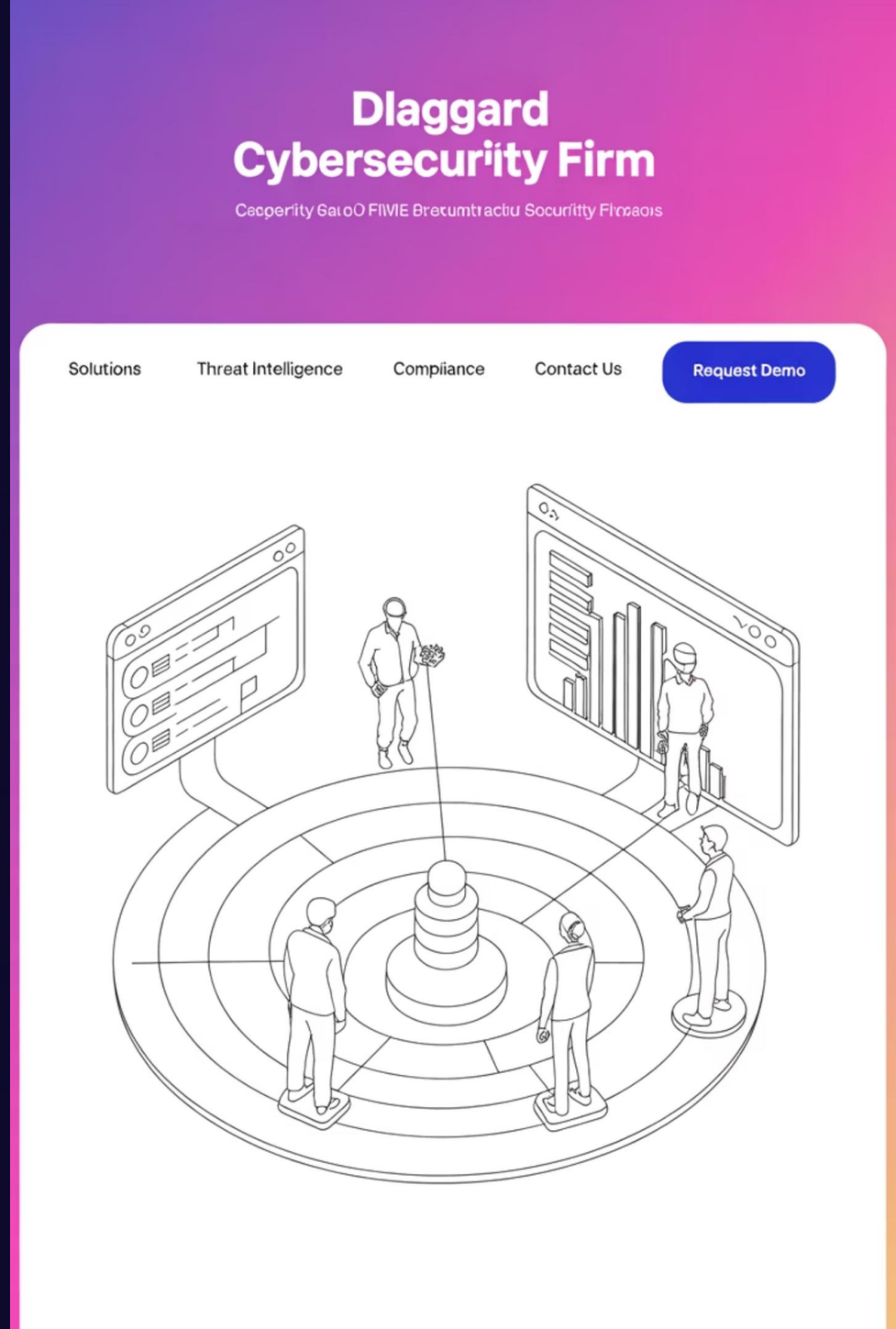
Security Governance, Risk Management, and Ethics Foundation

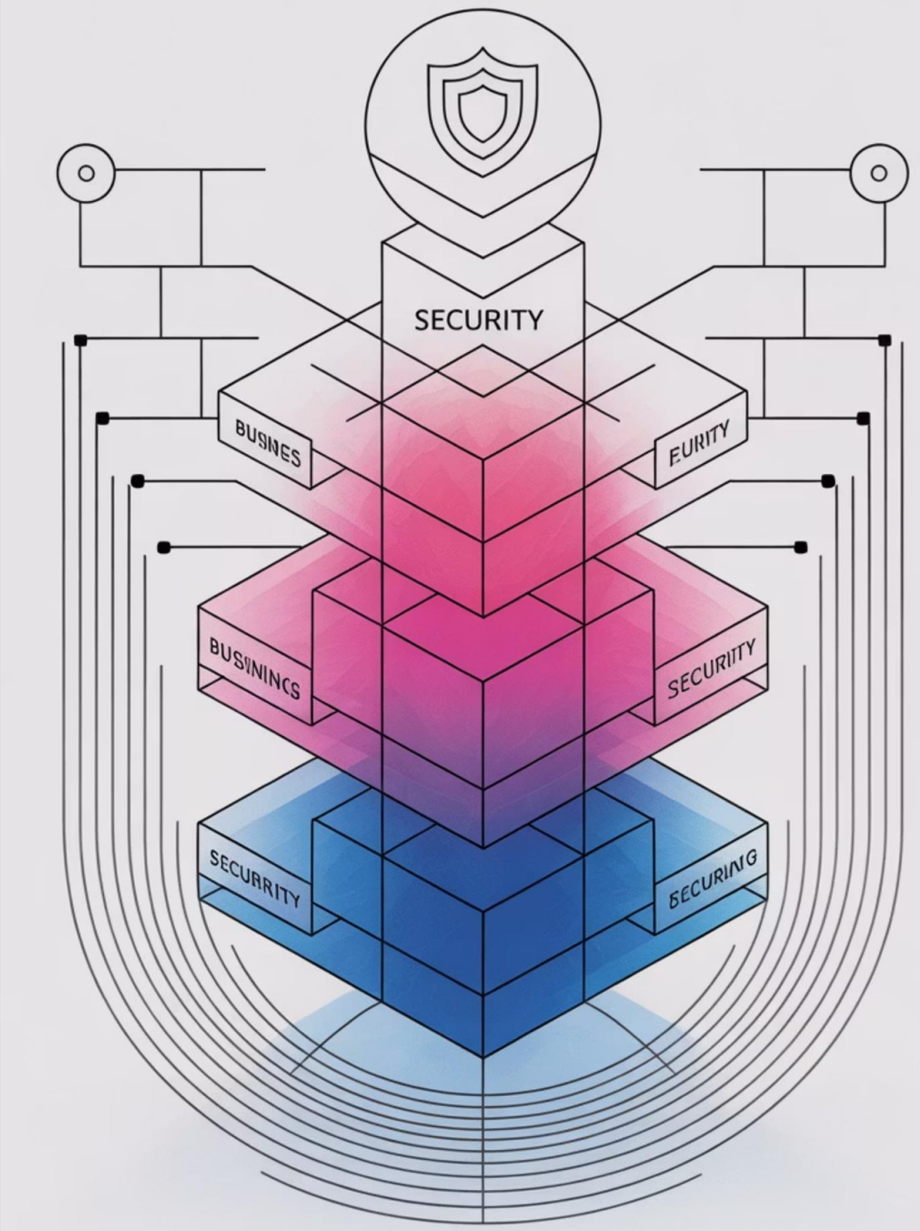
To strategically align information security with enterprise objectives, establish rigorous policy and governance frameworks, and apply formal risk assessment methodologies to ensure due diligence and due care are maintained.

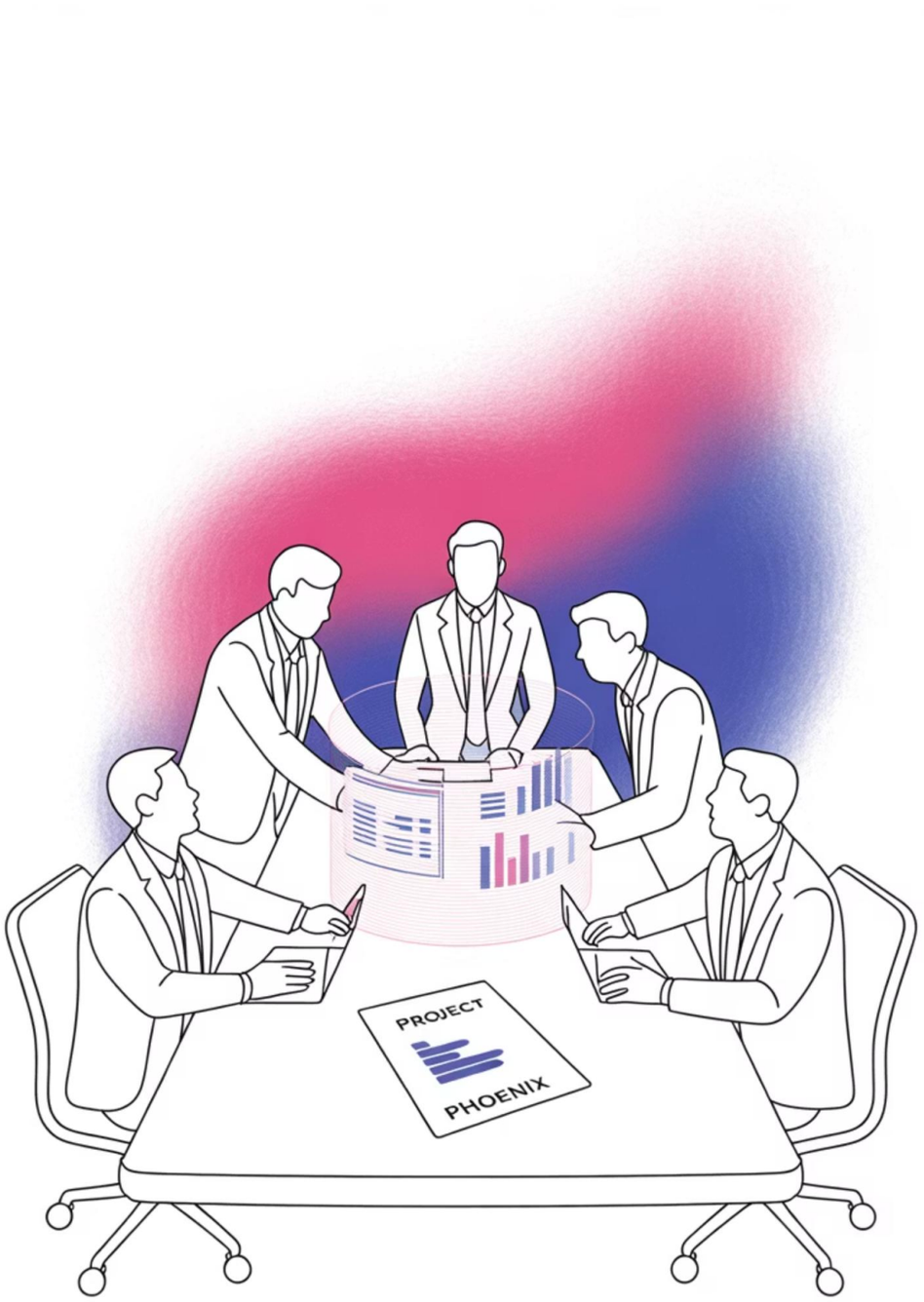


Governance, Documentation, and Risk Strategy

Strategic Alignment and Governance Structure (GOVERN Function)

The foundation of effective security governance begins with establishing clear structures that align security initiatives with business objectives whilst maintaining rigorous oversight and accountability.



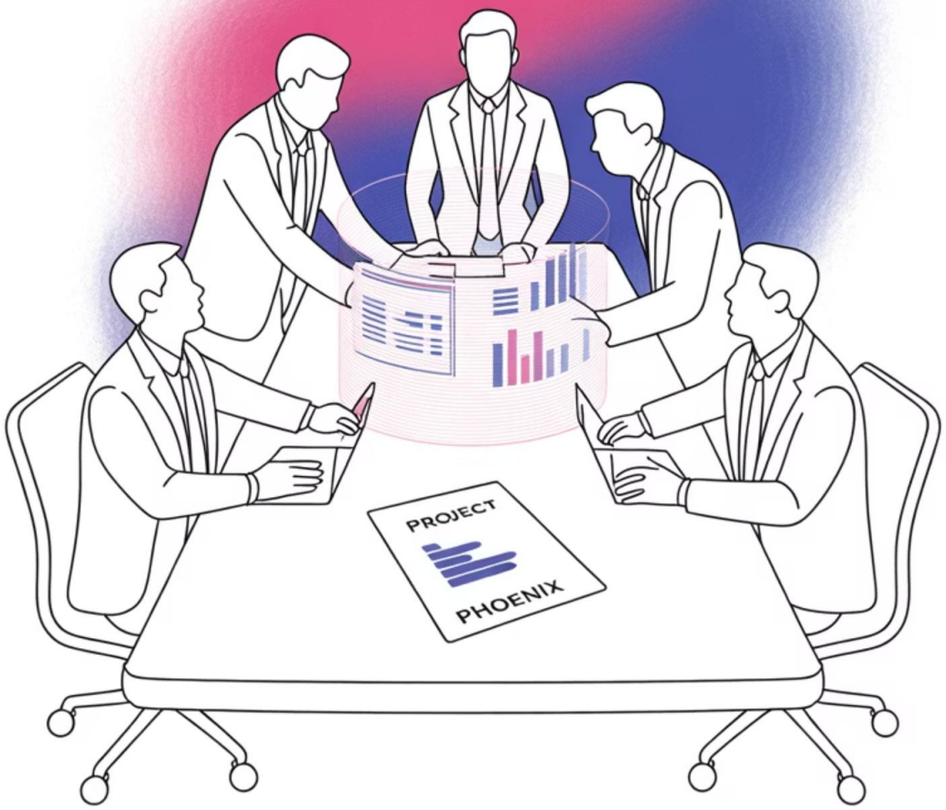


1. Align Security with Business Objectives

Safeguard Action: Ensure the security function aligns with the organisation's strategy, goals, mission, and objectives.

Implementation Steps: Define the Organisational Context (GV.OC) to document high-level facts and assumptions for defining the scope of security initiatives.

Best Practice Value/Impact: Transforms information security and privacy from being seen purely as a cost into a component that delivers business wins. Guarantees that security efforts support business continuity and enterprise goals.



The Organisational Context (GV.OC) is a Category focused on understanding the **circumstances** surrounding the organisation's cybersecurity risk management decisions

- The **mission** of the organisation.
- **Stakeholder expectations**.
- **Dependencies**.
- **Legal, regulatory, and contractual requirements**

Identifier	Description
GV.OC-01	The **organizational mission** is understood and informs cybersecurity risk management
GV.OC-02	**Internal and external stakeholders** are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
GV.OC-03	**Legal, regulatory, and contractual requirements** regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
GV.OC-04	**Critical objectives, capabilities, and services that external stakeholders depend on or expect** from the organization are understood and communicated
GV.OC-05	**Outcomes, capabilities, and services that the organization depends on** are understood and communicated

2. Establish a Formal Policy Structure

Safeguard Action: Develop a hierarchy of documentation starting with Policies (high-level intent, 'what' and 'why'). Follow with Standards (compulsory requirements, setting minimum security levels), and detailed Procedures (step-by-step 'how-to' instructions for consistency).

Best Practice Value/Impact: Provides clarity, consistency, and adaptability. Standardisation and consistency of results ensured by procedures. Makes it easier to update and redistribute changes by separating documentation types.

01

Policies

High-level intent, 'what' and 'why'

02

Standards

Compulsory requirements, setting minimum security levels

03

Procedures

Step-by-step 'how-to' instructions for consistency

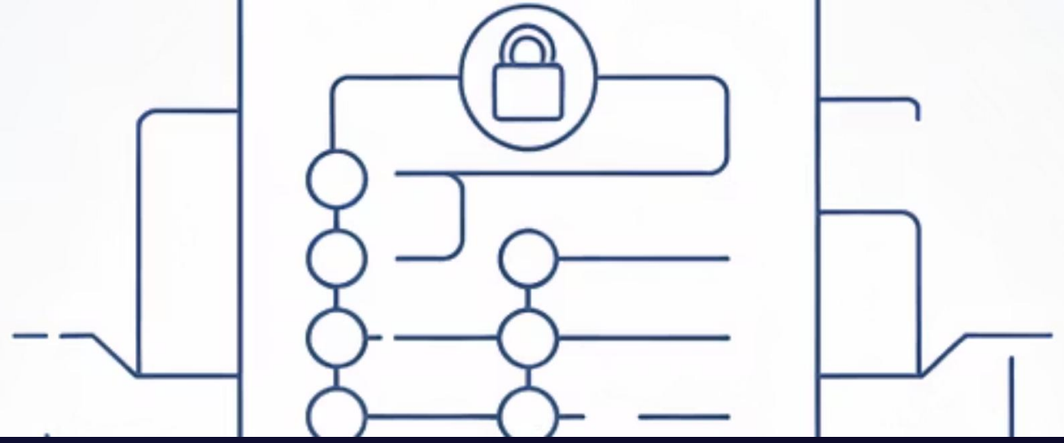
Baseline, Guideline?

3. Define and Assign Accountability

Safeguard Action: Determine and document organisational roles and responsibilities (GV.RR). Roles often include the Data Owner (defining classification), Custodian (protection/implementation), and Users.

Best Practice Value/Impact: Ensures actions are traceable and that day-to-day responsibilities are clearly allocated. This allocation is fundamental to maintaining accountability.

Data Owner	Custodian	Users
Defining classification	Protection/implementation	Day-to-day operations



Implementing an Information Security Management System

4. Adopt a Recognised Management Framework

Safeguard Action: Use a globally recognised standard like ISO 27001:2013 to establish, implement, maintain, and continually improve the ISMS. Utilise ISO 27002 for guidance on implementing the necessary controls.

Best Practice Value/Impact: Allows the organisation to achieve independent highly respected certification demonstrating commitment to stakeholders. Following a comprehensive framework results in a higher return on investment (RoI).

5. Integrate Compliance Requirements

Safeguard Action: Determine compliance and other requirements (legal, regulatory, contractual, and industry standards) applicable to the organisation. Fulfil security duties based on the multi-level protection system for cybersecurity (MLPS) when handling data through information networks.

Best Practice Value/Impact: Ensures systems meet baseline security requirements required by authorities, such as the CMMC Level 1 practices for safeguarding Contract Information. Helps achieve the foundational principles of **Legality, Propriety, and Necessity** in handling personal information.

6. Demonstrate Due Diligence and Due Care

Safeguard Action: Practice due diligence by establishing the necessary plan, policy, and processes. Demonstrate due care by performing the specific individual activities required to maintain security, aligning with the "prudent person rule".

Best Practice Value/Impact: Provides legal and ethical defence by showing management established and executed measures to protect organisational interests. **Crucial for preventing legal liabilities and criminal prosecution related to breaches.**

1

Due Diligence

Establishing necessary plan, policy, and processes

2

Due Care

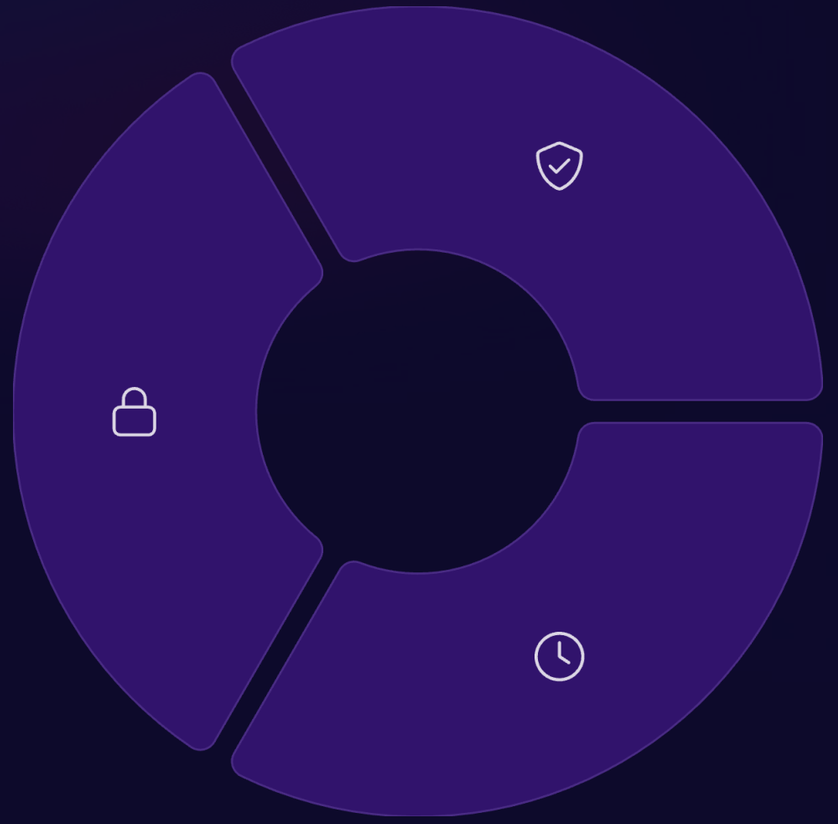
Performing specific activities to maintain security

Formal Risk Management Practices (IDENTIFY Function)

7. Perform Risk Assessment based on CIA

Safeguard Action: Conduct an identification and evaluation of risks based on impacts to Confidentiality, Integrity, and Availability (CIA). Incorporate other concepts like authenticity and nonrepudiation.

Best Practice Value/Impact: Ensures focus is placed on fundamental security objectives. Allows risks to be quantified based on potential impact, such as loss of valuable information (financial, personal, contracts).



Integrity

Ensuring information accuracy and completeness

Confidentiality

Protecting information from unauthorised access

Availability

Maintaining accessible and usable information

8-10. Advanced Risk Management Implementation

8. Quantify Risk Exposure (Quantitative Analysis): Inventory assets and assign an Asset Value (AV). For each asset-threat pair, calculate the Exposure Factor (EF) and Annualised Rate of Occurrence (ARO). Calculate the Annualised Loss Expectancy (ALE) using the formula: ALE = SLE * ARO (where SLE = AV * EF). Provides objective (more so than qualitative), financially driven data to justify security spending.

9. Manage Supply Chain Risk (SCRM): Apply SCRM concepts. This involves assessing and monitoring third parties. When working with service providers (TPSPs), ensure a written agreement defines their security responsibilities Reduces risks associated with hardware, software, and services inherited from external parties.

10. Apply Risk Treatment (Controls): Select countermeasures based on whether the risk is managed through mitigation, transfer, avoidance, or acceptance. Implement preventive controls (to avert incidents), detective controls (to discover incidents), and corrective controls (to remedy circumstances after an event). Reduces total risk to an acceptable residual risk. Applying multiple layers (Defence in Depth) ensures a single failed control does not compromise the system.

Note

Quantify Risk Exposure, or Quantitative Risk Analysis, is a risk assessment methodology that assigns real dollar figures to the loss of an asset and is based on mathematical calculations. The end result of the quantitative method is a report that contains numeric indications of relative risk potential, specifically dollar figures for levels of risk, potential loss, cost of countermeasures, and the value of safeguards.

Major Steps in Quantitative Risk Analysis

1. **Inventory assets** and assign an **Asset Value (AV)**.
2. Research each asset and list all possible threats, resulting in **asset-threat pairings**.
3. Calculate the **Exposure Factor (EF)** for each asset-threat pairing.
4. Calculate the **Single Loss Expectancy (SLE)** for each asset-threat pairing.
5. Perform a threat analysis to calculate the **Annualized Rate of Occurrence (ARO)** for each threat.
6. Derive the overall loss potential per threat by calculating the **Annualized Loss Expectancy (ALE)**.
7. Research countermeasures and calculate the changes to ARO, EF, and ALE based on applying a countermeasure.
8. Perform a **cost/benefit analysis** of each countermeasure for each threat for each asset, then select the most appropriate response.

Note

Term	Definition
Asset Value (AV)	A dollar figure assigned to an asset based on factors such as its importance, use in critical processes, actual cost, and nonmonetary expenses.
Exposure Factor (EF)	The percentage of loss that an organization would experience if a specific asset were violated by a single realized risk. It is expressed as a percentage.
Single-Loss Expectancy (SLE)	The potential loss associated with a single realized threat against a specific asset, expressed in a dollar value.
Annualized Rate of Occurrence (ARO)	The expected frequency with which a specific threat or risk will occur (become realized) within a single year. This is also known as a probability determination and is expressed as a number per year.
Annualized Loss Expectancy (ALE)	The **possible yearly loss** of all instances of a specific realized threat against a specific asset. The largest ALE is considered the biggest problem the organization faces and the first risk to be addressed. ALE = SLE * ARO or ALE = AV * EF * ARO

Note

Cybersecurity Maturity Model Certification (CMMC) Level 1 practices organised by domain. Level 1 focuses on basic cyber hygiene to protect Contract Information:

Access Control (AC)

- **AC.L1-3.1.1**: Limit information system access to authorised users
- **AC.L1-3.1.2**: Limit information system access to the types of transactions and functions that authorised users are permitted to execute

Identification and Authentication (IA)

- **IA.L1-3.5.1**: Identify information system users, processes acting on behalf of users, or devices
- **IA.L1-3.5.2**: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organisational information systems

Note

Media Protection (MP)

- **MP.L1-3.8.1**: Protect (i.e., physically control and securely store) information system media containing Federal Contract Information, both paper and digital
- **MP.L1-3.8.2**: Limit access to information on information system media to authorized users
- **MP.L1-3.8.3**: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse

Physical Protection (PE)

- **PE.L1-3.10.1**: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals
- **PE.L1-3.10.3**: Escort visitors and monitor visitor activity
- **PE.L1-3.10.4**: Maintain audit logs of physical access
- **PE.L1-3.10.5**: Control and manage physical access devices

Note

System and Communications Protection (SC)

- **SC.L1-3.13.1**: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems
- **SC.L1-3.13.5**: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks

System and Information Integrity (SI)

- **SI.L1-3.14.1**: Identify information system flaws and take corrective action
- **SI.L1-3.14.2**: Provide protection from malicious code
- **SI.L1-3.14.4**: Update malicious code protection mechanisms
- **SI.L1-3.14.5**: Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed

Note

1. Legality

Personal information must be processed in accordance with laws and regulations. This means:

- Having a valid legal basis for processing (such as consent, contract performance, legal obligations, etc.)
- Following prescribed procedures and requirements
- Not using illegal means to collect or process personal information
- Complying with all applicable laws and regulations throughout the processing lifecycle

2. Propriety

Personal information processing must be legitimate and justified, which requires:

- Having genuine and reasonable purposes for processing
- Processing methods that are appropriate and not excessive
- Maintaining transparency about processing activities
- Ensuring the processing aligns with reasonable expectations of data subjects
- Not using personal information for improper or unethical purposes

Note

. Necessity

Personal information processing must be limited to what is necessary, encompassing:

- Collecting only the minimum amount of personal information needed to achieve the stated purpose
- Limiting the scope of processing to what is essential
- Implementing data minimization principles
- Not over-collecting or over-retaining personal information
- Ensuring processing methods have the least impact on individual rights and interests