MIS761
Cyber Security Strategies

Dept. of Information Systems & Business Analytics

Deakin Business School

Week 8 –Security Governance, Policies and Outsourcing

AACSB
ACCREDITED

DEAKIN
BUSINESS
SCHOOL

Information Security Governance

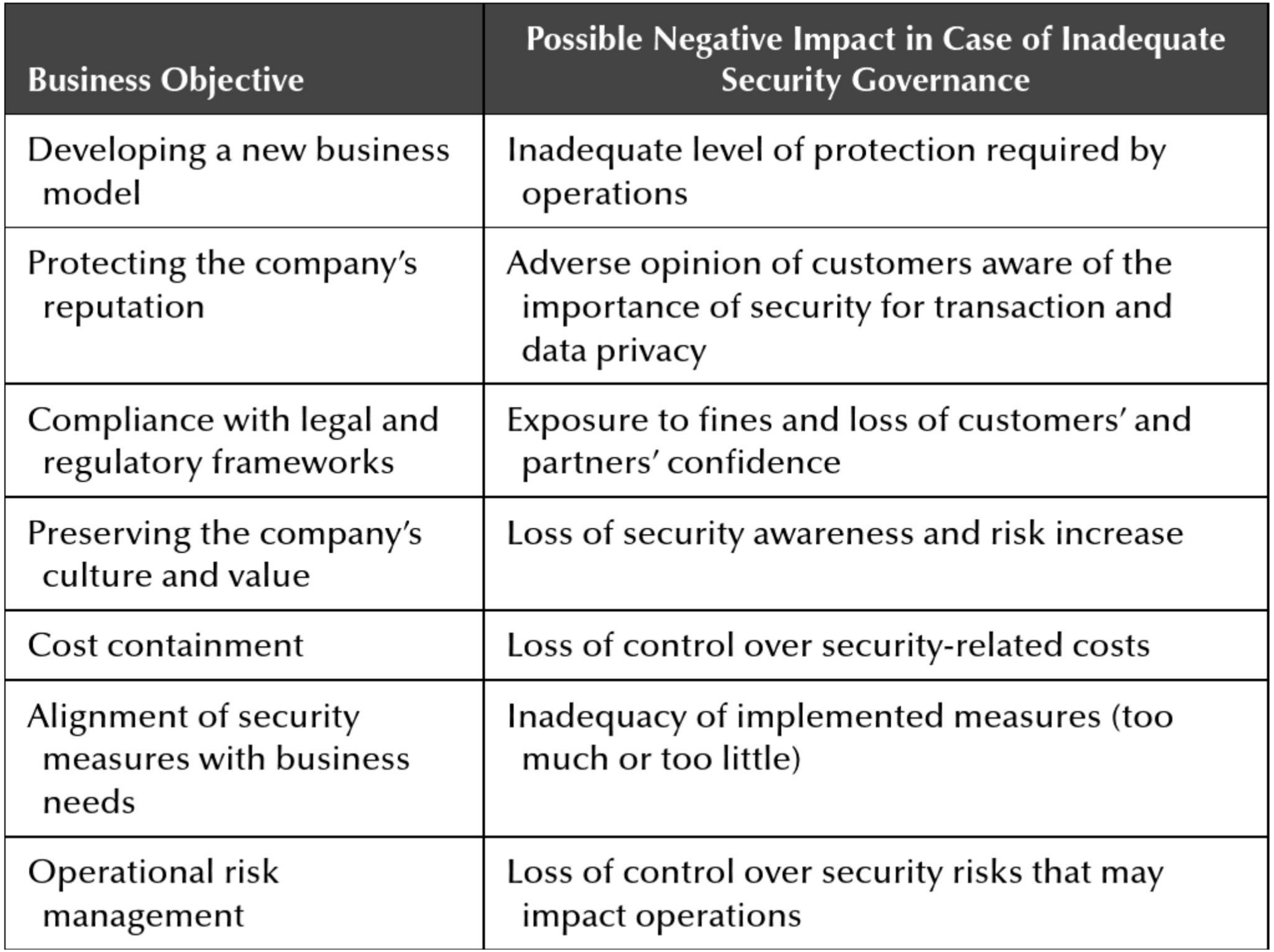
- **Security Governance is the system by which an organization's information security activities are directed and controlled.**
  - establishing a culture of security
  - setting strategic directions for security
  - making decisions,
  - and monitoring
- **Distinguish from Information Governance and IT Governance:**
  - Security Governance concentrates on managing risks related to information and its supporting IT infrastructure.
- **Why another Governance:**
  - May not be adequately addressed in IG/ITG
  - A more targeted focus on protecting the organization from security threats and vulnerabilities.

Objectives of Security Governance

Security governance must contribute to the following five objectives (Guidance for Information Security Managers, ITGI 2008):

- 1. Strategic alignment of information security with business strategy to support organizational objectives.
- 2. Effective risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
- 3. Value delivery by optimizing information security investments in support of organizational objectives.
- 4. Resource management by using information security knowledge and infrastructure efficiently and effectively.
- 5. Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure achievement of organizational objectives.

Negative Effects of Inefficient IS Governance



Business Objective	Possible Negative Impact in Case of Inadequate Security Governance
Developing a new business model	Inadequate level of protection required by operations
Protecting the company's reputation	Adverse opinion of customers aware of the importance of security for transaction and data privacy
Compliance with legal and regulatory frameworks	Exposure to fines and loss of customers' and partners' confidence
Preserving the company's culture and value	Loss of security awareness and risk increase
Cost containment	Loss of control over security-related costs
Alignment of security measures with business needs	Inadequacy of implemented measures (too much or too little)
Operational risk management	Loss of control over security risks that may impact operations

IS Governance: Effective vs Ineffective

Indicators of Ineffective IS Governacne

- IS controls managed by one department.
- IS deemed exclusive responsibility of CISO/CIO.
- Board abstains from strategic IS decisions.
- IS officer lacks resources for policy enforcement.
- Business changes aren't security-risk assessed.
- Board lacks IS reports and its value assessment.
- Security officers feel unheard, unsupported, reactive.

Characteristics of Effective IS Governacne

- The whole company is involved
- Responsibilities are defined
- The level of protection depends on risk appetite
- Security is actively managed

Information Security Management vs. Governance

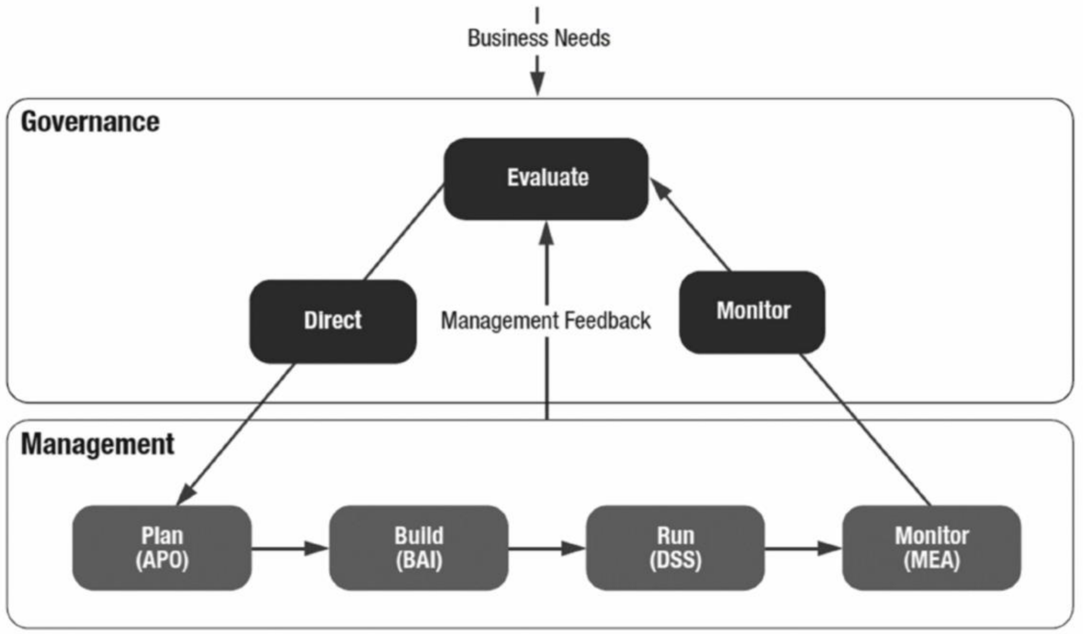
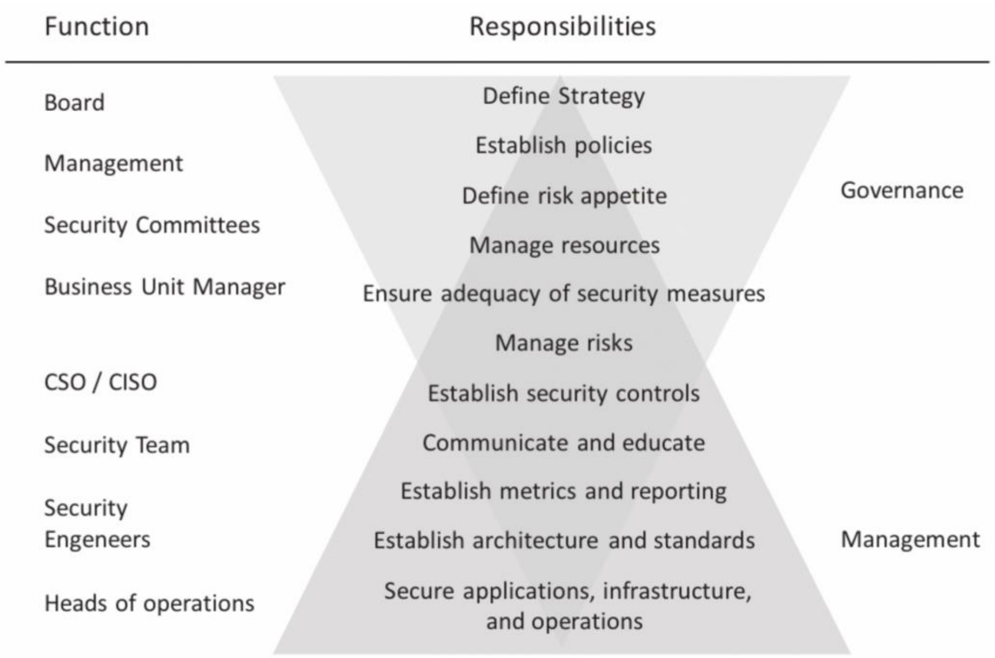


Figure 1.2 Distinction between governance and security management according to CobIT [CobIT5, "A Business Framework for the Governance and Management of Enterprise IT", ISACA, 2012].

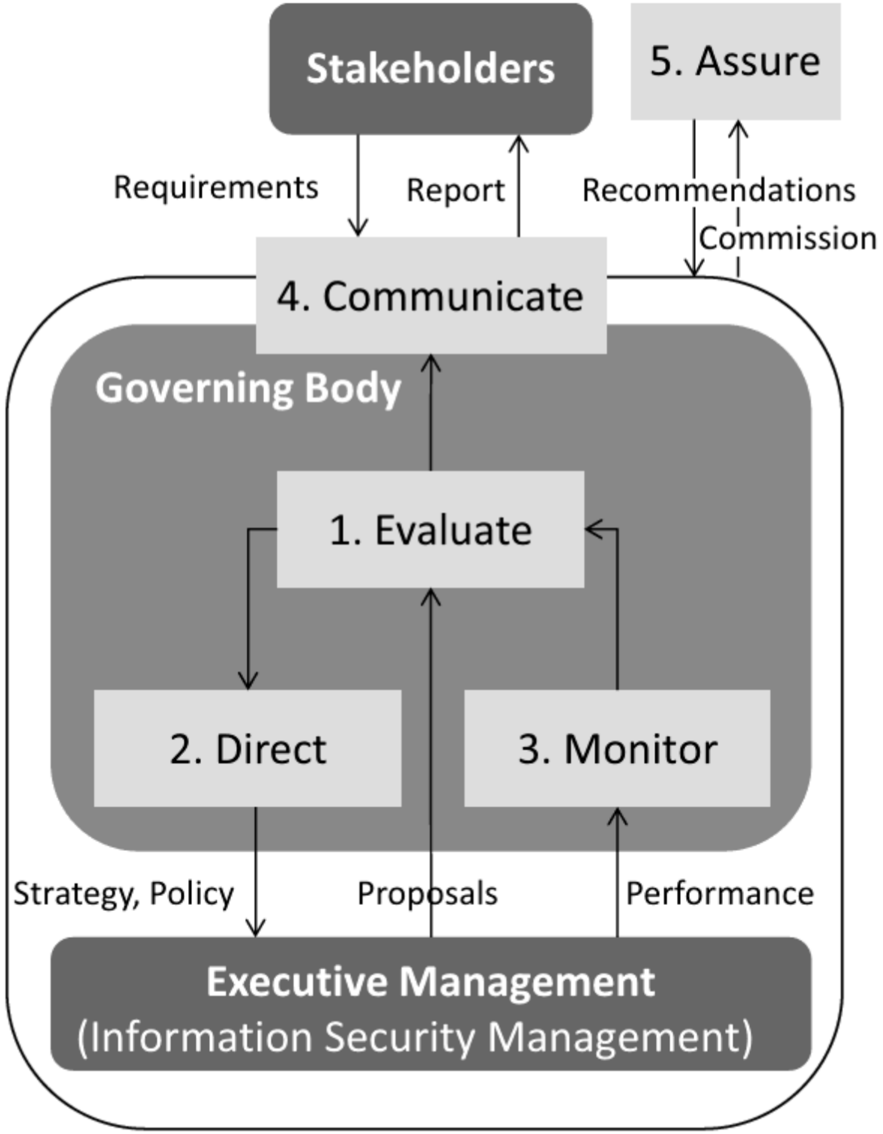


Function	Responsibilities	
Board	Define Strategy	
Management	Establish policies	
	Define risk appetite	Governance
Security Committees	Manage resources	
Business Unit Manager	Ensure adequacy of security measures	
	Manage risks	
CSO / CISO	Establish security controls	
Security Team	Communicate and educate	
Security Engeneers	Establish metrics and reporting	
	Establish architecture and standards	Management
Heads of operations	Secure applications, infrastructure, and operations	

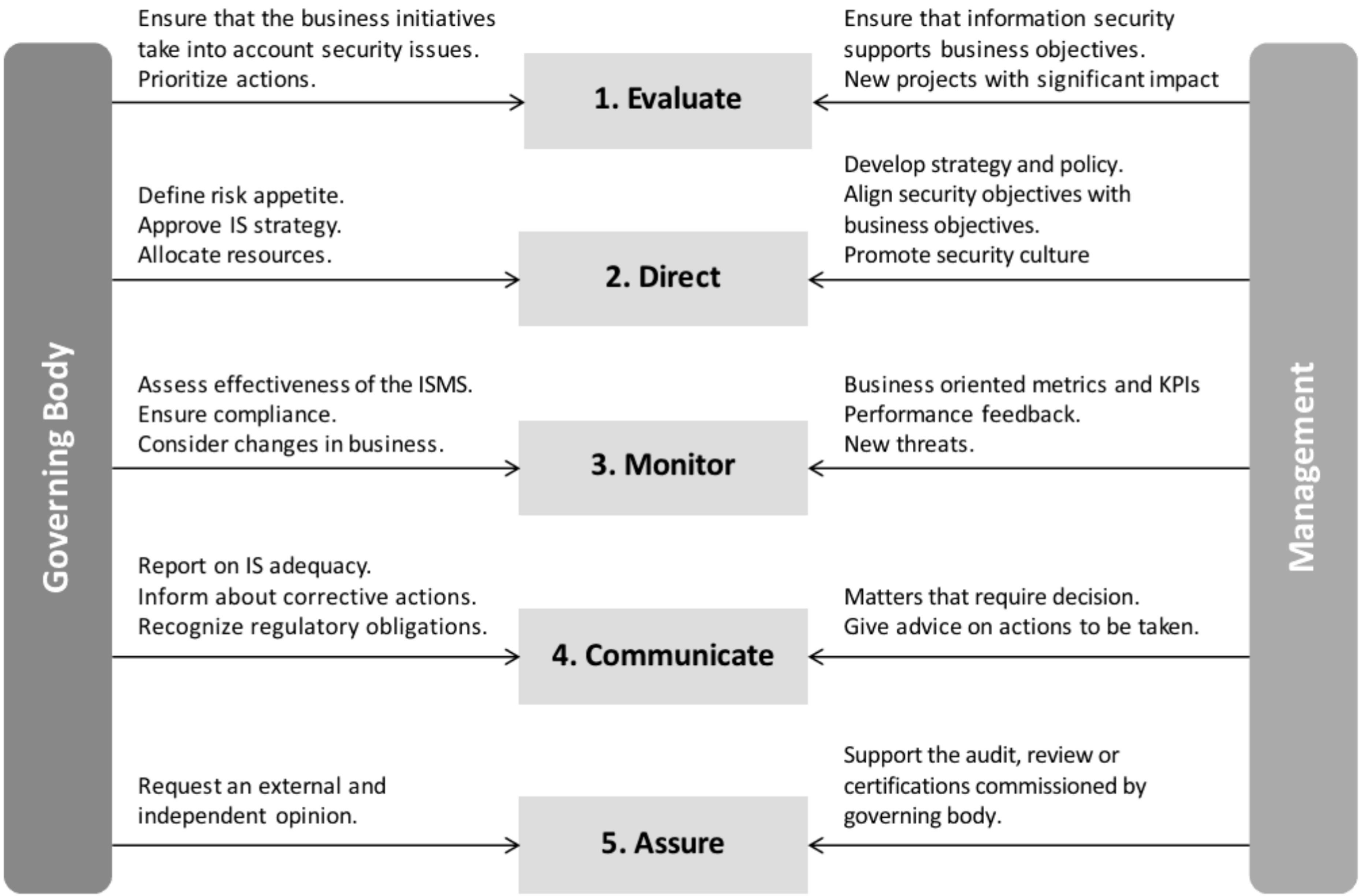
Figure 1.3 Distribution of responsibilities between governance and management.

ISO27014 Governance of Information Security

- Principle 1 : Establish organization-wide information security.
- Principle 2 : Adopt a risk-based approach.
- Principle 3 : Set the direction of investment decisions.
- Principle 4 : Ensure conformance with internal and external requirements.
- Principle 5 : Foster a security-positive environment.
- Principle 6 : Review performance in relation to business outcomes.



ISO27014 Governance of Information Security



Governing Body

Management

Ensure that the business initiatives take into account security issues.
Prioritize actions.

1. Evaluate

Ensure that information security supports business objectives.
New projects with significant impact

Define risk appetite.
Approve IS strategy.
Allocate resources.

2. Direct

Develop strategy and policy.
Align security objectives with business objectives.
Promote security culture

Assess effectiveness of the ISMS.
Ensure compliance.
Consider changes in business.

3. Monitor

Business oriented metrics and KPIs
Performance feedback.
New threats.

Report on IS adequacy.
Inform about corrective actions.
Recognize regulatory obligations.

4. Communicate

Matters that require decision.
Give advice on actions to be taken.

Request an external and independent opinion.

5. Assure

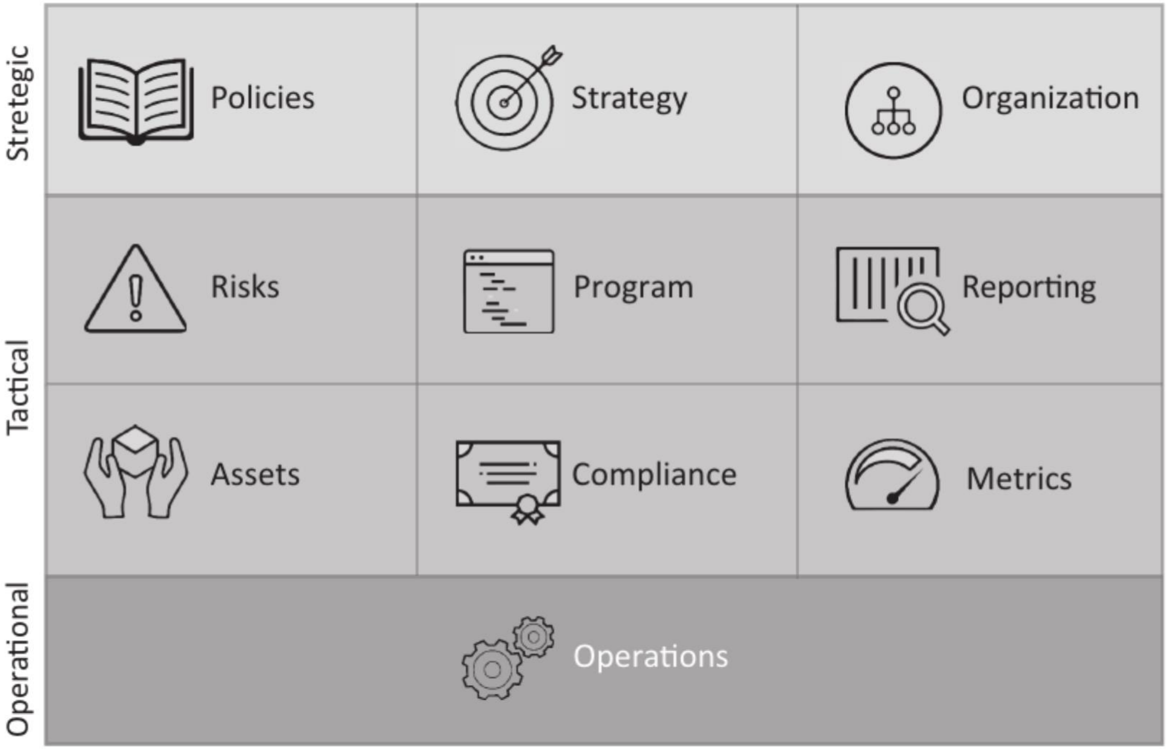
Support the audit, review or certifications commissioned by governing body.

Security Governance Control Framework

- **Standards like ISO27041 are good but …**
  - Challenges for for non-experts due to the mingling of high-level and operational security tasks.
  - Importance of distinguishing controls by levels of responsibility - governance, management, and operations.
- **Benefits of Security Governance Control Framework**
  - Facilitates easier comprehension and implementation of security governance.
  - Efficiently uncovers weak spots in security and guides improvement.
  - Ensures alignment of security strategies with business objectives.
  - Enables effective allocation and understanding of responsibilities.

Security Governance Control Framework -Responsibility Levels & Structure of Controls

- **Three-Level Control Approach**
  - Strategic Level: Provides overall direction for the security program.
  - Tactical Level: Sets up and manages the security program.
  - Operational Level: Handles operational and technical controls.
- **Problem with Unstructured Controls**
  - Misalignment wastes resources, causes misunderstanding.
  - Poor alignment obstructs understanding of program-business alignment.



Stretegic: Policies, Strategy, Organization

Tactical: Risks, Program, Reporting; Assets, Compliance, Metrics

Operational: Operations

Security Governance Control Framework - Roles of Different Actors

- **Board of Directors and Business Unit Heads**
  - Primarily involved at the strategic level.
  - Sets direction and assurance for the program.
- **CISO and Functional Managers**
  - Primarily involved at the tactical level.
  - Manages and steers the security program.
- **Security Specialists**
  - Primarily involved at the operational level.
  - Handles technical controls or processes.

Security Governance Control Framework
-Strategy in Security Governance

- **Importance of Strategy**
  - Defines vision and direction for IS program
  - Avoids inefficient, cost-heavy protective measures
- **Components of a Security Strategy**
  - Understanding external environment and business context
  - Acknowledging the legal and regulatory framework
  - Addressing changes in threats, vulnerabilities, and technologies
- **Consequences of Poor Strategy**
  - Increased costs and inefficiency
  - Misalignment with company objectives and management understanding

Security Governance Control Framework
-Policies in Security Governance

- **What Are Policies?**
  - Translate strategy into more restrictive terms
  - Guide for implementing security controls
- **How Policies Support the Business**
  - Reflect business needs and differing risk appetites
  - Serve various stakeholders: board, managers, security officers, auditors
- **Consequences of Poor Policies**
  - Misalignment with business needs
  - Ineffective control implementation and justifications

Security Governance Control Framework -Organization in Security Governance

- **Modern Security Organization**
  - No longer limited to appointing a CISO
  - Coordinating efforts across company: HR, Business Units, IT
- **Evolving Role of the CISO**
  - From head of user access rights to leading multidisciplinary teams
  - Ensures there's no conflict of interest, has sufficient authority
- **Consequences of Poor Organization**
  - Inability to achieve strategic objectives
  - Conflict of interest, ineffective decision-making

Understanding Internal Regulatory Frameworks

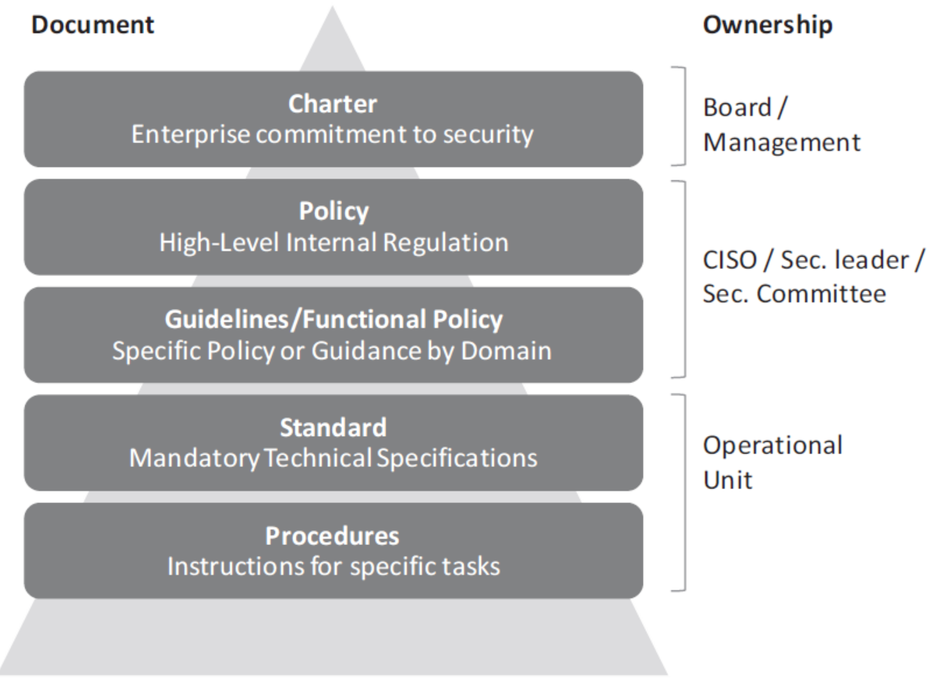
- An internal regulatory framework consists of a set of policies, guidelines, and lower-level instructions that establish rules for company operations to ensure the protection of assets.
- **Purpose:**
  - Serves as a governance tool translating strategic objectives into actionable security measures.
  - Provides a clear structure to support business operations while safeguarding confidentiality, integrity, and availability of information.
- **Importance:**
  - Aligns with business needs and supports operations.
  - Must be well-constructed with input from business units, free of gaps or ambiguities, and understood and endorsed by management.
  - Ensures consistent interpretation and application of security measures across the organization.

Understanding Internal Regulatory Frameworks

- **Characteristics:**
  - Comprehensive, consistent, enforceable, and accessible.
  - Resistant to technological changes and stable over time.
  - Reviewed and updated regularly to remain effective.
- **Implementation:**
  - Documents should be easily accessible, ideally hosted on an intranet for employee reference.
  - Regular reviews by designated committees to ensure relevance and accuracy.

Distinguishing Policies, Guidelines, and Standards

- **Charter:**
  - A high-level document outlining the overall vision, objectives, and risk appetite of the company.
  - Sets a clear mandate for security and is signed by top management.
- **Policy:**
  - Top-level documents that provide binding requirements and objectives set by management and the board.
  - Define the "what" and "why" of security efforts, outlining key principles, scope, and governance.



Document

Ownership

Charter
Enterprise commitment to security

Board / Management

Policy
High-Level Internal Regulation

Guidelines/Functional Policy
Specific Policy or Guidance by Domain

CISO / Sec. leader / Sec. Committee

Standard
Mandatory Technical Specifications

Procedures
Instructions for specific tasks

Operational Unit

Figure 5.1 Hierarchy of documents in a regulatory framework.

Distinguishing Policies, Guidelines, and Standards

- **Guideline:**
  - Mid-level documents that offer more detailed explanations of policies.
  - Describe security requirements for specific processes, business units, or areas, without naming specific technologies or products.
- **Standard:**
  - Detailed documents that translate policies and guidelines into specific operational terms.
  - Provide instructions for system users on security configurations, procedures, and compliance measures.
- **Procedures:**
  - The most detailed, lowest-level documents, often considered "recipes."
  - Provide step-by-step instructions for specific tasks like encryption, system hardening, and password management.

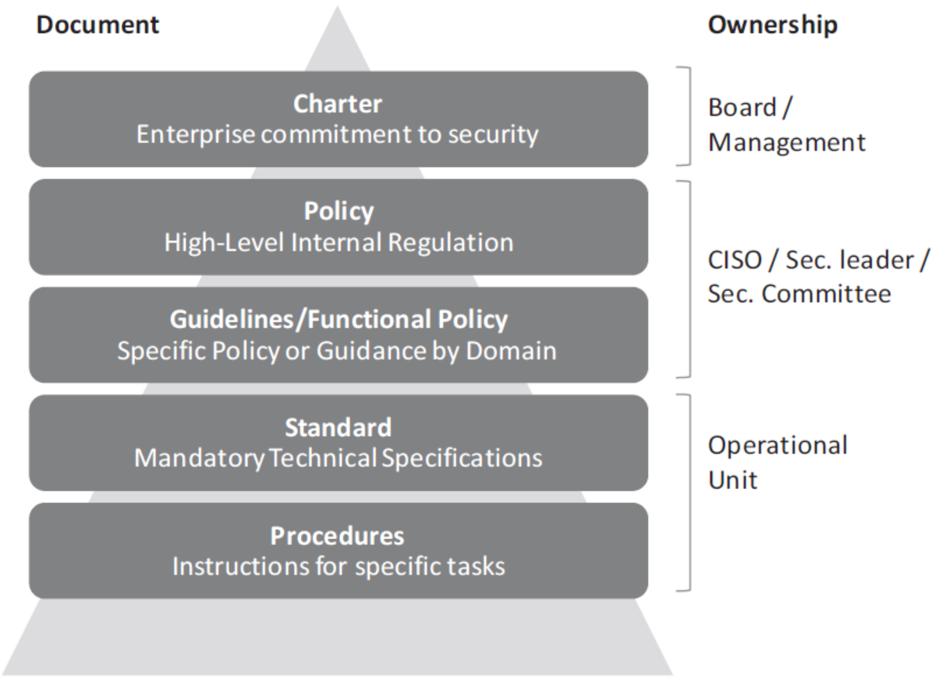

Document
Ownership
Charter
Enterprise commitment to security
Policy
High-Level Internal Regulation
Guidelines/Functional Policy
Specific Policy or Guidance by Domain
Standard
Mandatory Technical Specifications
Procedures
Instructions for specific tasks
Board / Management
CISO / Sec. leader / Sec. Committee
Operational Unit

Figure 5.1 **Hierarchy of documents in a regulatory framework.**

Distinguishing Policies, Guidelines, and Standards -Examples

- **IDENTITY AND ACCESS RIGHTS MANAGEMENT**
- **Security Charter:**
  - “ We advocate centralized management and the supervision of access rights … ”
- **At the policy or functional policy level:**
  - “ Access rights are assigned based on business roles … Business roles are established by business unit managers … Roles are built on the principle of least privilege (sufficient to perform a specific task) … Data Owners validate data access requests … The organization, roles and responsibilities are as follows … ”
- **At the standard level (operations):**
  - “ When authorization has been given by the employee’ s manager and HR, the operator triggers the privilege provision process on different platforms.”

- **DATA PROTECTION**
- **Security Charter:**
  - “ Our data must be protected according to their level of confidentiality … ”
- **At the policy or functional policy level:**
  - “ Data classification is as follows … Data protection rules by class are as follows … Any application processing data classified as highly confidential must use a strong authentication system … ”
- **At the standard level (operations):**
  - “ To develop applications using strong authentication the following standards should be used … ”

Organizing Regulatory Framework Documents Effectively

- **Importance of Organization:**
  - Facilitates understanding and acceptance by employees.
  - Strengthens governance and eases document maintenance.
- **Document Framework Structure:**
  - Large companies: Use a three-dimensional (Document Hierarchy, Business Unit/Sector, Security Domain) matrix to manage diverse business units and risk appetites.
  - Smaller companies: May use a simpler document summarizing rules and IT standards.
- **Common Mistakes:**
  - Accumulation of overlapping documents across different hierarchical levels.
  - Lack of clear organization and accessibility, making it harder to maintain.
- **Key Organization Principles:**
  - Clear hierarchy: Policies, guidelines, standards, procedures.
  - Accessibility: All documents should be easily accessible, ideally through the company intranet.
  - Differentiation: Use functional policies for specific domains with unique risks or regulations.
- **When to Use Functional Policies:**
  - Unique context or external conditions.
  - Specific risks, threats, or vulnerabilities.
  - Legal and regulatory requirements.
  - Distinct roles, responsibilities, or domain-specific controls.

Key Elements and Structure of a Security Policy

- **1. Introduction or Context:**
  - Defines the company's internal and external environment.
  - Explains the policy's purpose, scope, and importance.
  - Announces high-level security requirements.
- **2. Scope and Target Audience:**
  - Identifies who the policy applies to and who should follow it.
  - Outlines the principles and frameworks the policy is based on.
  - States the objectives and intent of the policy owners.
- **3. Positioning in Internal Framework:**
  - Shows where the policy fits within the company's broader regulatory framework.
- **4. Principles:**
  - Lists the fundamental security goals the policy aims to achieve.
- **5. Policy Statements:**
  - High-level declarations of policy objectives.
  - Explains the rationale and application of each statement.

Key Elements and Structure of a Security Policy

- **6. Organization, Roles, and Responsibilities:**
  - Details governance and management roles.
  - Defines responsibilities across the organization (RACI matrix).
    - Responsible, accountable, consulted and informed (RACI) matrix summarizing the responsibilities of all functions involved
- **7. Specific Area Orientations:**
  - Provides top-level guidance for key security areas (e.g., risk management, data protection).
- **8. Disciplinary Actions:**
  - Outlines consequences for noncompliance.
- **9. Review Process:**
  - Describes how and when the policy will be reviewed and updated.
- **10. Glossary:**
  - Clarifies specific terms used in the policy for better understanding.

Steps to Establish a Security Policy

- **1. Preparation:**
  - Understand business context, strategy, and security needs.
  - Identify and classify assets needing protection.
  - Review existing security risks and controls.
  - Decide on the framework architecture and accessibility.
  - Engage stakeholders from management, business units, and IT.
- **2. Policy Elaboration:**
  - Define security governance and management roles.
  - Identify key points needing clarity through a bottom-up approach.
  - Develop and validate the charter and general security policy.
  - Ensure policies are specific, measurable, realistic, and time-bound (SMART).
- **3. Developing Functional Policies or Guidelines:**
  - Form a team for each specific security domain.
  - Develop functional policies similar to general policies.

Steps to Establish a Security Policy

- **4. Establishing Standards:**
  - Use ISO 27001 (and Annex A) as checklists to ensure comprehensive coverage and completeness of the regulatory framework.
  - **Checklist for Developing the Regulatory Framework:**
    - ✓ **Granularity:** Are the documents detailed enough based on business needs?
    - ✓ **Coverage:** Have all necessary topics been addressed? Identify any gaps and plan corrections.
    - ✓ **Optimization:** Can the framework be streamlined? Consider merging or updating documents rather than creating new ones.
    - ✓ **Accessibility and Updates:** Are documents current and easily accessible? Have review processes and responsibilities been established?
  - **Key Reminder:** A documentation framework should add value to all parts of the organization—business units, IT, HR, and management. Regular engagement with key stakeholders ensures its relevance and effectiveness.

Why Outsource Cybersecurity?

- **Addressing the Talent Gap:**
  - *Difficulty in hiring and retaining skilled cybersecurity professionals.*
  - *Outsourcing transfers staffing challenges to a specialized provider.*
- **Outsourcing as a Trust Issue:**
  - *Outsourcing cybersecurity involves trust and isn't always a straightforward decision.*
- **Factors to Consider:**
  - *Cultural fit and the uniqueness of your organization.*
  - *Concerns about protecting valuable trade secrets.*
- **Benefits of Outsourcing:**
  - *Cost reduction and improved efficiency.*
  - *Allows your internal team to focus on core strengths.*

Benefits of Outsourcing Cybersecurity

- **Financial Benefits:**
  - *Cost-effective access to industry experts without full-time hires.*
  - *Lower capital expenditure—vendor provides tools and infrastructure.*
  - *Risk reduction through expert management and compliance support.*
- **Enhanced Focus and Efficiency:**
  - *Free up internal resources to focus on core business functions.*
  - *24/7 monitoring and automated updates ensure constant protection.*
  - *Improved decision-making by leveraging vendor expertise.*
- **Scalability and Future-Proofing:**
  - *Easily scale cybersecurity services as your business grows.*
  - *Access to advanced tools and technologies without heavy investment.*
  - *Protection against evolving cyber threats with cutting-edge solutions.*

Risks of Outsourcing Cybersecurity

Misalignment of Goals:

- **Lack of Control:**
  - *Outsourcing reduces direct control over cybersecurity processes and data management.*
  - *Decisions are made by the vendor, which might not align with internal practices.*
- **Reliability and Quality Concerns:**
  - *Varying standards and response times during critical incidents.*
  - *Providers may prioritize other clients, affecting turnaround time.*
- **Limited Organizational Knowledge:**
  - *Vendors may offer generic solutions that lack understanding of your specific needs.*

Hidden Costs:

- **Unexpected Expenses:**
  - *Costs for knowledge transfer, system integration, and operational expenses not included in initial estimates.*
  - *Additional charges for out-of-scope services; comprehensive contracts are essential.*
- **Security and Confidentiality Risks:**
  - *Risk of data breaches increases when sensitive information is shared externally.*
  - *Need for stringent vetting and adherence to data privacy standards.*
- **Communication Challenges:**
  - *Potential delays in updates and response times.*
  - *Importance of clear communication channels and robust SLAs.*

Key Differences in Managing Outsourced Cybersecurity

- **Control:**
  - *In-house management offers daily oversight and task control.*
  - *Outsourcing limits direct control; the vendor manages their own staff and operations.*
- **Measurement:**
  - *Internal teams are measured by performance indicators like attendance and deadlines.*
  - *Outsourced work is assessed by specific deliverables and results, such as timely security scans.*
- **Flexibility:**
  - *In-house staff can be reassigned quickly based on changing priorities.*
  - *Outsourced teams are dedicated to predefined tasks and roles, with less flexibility to shift focus.*

Overview of the Five Steps to Outsource Cybersecurity

- **Step 1: What to Outsource?**
  - *Identify the specific cybersecurity tasks or functions that can be effectively outsourced.*
  - Examples: Firewall management, network monitoring, incident response.
- **Step 2: Define Your Needs**
  - *Clearly document what you expect from the outsourcing arrangement, including desired outcomes and performance levels.*
  - Examples: Service Level Agreements (SLAs), expected response times, compliance requirements.
- **Step 3: Whom to Outsource To?**
  - *Evaluate potential vendors and conduct thorough due diligence to select the right partner.*
  - Considerations: Vendor experience, reputation, technical capabilities, industry fit.
- **Step 4: How to Formalize the Partnership?**
  - *Negotiate terms and formalize the contract to establish clear expectations and responsibilities.*
  - Key Points: Contract terms, SLAs, data protection clauses, penalties for non-compliance.
- **Step 5: How to Implement and Manage?**
  - *Transition the work to the vendor, manage the partnership, and review performance regularly to ensure success.*
  - Actions: Smooth handover, regular communication, continuous performance monitoring, feedback loops.

Case Study Background: Mid-Sized Retail Chain

- **Company Overview:**
  - *Mid-sized retail chain with 30 stores across several states.*
  - *Expanding online presence, increasing cybersecurity risks.*
- **Current IT and Security Situation:**
  - *Small IT team responsible for all digital operations.*
  - *Limited cybersecurity expertise in-house.*
- **Recent Security Incidents:**
  - *Attempted phishing scams.*
  - *Close call with a ransomware attack.*
- **Need for Outsourcing:**
  - *Lack of internal resources to effectively manage cybersecurity threats.*
  - *Decision to consider outsourcing to enhance security measures.*
- **Initial Outsourcing Plan:**
  - *Outsource firewall management and network monitoring.*
  - *Partner with a Managed Security Service Provider (MSSP).*
  - *Goal: Free up IT staff for strategic initiatives and strengthen cybersecurity.*

Step 1: Defining What to Outsource

- **IT Manager's Initial Task:**
  - *Evaluate which cybersecurity tasks could be outsourced safely.*
  - *Ensure no loss of control over critical operations.*
- **Quick Audit Findings:**
  - *Identified two non-core, essential tasks:*
    - **Firewall Management**
    - **Network Monitoring**
  - *Tasks are labor-intensive and outside the team's expertise.*
- **Primary Objective:**
  - *Improve cybersecurity without overburdening the IT team or increasing costs dramatically.*
- **Internal Concerns:**
  - **COO:** Worry about losing control and potential vulnerabilities.
  - **CFO:** Concerned about high costs of outsourcing.
  - **CEO:** Supports outsourcing to strengthen security capabilities.

Step 1: Defining What to Outsource
- How to Sort Work and Decide What to Outsource

- **Rule of Thumb for Outsourcing:**
    - *Keep core tasks in-house with employees.*
    - *Outsource non-core tasks.*
- **Three Categories of Tasks:**
    - **Core Tasks:**
        - *Require deep understanding of the business and strong internal relationships.*
        - *High-quality decisions needed that outsourcers can't provide.*
        - *Examples:*
            - Chairing the Information Security Steering Committee.
            - Supporting the renewal of cybersecurity insurance policies.
    - **Strategic Outsource Tasks:**
        - *Involve research or analysis that does not require deep internal knowledge.*
        - *Decision-making requires understanding of the business.*
        - *Examples:*
            - Assessing firewall effectiveness.
            - Performing digital forensics for incident management.
    - **Commodity Outsource Tasks:**
        - *Tasks done mostly by external teams under employee oversight.*
        - *Decisions are made based on pre-set rules and guidelines.*
        - *Examples:*
            - Resetting passwords.
            - 24/7 network security monitoring.

Step 2: Developing a Detailed Requirements Document

- **Purpose of the Requirements Document:**
    - *Outline what is expected from the Managed Security Service Provider (MSSP).*
- **Key Requirements Included:**
    - **24/7 Network Monitoring:**
        - *Continuous monitoring to quickly detect and respond to threats.*
    - **Proactive Firewall Management:**
        - *Manage firewall settings to block unauthorized access and handle new threats promptly.*
    - **Service Level Agreements (SLAs):**
        - *Clear response times for alerts and regular monthly reporting.*
- **Team Dynamics and Concerns:**
    - *IT staff worried about job security and losing control over key functions.*
    - *CFO concerned about keeping costs low.*
- **Finding a Compromise:**
    - *Agreed to start with a basic service package with the potential to expand later.*

Step 2: Developing a Detailed Requirements Document - Key Considerations for Outsourcing Requirements

- **Focus on Outcomes, Not Just Processes:**
    - *Think about the results you need, not just how the work gets done.*
    - *Examples of outcomes:*
        - **Response Times:** How quickly should threats be addressed? Is 15 minutes enough to verify an alert is genuine?
        - **Firewall Rule Implementation:** How soon should new rules be applied—within four hours of the initial request or after clarifications?
- **Consider Broader Impact:**
    - *Outsourcing can affect team morale and other business goals.*
    - *Think about outcomes for your staff and how to manage their transition or concerns.*

Step 2: Developing a Detailed Requirements Document -'How' the Work is Done Still Matters

- **Importance of How Work is Done:**
  - *Processes matter for cybersecurity, not just the end result.*
  - *Examples of risks:*
    - **Excessive Permissions:** Too much access can lead to data breaches.
    - **Improper Data Handling:** Storing sensitive info, like passwords, improperly can cause security incidents.
- **Managing Work Processes:**
  - *Let vendors create their own procedures, but review them thoroughly.*
  - *Conduct regular checks to ensure standards are maintained.*

Step 2: Developing a Detailed Requirements Document -Using SLAs to Manage Outsourced Work

- **What is a Service-Level Agreement (SLA)?**
  - *Contract that defines the services, performance levels, and accountability.*
  - *Key elements:*
    - **Service Descriptions:** What tasks will the vendor perform?
    - **Performance Levels:** How fast and reliably will they do it?
    - **Monitoring and Reporting:** How will performance be tracked?
- **Tips for Effective SLAs:**
  - *Review and update SLAs regularly as needs change.*
  - *Consider independent monitoring to verify vendor performance.*

Step 3: Vendor Selection and Due Diligence

- **Sending Out RFPs:**
  - *RFPs sent to multiple MSSPs based on finalized requirements.*
  - *Vendor responses varied in pricing and service quality.*
- **Choosing a Vendor:**
  - *One vendor stood out:*
    - **Experience with retail clients.**
    - **Balanced cost and quality.**
    - **Additional services:** Quarterly security assessments, employee training.
- **Due Diligence Concerns:**
  - *Potential red flag: Legal dispute with a former client.*
  - *COO's concerns heightened; vendor clarified misunderstanding and agreed to adjustments.*
- **Reaching an Agreement:**
  - *Tense negotiations over SLAs.*
  - *CEO involvement helped finalize the deal.*
  - *Contract includes a review after six months.*

Selecting a Vendor: Key Considerations

- **Your Responsibility:**
  - *Even with an MSSP, ultimate responsibility for security remains with you.*
  - *The relationship is not "set it and forget it"—ongoing management is essential.*
- **Potential Conflicts:**
  - **Your Goal:** Great outcomes for non-core tasks.
  - **MSSP's Goal:** Profitable growth.
  - *Risk: Cutting corners to increase profits, potentially compromising your security.*
- **Example: Intrusion Detection System (IDS) Monitoring:**
  - *MSSP might reduce the number of alarms investigated to cut costs.*
  - *Risk: Real threats could be missed if alarms are tuned too low.*
- **How to Mitigate Risks:**
  - *Understand how the MSSP performs the work.*
  - *If possible, verify their reports independently to ensure accuracy.*

Evaluating an MSSP: What to Look For

- **Service Features and Functions:**
  - *Does the MSSP's solution meet your needs?*
  - *Are their reporting and performance metrics clear and actionable?*
  - *Availability, scalability, and cost considerations*.
- **Business Structure:**
  - *Is the MSSP located in a stable country with reliable infrastructure?*
  - *Do their working hours align with your team's needs?*
  - *Is there a good cultural fit?*
  - Financial stability and customer satisfaction. *What do their other clients say about them?*
- **Security Practices:**
  - *Review independent evaluations like SOC2 reports*.
  - *Do they have a clear transition and implementation plan?*
  - *What's your exit strategy if things don't work out?*
  - *Check their security protocols and practices*.
  - *Consider visiting their site to verify physical security and operational practices*.

Step 4: Contract Negotiation and Finalization

- **Initial Contract Challenges:**
  - *Vendor’s contract heavily favored their own interests.*
  - *Limited liability for breaches, vague on incident response.*
- **Key SLAs That Led to Tension:**
  - **1. Rapid Incident Response Times:**
    - *Requirement:* Act on critical threats within 15 minutes of detection.
    - *Vendor's Pushback:* Preferred 1-hour response, citing resource challenges.
  - **2. Zero Tolerance for Critical Security Breaches:**
    - *Requirement:* Financial penalties for any breach of customer data.
    - *Vendor's Pushback:* Suggested tiered penalties based on breach severity
  - **3. Proactive Threat Intelligence and Reporting:**
    - *Requirement:* Weekly threat reports and monthly in-depth analysis sessions.
    - *Vendor's Pushback:* Proposed bi-weekly reports to manage workload.
- **Negotiation Outcomes:**
  - *Response time adjusted to 30 minutes with escalation path.*
  - *Tiered penalty system for data breaches based on severity.*
  - *Bi-weekly threat reports agreed upon, with immediate updates for significant threats.*

How to Contract with a Vendor: Key Considerations

- **Importance of a Solid Contract:**
  - *Always involve a lawyer or contracts manager.*
  - *Contracts need to be flexible to adapt to changing needs and technologies.*
- **Think in Terms of a Contract Lifecycle:**
  - **Beginning:** Start with clear terms and expectations.
  - **Middle:** Regular performance reviews and rights to audit.
  - **End:** Terms for renewal, revision, or termination.
- **Key Contract Terms to Include:**
  - *Termination for convenience.*
  - *Financial reimbursement for breaches (indemnification).*
  - *Regular performance reviews and right to audit.*

Tips for Contracting Successfully with an MSSP

- **Use a Responsibility Assignment Matrix:**
  - *Clarify roles and responsibilities (RACI model).*
  - *Helps manage risks and keep the vendor aligned with your procedures.*
- **Decide Whose Contract Template to Use:**
  - *Evaluate the vendor’s contract carefully if you don’t have your own.*
  - *Consider developing your own templates for different risk levels.*
- **Include Vendor in Risk Management:**
  - *Add the vendor to your third-party risk management program.*
  - *Require them to protect your sensitive data and include penalties for non-compliance.*
- **Retain Ownership of Cybersecurity Risks:**
  - *You can't outsource all risk—maintain a strong sense of ownership and oversight.*

Step 5a: Transition and Initial Management

- **Smooth Start but Initial Hiccups:**
  - *Vendor took over firewall management and set up monitoring systems.*
  - *Regular check-ins scheduled by IT manager to monitor progress.*
- **Challenges Faced:**
  - *False positives in monitoring caused unnecessary alerts and confusion.*
  - *Uncommunicated firewall changes led to minor network disruptions.*
- **Addressing the Issues:**
  - *Store managers voiced concerns; IT team felt pressure from disruptions.*
  - *Meetings with vendor led to adjustments in monitoring and improved communication.*
- **Early Benefits Seen:**
  - *Proactive monitoring prevented a potential ransomware attack.*
  - *IT team could focus more on strategic improvements.*

Step 5b: Ongoing Management, Review, and Contract Renewal

- **Ongoing Management and Monitoring:**
  - *Regular review meetings to assess performance and compliance with SLAs.*
  - *Improvements in feedback from employees and store managers.*
- **Performance Review and Positive Outcomes:**
  - *Six-month performance review showed most SLAs were met or exceeded.*
  - *Cybersecurity posture and cost-effectiveness improved significantly.*
- **Contract Renewal and Future Plans:**
  - *Contract renewed with adjustments to SLAs and improved communication.*
  - *Exploration of new collaboration opportunities for advanced threat detection.*

Transition to a New Vendor: Key Steps for a Smooth Start

- **Prepare for Transition:**
  - *Review the vendor's standard transition plan carefully.*
  - *Ensure both sides assign experienced people to manage the transition.*
- **Focus on People and Communication:**
  - *Support employees through changes; manage concerns and expectations.*
  - *Use multiple communication channels to keep everyone informed and engaged.*
- **Schedule Early Performance Reviews:**
  - *Set up regular check-ins from the start to quickly address any issues.*
  - *Test the vendor's services with unexpected requests to ensure reliability.*

Managing the Vendor Relationship: Ongoing Oversight and Communication

- **Establish Strong Relationship Management:**
  - *Create a clear escalation process for any conflicts.*
  - *Maintain open lines of communication with regular meetings and updates.*
- **Monitor Performance and Celebrate Wins:**
  - *Use SLAs to track performance and hold the vendor accountable.*
  - *Acknowledge good performance and identify areas for improvement.*
- **Address Issues Quickly:**
  - *Be proactive in addressing any problems to maintain a strong partnership.*
  - *Encourage the vendor to improve and grow, rather than focusing only on mistakes.*

Contract Renewal and Planning for the Futur

- **Prepare for Renewal Early:**
  - *Decide if you want to continue with the vendor at least 60 days before contract end.*
  - *Consider any necessary changes to service levels or terms.*
- **Options During Renewal:**
  - *Renew with updated terms or extend the current contract with no changes.*
  - *Decide if it's time to move on—evaluate performance and future needs.*
- **Know When to Walk Away:**
  - *Identify signs it's time to end the contract (poor performance, unresolved issues).*
  - *Be aware of any renewal clauses, like evergreen clauses, that could complicate ending the contract.*