001, "Information technology – Security techniques – Information security management systems – Requirements"" (www.iso.org/isoiec-27001-information-security.html)
- ISO 27002, "Information Technology: Security techniques – Code of practice for information security controls" (https://www.iso.org/standard/75652.html) □ New version

ISO Standards are copyrighted

Chapter 5: Protecting Security of Assets

ISO/IEC 27002:2022 – Section 8, Technical Controls



8.1 User endpoint devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities
8.17 Clock synchronization
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Networks security
8.21 Security of network services
8.22 Segregation of networks
8.23 Web filtering
8.24 Use of cryptography
8.25 Secure development life cycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles
8.28 Secure coding
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit testing

Chapter 5: Protecting Security of Assets

Data Protection Methods

Digital Rights Management

- A set of tools and processes focused on controlling the use, modification, and distribution of intellectual property (IP) throughout its lifecycle.
- DRM allows you to restrict access, editing, copying, and printing of your digital assets.
- *Information rights management* (IRM) - more broadly protects data from unauthorized access by controlling who can view, copy, delete, or otherwise modify data.

Chapter 5: Protecting Security of Assets

Data Protection Methods

Data Loss Prevention (DLP)

aka Data Leakage Protection

- Set of technologies and practices used to ensure that sensitive data is not lost or accessed by unauthorized parties.
- Analyzes data storage, identifies sensitive data elements, and prevents users from accidentally or intentionally transmitting sensitive data.

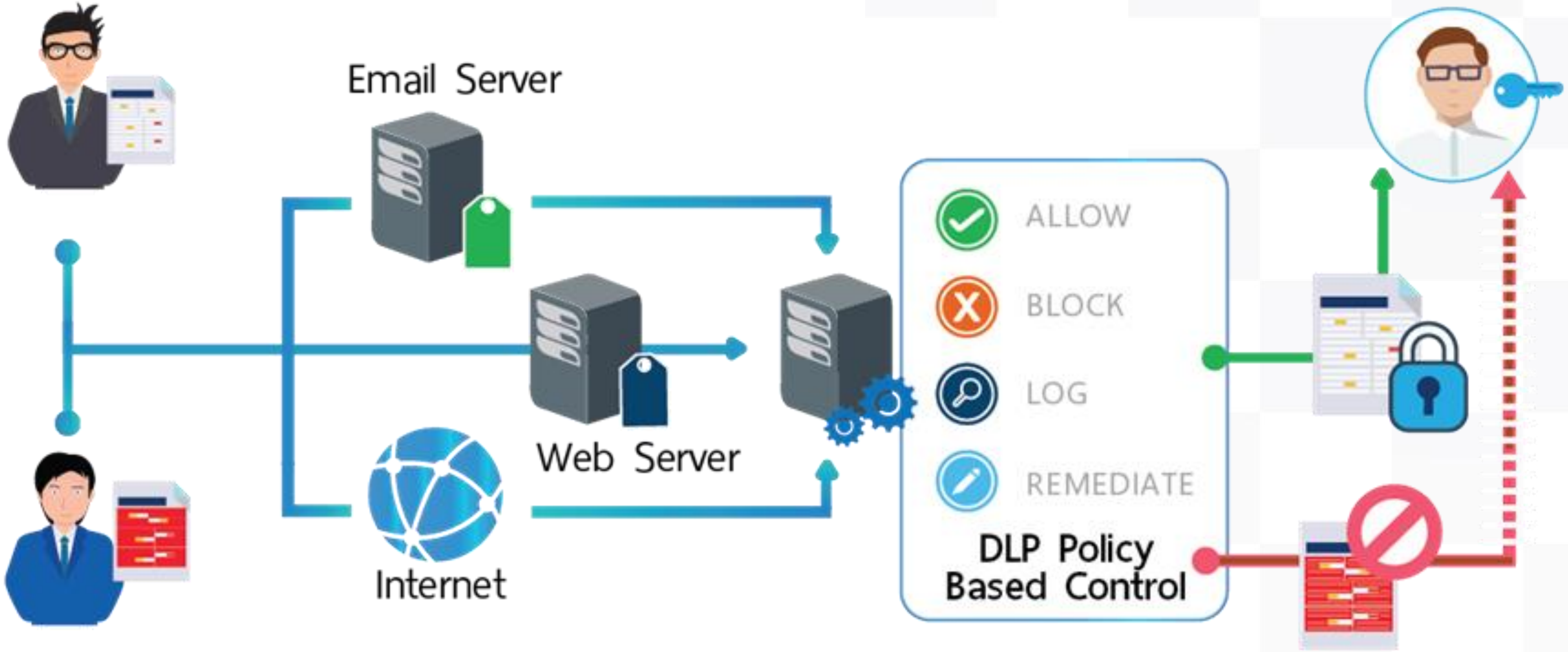
Tip: Protect data where it lives and travels.
This means that you might need to have multiple types of DLP controls from Endpoint to Network and to the Cloud services.
They might each function in a different manner, and understanding how they function would be fundamental to you DLP protection program overall.

Chapter 5: Protecting Security of Assets

Data Protection Methods

Data Loss Prevention (DLP)

aka Data Leakage Protection



Chapter 5: Protecting Security of Assets

Data Protection Methods

Data Loss Prevention (DLP)

3 Core Stages:

1. Discovery & Classification
2. Monitoring
3. Enforcement

Chapter 5: Protecting Security of Assets

Data Protection Methods

Data Loss Prevention (DLP)

aka Data Leakage Protection

DLP during 3 States of Data:

1. DLP at Rest – Wherever data is stored
2. DLP in Transit – Network-based DLP
3. DLP in Use – Host-based DLP

Chapter 5: Protecting Security of Assets

Data Protection Methods

Cloud Access Security Broker (CASB)

Software application that sits between cloud users and cloud services and applications.

Actively monitor all cloud activity and implement centralized controls to enforce security.

Data travels both in motion & can be at at rest

Chapter 5: Protecting Security of Assets

Data Protection Methods

Cloud Access Security Broker (CASB)

4 Functions:

1. Visibility – Provide insight into cloud usage
2. Data Security – Monitor & help prevent data exfiltration
3. Threat Protection
4. Compliance

Chapter 5: Protecting Security of Assets

Data Protection Methods

Cloud Access Security Broker (CASB)

3 Primary Types of CASB:

1. *Forward Proxy* – Resides on end-points, inspects and forwards cloud traffic for the user. Requires install of certificates.
2. *Reverse Proxy* – Integrates into identity services. Inline monitoring.
3. *API-based* – Monitors data within the cloud itself, rather than on a perimeter-based proxy

Chapter 5: Protecting Security of Assets

Data Protection Methods

Integrity Checking

Not mentioned in Chapter

- File Integrity Monitoring (FIM)
- Verifies integrity of systems and files
- Comparing against trusted baselines
- Works with change management procedures.

Chapter 5: Protecting Security of Assets

What's the difference between ignorance and apathy?

Don't know,
Don't care.

Chapter 5: Protecting Security of Assets – Pop Quiz

Which of the following statements is true about the information life cycle?

A. The information life cycle always begins with governance and ends with its recovery.

B. Most information must be retained indefinitely.

★ C. The information life cycle begins with its acquisition/generation and ends with its disposal/destruction.

D. Preparing information for use does not typically involve adding metadata.

Chapter 5: Protecting Security of Assets – Pop Quiz

This is a set of technologies and practices used to ensure that sensitive data is not lost or accessed by unauthorized parties?

A. File Integrity Monitoring (FIM).

[✓ B. Data Loss Prevention (DLP).]

C. Cloud Access Security Broker.

D. Compensating security controls (CSC).

Chapter 5: Protecting Security of Ass

YAY! 👍
Another Domain done!

Topics:

- Identify and Classify Information and Assets
- Establish Information and Asset Handling Requirements
- Provision Resources Securely
- Manage Data Lifecycle
- Ensure Appropriate Asset Retention
- Determine Data Security Controls and Compliance Requirements

Questions on Domain 2?