Information Security Governance

The First Unit: Course Introduction

At the end of the unit, the trainee should be able to:

- The trainee learns about information security governance.

- Explains the importance of information security governance.

- Explores the role of governance and its impact on data quality.

- Demonstrates the role of governance in making strategic decisions based on a solid foundation**.**

Lesson1 : Course Introduction

This course discusses how information security governance helps organizations to move from a reactive approach to cybersecurity to a proactive approach. This course discusses how the information security governance will Categorize and mitigate risks and threats, prepare an organization for identifying, remediating, and recovering from a cyberattack or breach, provide a method for executive leadership to understand their risk posture and maturity levels, and outline a risk-based approach to the people, systems, and technology that are used every day.

The overarching concepts and values that govern how you operate your organization are known as governance. That has to do with your company's vision, objectives, and ideals. Your company's corporate governance is its heart; it keeps everyone on task and aids in your success. Your company's information governance keeps its data on point and strengthens the integrity and accuracy of operations What is information security governance?

Information is more than a collection of details, names, numbers and records… Information is a critical asset of most organizations. Significant impact rides on the security of this information, protecting it from breaches or damage, and directly affecting the reputation and continuity of the organization.

Utmost care for an organization's information is absolutely critical. From storage and transit to accessibility and retrieval, information security must be carefully monitored and managed throughout its lifecycle.

Information governance are the policies, processes and controls created specifically to manage and secure information. These will cover information security, integrity, accessibility, authorization, deletion and overall management.

Information Security Triad

The famous triad of information security is made up of:

- Confidentiality: Sensitive or private information must remain that way. This means processes must protect the accessibility or the information, control who is authorized to interact with it, and protect it from unauthorized breaches.
- Integrity: Information is valuable as long as it is accurate and true. The risk of information being compromised or changed heightens when it is accessed by users with the ability to alter it, or when it is in transit.
- Availability: Information needs to be accessible to its authorized users in a timely manner. For systems categorized as critical, extreme availability requirements are typically present (power generation, medical equipment, safety systems). These systems must be resistant to cyberattacks and include safeguards against incidents that could limit system availability, such as hardware failures, power outages, and others.

Information security governance and risk management go hand in hand. In order to secure information, a comprehensive risk assessment must be undertaken to identify and prioritize the risks facing information security. Gaining insights into controls that may be missing or necessary remediation steps also make a risk assessment an important endeavor.

Benefits of Information Security Governance

If your organization offers poor management of data security (another term for information security), you'll be left with issues of accessibility, ease of use, timeliness and security. Proper governance can remedy these problems and ensure your organizational information is in tip-top shape.

- Keeping compliant with standards, regulation and laws – A robust information security program will ensure a company is ready to meet compliance. Not only does better compliance increase security, but increased security prepares for better levels of compliance. Compliance for information security governance may mean complying with any of the information security governance frameworks or standards
- Single Source of Truth (SSOT) – Proper information governance will reduce the chance of the same information being stored multiple times causing confusion through conflicting versions. Effective governance will establish a single source of truth (SSOT) and ensure smooth reference to and use of information.
- Data as valuable business information – The majority of organizations have a ton of data, but it can be difficult to deliver it to the right people, at the right time. Without the

correct organization of information, companies will gloss over the important insights that could be gleaned to transform that data into business information. Data analysis is built upon strong information governance.

-

- Reduce risks and costs of discovery and litigation – Inaccurate or damaging information can lead to lawsuits, compliance penalties and reputational damage.
- Improved decision making – Being able to clearly see all your information means being able to look at the details against the big picture and make informed business decisions.

Good information security will involve a holistic approach taking into account systems, networks, people and more. Undertaking a comprehensive risk assessment will act as the basis for a strong foundational evaluation of your security posture and what could be affecting your information systems. Ensure findings are incorporated into building robust and manageable policies and that roles and responsibilities of infosec are clearly defined. Check out the Central eyes platform today to begin building a safe environment for your information security.

What Is Information Security Governance?

This governance describes the way a company manages its information security needs. Ideally, it protects the integrity, confidentiality, and availability of information. IT managers begin by identifying all possible risks. They then design proactive policies and frameworks to tackle these issues at the source.

Information security governance transcends systems and databases. A more holistic approach also ensures employees understand the importance of confidentiality and their role in maintaining it.

What Are the Main Elements of Information Security Governance?

Building a governance system requires an in-depth analysis of an organization's information, storage needs, and security status. These are the five main areas managers need to cover when evaluating their organizations' information security governance needs.

1. Information Security Strategy

Managers must create a well-defined plan that aligns well with organizational goals. This strategy should outline the overall approach for managing and protecting information assets.

2. Policies and Procedures

Employees need comprehensive and up-to-date policies to help organizations safeguard data. For example, the effectiveness of multi-factor authentication has **dropped from 99%** to as little as 30%. Companies must update policies to match these and other changes.

3. Risk Management

You can't manage risk without first identifying the threats present. IT managers should follow a basic process to address this:

- Identify the potential risks.
- Assess the organization's exposure to these risks.
- Implement solutions that mitigate these risks.

- Monitor and review how well these solutions protect the organization.

4. Compliance and Audit

Failure to comply is expensive. In 2022, Morgan Stanley Smith Barney paid **a $35 million settlement** to resolve SEC charges of failing to protect personal information. Effective managers conduct regular audits and assessments to ensure compliance.

5. Incident Response and Management

Organizations should have a well-defined incident response plan to detect and address threats. Start by establishing a dedicated, multi-disciplinary incident response team. It should include lawyers, communication specialists, and compliance officers. This team should develop a response strategy to deploy instantly when needed.

What Is Information Security Governance?

This governance describes the way a company manages its information security needs. Ideally, it protects the integrity, confidentiality, and availability of information. IT managers begin by identifying all possible risks. They then design proactive policies and frameworks to tackle these issues at the source.

Information security governance transcends systems and databases. A more holistic approach also ensures employees understand the importance of confidentiality and their role in maintaining it.

hat Are the 4 Steps of Information Security Governance?

Information security governance consists of four main steps to strengthen an organization's defense. Organizations may change and expand on these as they see fit, but they should know the core four before making adjustments:

1. **Create a strategy.** Identify the ways governance will affect your organization and define the main goals and objectives of information security governance. This should include a clear understanding of an organization's risk tolerance, resources, and legal requirements.
2. **Build the framework.** IT governance requires more than just ideas on paper or ambitious policies. Professionals must also build a framework that will meet those needs. IT admins can simplify this by choosing a premade option and carefully configuring it or creating a customized solution from scratch.

3. **Test and implement the system.** Development teams must also test the system to ensure it works correctly and meets all requirements. Once tested, the IT team can deploy the governance system across an organization's network and devices.
4. **Monitor and adjust.** The final step is to monitor information security governance performance regularly and make necessary adjustments or improvements. This will help organizations maintain a secure and compliant environment.

What Are the Main Challenges and Threats for Information Security Governance?

An in-depth analysis is the best way to identify threats and challenges unique to your organization. Here are some of the most common ones you might uncover.

Human Factors

One Forbes article suggests that **employees cause 85%** of security breaches. Ensuring employees know their responsibilities and follow the organization's policies and procedures is a significant challenge. Another human factor is the difficulty of securing buy-in at all levels. Resistance from staff can seriously impede IT governance efforts.

Lack of Organizational Resources

A lack of capital and other resources can impede an organization's ability to manage its governance system effectively. Organizations should allocate sufficient funds for this task. Too often, companies treat information security governance as an afterthought, increasing the potential risk.

Insufficient Technology Capabilities

Organizations need to prioritize the latest technologies, such as cloud computing or AI-based solutions, and ensure that their existing systems are up to date. Inadequate technological infrastructure can expose organizations to cyber threats such as malware attacks, phishing scams, and data breaches.

What Are the Benefits of Information Security Governance?

The advantages of a governance system vary based on your industry, the design of your system, and how well the IT team implemented it. Even so, here are some general benefits you can expect.

Improved Data Security

Organizations can better protect their sensitive information from unauthorized access, disclosure, or alteration by implementing well-defined policies. This includes using MFA and tiered access based on clearance levels within the organization.

Reduced Risk of Security Incidents

A robust information security governance framework helps to minimize the likelihood of security incidents, such as data breaches and cyberattacks. It's not enough to just respond to incidents; IT admins must seek out proactive solutions.

Compliance with Regulations

Organizations must comply with various regulatory requirements and industry standards, such as the General Data Protection Regulation, the Health Insurance Portability and Accountability Act, and the Payment Card Industry Data Security Standard. Information security governance

ensures compliance by establishing policies and processes that align with all applicable standards. You could also expand compliance to include the ability to comply with **e-Discovery requests**.

Improved Business Continuity

Can your organization continue to operate during natural disasters, cyberattacks, and other unexpected events? Create a plan to protect critical information assets and maintain essential functions during a crisis. This includes having backup and recovery procedures for data and strategies for managing incidents and restoring operations quickly.

Disaster Recovery

Fujifilm provides an excellent example of how information security governance can protect an organization. When hackers gained unauthorized access to the company, it reportedly refused to pay the ransom. Instead, it **restored its system from backups** and returned to normal operations. Could your team do the same? An effective recovery plan outlines the steps an organization will take to bounce back from a significant disaster that results in the loss of critical systems and data.

How Can the Cloud Improve Your Plan?

Cloud migration can significantly streamline information security governance. For starters, some of the cybersecurity responsibilities get outsourced to the owner of the servers, such as Microsoft or Amazon. Using the cloud streamlines your IT governance with these features:

1. **Shared Responsibility Model:** The cloud service provider is responsible for securing the underlying infrastructure and platform, while the organization is responsible for securing its applications and data. This division of responsibilities make many processes more efficient and manageable.
2. **Centralized Security Management:** CSM makes it easy for organizations to maintain and monitor their security posture across all applications and services in the cloud. This centralization simplifies governance by consolidating security controls.
3. **Advanced Security Technologies:** These higher-end capabilities can help organizations detect and respond to cyber threats more effectively. Automation can also reduce the risk of threats going undetected.

4. **Compliance Simplification:** CSPs often have pre-built compliance frameworks and tools that align with regulatory requirements and industry standards, such as GDPR, HIPAA, and PCI DSS. These providers may also offer e-Discovery solutions, such as Microsoft's Purdue.
5. **Scalability and Flexibility:** Cloud-based solutions offer virtually limitless scalability and flexibility, allowing organizations to adapt their security infrastructure as their needs evolve. This is another way companies can adjust to unexpected events, such as
6. plunging customer demand after an economic crash. Companies that cannot scale down will continue to pay high prices for services they cannot use.
7. **Enhanced Disaster Recovery:** Cloud-based solutions provide organizations with access to sophisticated disaster recovery options. Automated backups, data redundancy, and failover systems are just some examples. These features minimize downtime and boost business continuity.

How Can Cloud Migration Specialists Help?

Our Coefficient migration specialists streamline the process of upgrading to the cloud so that you can get these benefits and more for your organization. Now you know the answer to what is information security governance and you understand how the cloud helps. Are you ready to see that solution in action?

Lesson2 : Information Security Concepts

What is Information Security (InfoSec)?

Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information. InfoSec is a growing and evolving field that covers a wide range of fields, from network and infrastructure security to testing and auditing.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

The consequences of security incidents include theft of private information, data tampering, and data deletion. Attacks can disrupt work processes and damage a company’s reputation, and also have a tangible cost.

Organizations must allocate funds for security and ensure that they are ready to detect, respond to, and proactively prevent, attacks such as phishing, malware, viruses, malicious insiders, and ransomware.

Whitepaper: Meeting Data Security Challenges in the Age of Digital Transformation.

What are the 3 Principles of Information Security?

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

Confidentiality

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time).

The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

Information Security vs Cybersecurity

Information security differs from cybersecurity in both scope and purpose. The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security. Information security is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security. It is also closely related to information assurance, which protects information from threats such as natural disasters and server failures.

Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them. Another related category is data security, which focuses on protecting an organization's data from accidental or malicious exposure to unauthorized parties.

Information Security Policy

An Information Security Policy (ISP) is a set of rules that guide individuals when using IT assets. Companies can create information security policies to ensure that employees and other users follow security protocols and procedures. Security policies are intended to ensure that only authorized users can access sensitive systems and information.

Creating an effective security policy and taking steps to ensure compliance is an important step towards preventing and mitigating security threats. To make your policy truly effective, update it

frequently based on company changes, new threats, conclusions drawn from previous breaches, and changes to security systems and tools.

Make your information security strategy practical and reasonable. To meet the needs and urgency of different departments within the organization, it is necessary to deploy a system of exceptions, with an approval process, enabling departments or individuals to deviate from the rules in specific circumstances.

Top Information Security Threats

There are hundreds of categories of information security threats and millions of known threat vectors. Below we cover some of the key threats that are a priority for security teams at modern enterprises.

Unsecure or Poorly Secured Systems

The speed and technological development often lead to compromises in security measures. In other cases, systems are developed without security in mind, and remain in operation at an organization as legacy systems. Organizations must identify these poorly secured systems, and mitigate the threat by securing or patching them, decommissioning them, or isolating them.

Social Media Attacks

Many people have social media accounts, where they often unintentionally share a lot of information about themselves. Attackers can launch attacks directly via social media, for example by spreading malware via social media messages, or indirectly, by using information obtained from these sites to analyze user and organizational vulnerabilities, and use them to design an attack.

Social Engineering

Social engineering involves attackers sending emails and messages that trick users into performing actions that may compromise their security or divulge private information. Attackers manipulate users using psychological triggers like curiosity, urgency or fear.

Because the source of a social engineering message appears to be trusted, people are more likely to comply, for example by clicking a link that installs malware on their device, or by providing personal information, credentials, or financial details.

Organizations can mitigate social engineering by making users aware of its dangers and training them to identify and avoid suspected social engineering messages. In addition, technological systems can be used to block social engineering at its source, or prevent users from performing dangerous actions such as clicking on unknown links or downloading unknown attachments.

Malware on Endpoints

Organizational users work with a large variety of endpoint devices, including desktop computers, laptops, tablets, and mobile phones, many of which are privately owned and not under the organization's control, and all of which connect regularly to the Internet.

A primary threat on all these endpoints is malware, which can be transmitted by a variety of means, can result in compromise of the endpoint itself, and can also lead to privilege escalation to other organizational systems.

Traditional antivirus software is insufficient to block all modern forms of malware, and more advanced approaches are developing to securing endpoints, such as endpoint detection and response (EDR).

Lack of Encryption

Encryption processes encode data so that it can only be decoded by users with secret keys. It is very effective in preventing data loss or corruption in case of equipment loss or theft, or in case organizational systems are compromised by attackers.

Unfortunately, this measure is often overlooked due to its complexity and lack of legal obligations associated with proper implementation. Organizations are increasingly adopting encryption, by purchasing storage devices or using cloud services that support encryption, or using dedicated security tools.

Security Misconfiguration

Modern organizations use a huge number of technological platforms and tools, in particular web applications, databases, and Software as a Service (SaaS) applications, or Infrastructure as a Service (IaaS) from providers like Amazon Web Services.

Enterprise grade platforms and cloud services have security features, but these must be configured by the organization. Security misconfiguration due to negligence or human error can result in a security breach. Another problem is "configuration drift", where correct security configuration can quickly become out of date and make a system vulnerable, unbeknownst to IT or security staff.

Organizations can mitigate security misconfiguration using technological platforms that continuously monitor systems, identify configuration gaps, and alert or even automatically remediate configuration issues that make systems vulnerable.

Active vs Passive Attacks

Information security is intended to protect organizations against malicious attacks. There are two primary types of attacks: active and passive. Active attacks are considered more difficult to prevent, and the focus is on detecting, mitigating and recovering from them. Passive attacks are easier to prevent with strong security measures.

Active Attack

An active attack involves intercepting a communication or message and altering it for malicious effect. There are three common variants of an active attacks:

- **Interruption**—the attacker interrupts the original communication and creates new, malicious messages, pretending to be one of the communicating parties.
- **Modification**—the attacker uses existing communications, and either replays them to fool one of the communicating parties, or modifies them to gain an advantage.
- **Fabrication**—creates fake, or synthetic, communications, typically with the aim of achieving denial of service (DoS). This prevents users from accessing systems or

Active Attacks	Passive Attacks
Modify messages, communications or data	Do not make any change to data or systems
Poses a threat to the availability and integrity of sensitive data	Poses a threat to the confidentiality of sensitive data.
May result in damage to organizational systems.	Does not directly cause damage to organizational systems.
Victims typically know about the attack	Victims typically do not know about the attack.
Main security focus is on detection and mitigation.	Main security focus is on prevention.

- performing normal operations.

Passive Attack

In a passive attack, an attacker monitors, monitors a system and illicitly copies information without altering it. They then use this information to disrupt networks or compromise target systems.

The attackers do not make any change to the communication or the target systems. This makes it more difficult to detect. However, encryption can help prevent passive attacks because it obfuscates the data, making it more difficult for attackers to make use of it.

Information Security and Data Protection Laws

Information security is in constant interaction with the laws and regulations of the places where an organization does business. Data protection regulations around the world focus on enhancing the privacy of personal data, and place restrictions on the way organizations can collect, store, and make use of customer data.

Data privacy focuses on personally identifiable information (PII), and is primarily concerned with how the data is stored and used. PII includes any data that can be linked directly to the user, such as name, ID number, date of birth, physical address, or phone number. It may also include artifacts like social media posts, profile pictures and IP addresses.

Data Protection Laws in the European Union (EU): the GDPR

The most known privacy law in the EU is the General Data Protection Regulation (GDPR). This regulation covers the collection, use, storage, security and transmission of data related to EU residents.

The GDPR applies to any organization doing business with EU citizens, regardless of whether the company itself is based inside or outside the European Union. Violation of the guidelines may result in fines of up to 4% of global sales or 20 million Euro.

The main goals of the GDPR are:

- Setting the privacy of personal data as a basic human right
- Implementing privacy criteria requirements
- Standardization of how privacy rules are applied

GDPR includes protection of the following data types:

- Personal information such as name, ID number, date of birth, or address
- Web data such as IP address, cookies, location, etc.
- Health information including diagnosis and prognosis
- Biometric data including voice data, DNA, and fingerprints
- Private communications

- Photos and videos
- Cultural, social or economic data

Data Protection Laws in the USA

Despite the introduction of some regulations, there are currently no federal laws governing data privacy in general in the United States. However, some regulations protect certain types or use of data. These include:

- **Federal Trade Commission Act**—prohibits organizations from deceiving consumers with regard to privacy policies, failure to adequately protect customer privacy, and misleading advertising.
- **Children's Online Privacy Protection Act**—regulates the collection of data related to minors.
- **Health Insurance Portability and Accounting Act (HIPAA)**—regulates the storage, privacy and use of health information.
- **Gramm Leach Bliley Act (GLBA)**—regulates personal information collected and stored by financial institutions and banks.
- **Fair Credit Reporting Act**—regulates the collection, use, and accessibility of credit records and information.

Additionally, the Federal Trade Commission (FTC) is responsible for protecting users from fraudulent or unfair transactions such as data security and privacy. The FTC can enact regulations, enforce laws, punish violations, and investigate organizational fraud or suspected violations.

In addition to federal guidelines, 25 US states have enacted various laws to regulate data. The most famous example is the California Consumer Privacy Act (CCPA). The law went into effect in January 2020 and provides protection to California residents, including the right to access private information, request deletion of private information, and opt out of data collection or resale.

There also other regional regulations such as:

- Australian Prudential Regulatory Authority (APRA) CPS 234
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- Singapore Personal Data Protection Act (PDPA)

Information Security with Imperva

Imperva helps organizations of all sizes implement information security programs and protect sensitive data and assets.

Imperva Application Security

Imperva provides multi-layered protection to make sure websites and applications are available, easily accessible and safe. The Imperva application security solution includes:

- **DDoS Protection**—maintain uptime in all situations. Prevent any type of DDoS attack, of any size, from preventing access to your website and network infrastructure.
- **CDN**—enhance website performance and reduce bandwidth costs with a CDN designed for developers. Cache static resources at the edge while accelerating APIs and dynamic websites.
- **WAF**—cloud-based solution permits legitimate traffic and prevents bad traffic, safeguarding applications at the edge. Gateway WAF keeps applications and APIs inside your network safe.
- **Bot management**—analyzes your boat traffic to pinpoint anomalies, identifies bad bot behavior and validates it via challenge mechanisms that do not impact user traffic.
- **API security**—protects APIs by ensuring only desired traffic can access your API endpoint, as well as detecting and blocking exploits of vulnerabilities.
- **Account takeover protection**—uses an intent-based detection process to identify and defends against attempts to take over users' accounts for malicious purposes.
- **RASP**—keep your applications safe from within against known and zero-day attacks. Fast and accurate protection with no signature or learning mode.
- **Attack analytics**—mitigate and respond to real security threats efficiently and accurately with actionable intelligence across all your layers of defense.

Imperva Data Protection

Imperva's data security solution protects your data wherever it lives—on premises, in the cloud and in hybrid environments. It also provides security and IT teams with full visibility into how the data is being accessed, used, and moved around the organization.

Our comprehensive approach relies on multiple layers of protection, including:

- **Database firewall**—blocks SQL injection and other threats, while evaluating for known vulnerabilities.
- **User rights management**—monitors data access and activities of privileged users to identify excessive, inappropriate, and unused privileges.
- **Data masking and encryption**—obfuscates sensitive data so it would be useless to the bad actor, even if somehow extracted.
- **Data loss prevention (DLP)**—inspects data in motion, at rest on servers, in cloud storage, or on endpoint devices.

- **User behavior analytics**—establishes baselines of data access behavior, uses machine learning to detect and alert on abnormal and potentially risky activity.
- **Data discovery and classification**—reveals the location, volume, and context of data on premises and in the cloud.
- **Database activity monitoring**—monitors relational databases, data warehouses, big data and mainframes to generate real-time alerts on policy violations.
- **Alert prioritization**—Imperva uses AI and machine learning technology to look across
- the stream of security events and prioritize the ones that matter most.

Lesson3 : Information Security Governance Overview

As information and information technology are of increasing strategic importance, effective management of IT and information assets becomes a critical strategic concern. IT Governance (ITG) deals with the management of an organization's use of IT. According to the IT Governance Institute (2007), it is "an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives".

Information security has traditionally been defined as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (Whitman and Mattord, 2008). Traditional viewpoints on information security included access to information systems, securing communications, security management and development of secure information systems (Siponen and Oinas-Kukkonen, 2007). However, while security considerations are an essential part of IT governance, information security governance goes beyond the IT realm. Information security is increasingly a business issue (von Solms and von Solms, 2005) that calls for governance of its own (von Solms, 2006).

In the networked, always-on business environment of today, it may seem futile to try and keep systems patched and protected for viruses, intrusions and other attacks. IT-reliant wall-to-wall defense against all conceivable contingencies renders inadequate in the face of ever-new methods that bypass even the sturdiest firewalls. Thus, information security needs to be adaptive and guided by business objectives and goals as well as to be increasingly tied to the information and its life-cycle. The key elements to be protected include not just information itself but also organizational assets such as trust, reputation, brand, stakeholder value and customer loyalty for which security breaches could have negative effects.

Implementing and maintaining adequate security measures in all these facets should be seen as a nonnegotiable cost of doing business.

Effective information security governance shall integrate legal, managerial, operational, and technical considerations (Allen and Westby, 2007). It shall specify roles that have the requisite authority, accountability, and resources to implement and enforce policies, standards, awareness programs, security strategies, and other organizational procedures. Thereby, it establishes an appropriate framework for decision making that relies on well-informed decision-making and ensures that decisions are enacted, implemented and monitored consistently.

A number of standards and best practice frameworks for Information Security Management (ISM) have been developed. These frameworks help organizations assess and control their security risks and comply with given regulations and governance requirements.

One such framework is the international information security management standard ISO/IEC 27002:2005,

which is published by the International Organization for Standardization (ISO) and International

Electrotechnical Commission (IEC) and originally derived from the UK government's BS 7799. The standard defines 133 security controls strategies under 11 major headings. ISO/IEC 27002:2005

pronounces the importance of risk management and advises not to implement every stated guideline but only those that are relevant. The guiding principles rely on either legal requirements or generally accepted best practices and are the initial points for implementing information security.

Another established and comprehensive standard on information security is the business-oriented Standard of Good Practice for Information Security (SOGP) by Information Security Forum (ISF). The standard consists of six different aspects, each of which is broken down into summary areas and detailed sections. The full standard covers 36 summary areas and 166 sections.

We concur with Allen and Westby (2007) that governance and management of security are most effective when they are systemic and when the responsibility for enterprise security is assigned to roles that have the requisite authority, accountability, and resources to implement and enforce it. We also subscribe to Hoover Vorst's (2009) notion that change must be addressed from the constructional perspective that entails coherent and consistent design principles and holistically integrates various business and organizational aspects.

While the existing ISM frameworks identify different information security areas and define detailed security controls, they provide limited insight into how information security is systemically built into the organizational design. The frameworks typically lack the notion of organizational levels and horizontal dimensions pertinent to roles, accountabilities and policies, as well as the "organizational connection points horizontally and vertically" (Allen and Westby, 2007), needed for effective enterprise security. In essence, the frameworks are representative of management models rather than governance models.

Von Solms and von Solms (2006; 2009) provide a welcome exception to this observation. Their model for information security governance identifies three levels of management – strategic, tactical and operational – and three distinct "actions" across these levels – direct, execute and control. The strategic level "directives" are expanded into sets of information security policies, company standards and procedures at the tactical level and further to administrative guidelines and administrative procedures at the operational level. Execution then takes place at the lowest level, producing measurement data that is extracted at the operational level, compiled and integrated at the tactical level and finally aggregated and abstracted to perform measurement against the requirements of the directives at the strategic level.

Because of this Direct-Control Cycle, the model represents a governance model, not merely a

management model (von Solms and von Solms, 2006).

In a similar vein, our approach to governance model design is systemic and structural. Not unlike the von Solms brothers, we distinguish a number of decision-making levels, in our case five, but instead of processes like direct, execute and control flowing across these levels, we identify horizontal dimensions common to the levels. As the horizontal dimensions, we discern design, development, operations and monitoring. Somewhat different from the common convention of some typologies, including the one by von Solms and von Solms, and with respect to the governance principle of "separation of duties", we do not view "control" as a distinct dimension or action, but as being spread out over operations (prevention) and monitoring (detection).

CHANGING LANDSCAPE OF INFORMATION SECURITY

Issues, Controversies, Problems

The executive management's commitment to information security is a key aspect of effectively managing the security exposure and related risks to an organization's digital assets. Executive management should view information security as an essential component of business, equivalent to any other core business asset or function. Building a proper governance structure requires an understanding of the full range of actions and operations involved in creating an enterprise level program, framework and culture for information security. To achieve a sustainable capability, security must be addressed at the governance level by executive management and embraced at all levels of the organization. Contemporary information security is not to be relegated to a technical issue within the IT department (Allen, 2005).

The need for executive level governance of information security flows both a) from legal compliance requirements associated with laws, regulations, treaties and other duties in protecting data and b) from corporate governance practices such as fiduciary duty of care owed by executive management and directors to shareholders in case of business enterprise. Legal compliance requirements originate from domestic and increasingly from international law. Numerous laws require protections for various types of data such as financial, personal and medical information. Furthermore, tightening corporate governance

practices impose new requirements for data protection, traceability and transparency, record management and other internal controls.

Addressing security at the enterprise level is often hard to justify. Security measures are typically viewed as disaster prevention and the exact value of such investments is hard to measure. Without adequate executive sponsorship and understanding of the value of information security to business, organizations tend to approach security by fixing the problems as they appear and trying to cope with emerging external threats.

Legislation and regulation increasingly impose administrative, civil, and criminal penalties for security breaches that were made possible due to the lack of supervision or control by someone in a senior managerial or executive position. Examples of such legislation include U.S. Gramm-Leach-Bliley Act (1999), U.S. Health Insurance Portability and Accountability Act (1996), U.S. Sarbanes-Oxley Act (2002), European Union (EU) Data Protection Directives, etc.

Regulatory requirements for data protection include not only organizations' own information but increasingly also data collected on or stored by customers or consumers – users of the digital services that the organization provides – in different contexts. Such laws include, for example, compliance requirement on organizations to notify individuals in the event of a breach to their personal information such as address, credit card number or email account. Therefore, the information governance practices in today's organizations should not be limited to mere data protection but should also include measures such as active prevention, threat analysis, breach detection, and in the event of breach, damage control, recovery and other reactionary measures.

The current focus on sustainability and corporate social responsibility are also pushing for better

information security governance. From the executive management viewpoint, governance should not be seen only as a matter of regulatory compliance and accountability but also as a strategic means to reduce risks, create value and improve the long-term performance of the organization.

Also, several converging IT trends will have a significant impact on existing information governance practices. In the following, we will discuss a few of these trends: cloud computing, proliferation of digital information and consumerization of IT.

processing to software, e.g. instant, commitment-free and on-demand handling of e-mail by

external parties. Due to its virtualized, distributed and global nature, cloud computing will place new challenges to effective information security and risk management, as the control of information will be increasingly delegated to third parties. From information security management viewpoint, cloud computing initiatives should have a rigorous set of criteria designed to assess and manage the risk of adopting cloud services, to compare and measure suitable providers, and to monitor their operation and performance. Information security governance models should include a clear division of liabilities and responsibilities between customer and providers in the appropriate areas of security, access, audit control, recovery and incident management.

The proliferation of digital information will also pose new demands for information security practice. The amount of digital information handled and stored by organizations has been

increasing continuously for years and, according to a recent study by IDC (Gantz and Reinsel, 2010), it will continue to increase by several ten folds in the coming decade. IDC predicts that the average growth rate of information will exceed 50 % annually and the amount of sensitive information, both protected and unprotected, is growing even faster. As the amount of information, in general, and sensitive information, in particular, is growing, the importance of governance and management practices becomes ever more pronounced.

In the consumerization of IT, widely available consumer IT technologies, solutions and devices are making their way into workplace. Examples of these new technologies and solutions include smart phones, tablet PCs, social networking, blogs, wikis, etc. These developments have created many more avenues of vulnerability for organizations and have also changed the mindset of employees and technology users in terms of risk. IT departments in organizations no longer have full control over the devices and solutions used in the workplace; downright banning of their use is not an option either.

Employees accustomed to using new services will either break the rules or change their job.

Organizations need to recognize this trend and accommodate their information security management accordingly. Without proper oversight and governance, the proliferation of consumer technologies

presents a serious risk of data leakage, as information increasingly flows through environments that, by default, are more open than the ones organizations have become accustomed to.

In the increasingly networked economy, organizations constitute extended enterprises where even core functions are divided between partners, suppliers and service providers. The continuing trend towards outsourcing and offshoring also increases potential risks and security exposures. Albeit organizations internal security policies and controls are maintained and enforced, these external relationships may pose a significant risk, unless governed and managed properly. As globalization continues, legal and
cultural

differences across the globe must be understood and taken into account in a proper fashion.

.....

Unit Two : Major Information Security Governance Frameworks

At the end of the unit, the trainee will be able to:

- Feels the importance of information security governance in increasing operational efficiency

- Mention the role of information security governance in enhancing security and privacy.

- Demonstrates the extent to which information security governance is useful in improving decision-making.

- Shows the extent of the impact of governance on enhancing competitiveness**.**

Lesson1 : International Frameworks (ISO 27K, COBIT, NIST, GDPR)

1. Introduction

1.1 Introduction to the Framework

The current digital society has high expectations of flawless customer experience and continuous availability of services. The advancement of information technology ("IT") has brought rapid changes to the way businesses and operations are being conducted in the financial sector. Although IT plays an essential role combined with today's environment, it also exposes financial institutions to dynamically evolving IT risks.

In this regard, Saudi Central Bank ("SAMA") has established an Information Technology Governance Framework ("the Framework") to enable organizations regulated by SAMA ("the Member Organizations") to effectively identify and address risks related to IT. The objective of the Framework is as follows:

1. To create a common approach for addressing IT risks within the Member Organizations.
2. To achieve an appropriate maturity level of IT controls within the Member Organizations.
3. To ensure IT risks are properly managed throughout the Member Organizations.

The framework will be used to periodically assess the maturity level and evaluate the effectiveness of the IT controls at Member Organizations. The framework is based on the SAMA requirements and industry IT standards.

1.2 Definition of Information Technology Governance

An Information Technology (IT) governance ensures the effective and efficient use of IT to enable Member Organizations to achieve its goals and objectives. It enables Member Organizations formulating optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

1.3 Scope

The framework defines principles and objectives for initiating, implementing, maintaining, monitoring and improving IT governance controls within Member Organizations regulated by SAMA. The framework offers IT governance controls requirements which are applicable to the information assets of the Member Organizations. Additionally, the framework provides direction

for IT Governance requirements for Member Organizations and its subsidiaries, staff, third parties and customers. The framework should be implemented in conjunction with SAMA's

Cyber Security and Business Continuity framework respectively (figure 1). For specific Cyber Security and Business Continuity related requirements please refer to SAMA's Cyber Security Framework and Business Continuity Management Framework.
The Framework has an interrelationship with other corporate policies for related areas, such as change management and staff training. This framework does not address the non-IT requirements for those areas.
1.4 Applicability
The framework is applicable to Member Organizations regulated by SAMA.
1.5 Responsibilities
The framework is mandated by SAMA and will be circulated to Member Organizations for implementation. SAMA is the owner and is responsible for periodically updating the framework. The Member Organizations are responsible for implementing and complying with the framework.
1.6 Interpretation
SAMA, as the owner of the framework, is solely responsible for providing interpretations of the principles and Control Requirements, if required.
1.7 Target Audience
The Framework is intended for senior and executive management, business owners, owners of information assets, CIOs and those who are responsible for and involved in defining, implementing and reviewing IT controls within the Member Organizations.
1.8 Review, Updates and Maintenance SAMA will review the Framework periodically to determine the Framework's effectiveness, including the effectiveness of the Framework to address emerging IT threats and risks. If applicable, SAMA will update
the Framework based on the outcome of the review.
If a Member Organization considers that an update to the framework is required, the Member Organization should formally submit the requested update to SAMA. SAMA will review the requested update, and when applicable, the Framework will be adjusted on the next updated version.
The Member Organization will remain responsible to be compliant with the framework pending the next version update.
Please refer to 'Appendix A – How to request an Update to the Framework' for the process of requesting an update to the Framework.
Version control will be implemented for maintaining the framework. Whenever any changes are made, the preceding version shall be retired and the new version shall be published and communicated to all Member Organizations. For the convenience of the Member Organizations, changes to the framework shall be clearly indicated.
1.9 Reading Guide
The Framework is structured as follows. Chapter 2 elaborates on the structure of the Framework, and provides instructions on how to apply the Framework. Chapter 3 presents the actual framework, including the IT domains and subdomains, principles, objectives and Control Requirements.
2. Framework Structure and Features

2.1 Structure

The Framework is structured around four main domains, namely:
• Information Technology Governance and Leadership.
• Information Technology Risk Management.
• Information Technology Operations Management.
• System Change Management.
For each domain, several subdomains are defined. A subdomain focusses on a specific IT governance topic.
Per subdomain, the Framework states a principle and Control Requirements.
• A Principle summarizes the main set of required IT controls related to the subdomain.
• The Control Requirements reflects the mandated IT controls that should be considered.
The framework should be implemented in view of principles mentioned in per subdomains along with its associated Control Requirements.
Control Requirements have been uniquely numbered according to the following numbering system throughout the Framework:
Figure 2 – Control requirements numbering system
The figure below illustrates the overall structure of the Framework and indicates the IT Governance Framework domains and subdomains, including a reference to the applicable section of the Framework.

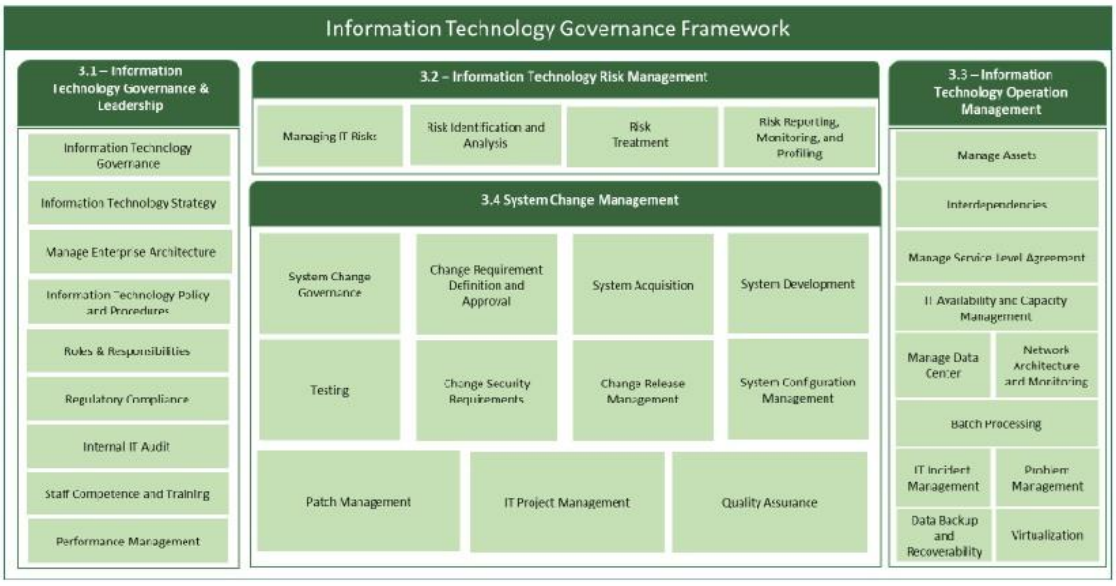


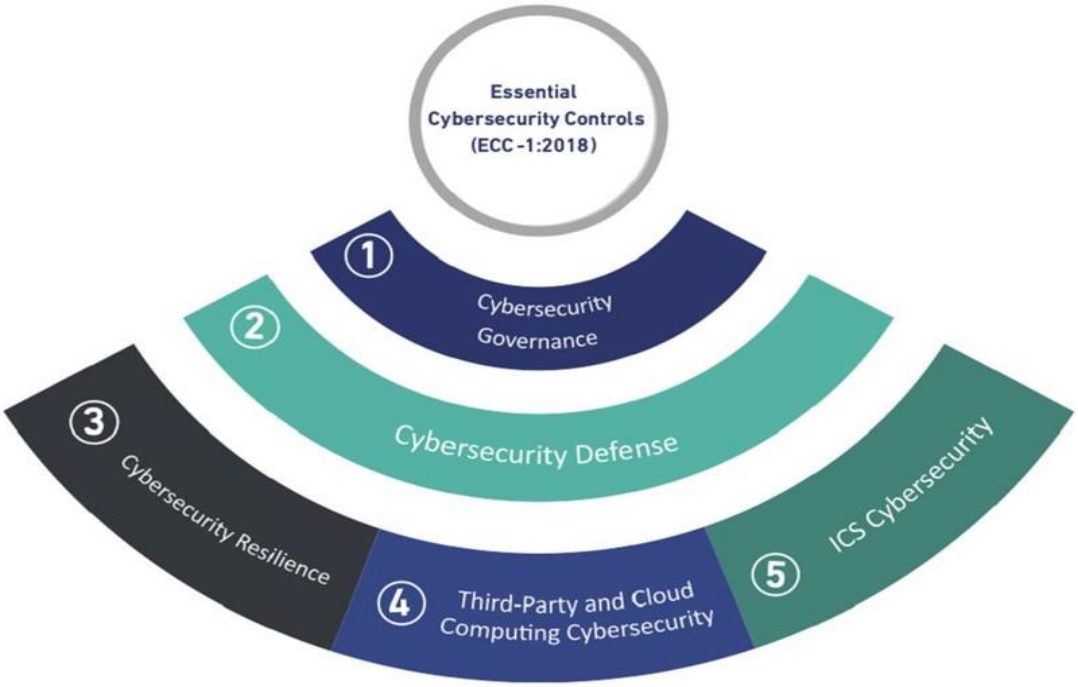
Figure 3 – Information Technology Governance Framework

Lesson2 : Local Frameworks (NCA, SAMA)

NCA & SAMA

As the saying goes...

Assisting your Enterprise to comply with the Kingdom's Regulations



HIDE Consultants can assist your organizations to implement the Kingdom's local regulations like NCA's ECC (Essential Cybersecurity Controls), Cloud Cybersecurity controls and the SAMA framework for Cybersecurity.

SAMA CSF

The Saudi Arabian Monetary Authority (SAMA) established a Cyber Security Framework ("the Framework") to enable Financial Institutions regulated by SAMA ("the Member Organizations") to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework.

NCA ECC

The objective of the Framework is as follows:

- To create a common approach for addressing cyber security within the Member Organizations.
- To achieve an appropriate maturity level of cyber security controls within the Member Organizations.

- To ensure cyber security risks are properly managed throughout the Member Organizations.

· The Framework will be used to periodically assess the maturity level and evaluate the effectiveness of the cyber security controls at Member Organizations, and to compare these with other Member Organizations.

· The Framework is based on the SAMA requirements and industry cyber security standards, such as NIST, ISF, ISO, BASEL and PCI.

NCA ECC

· The Essential Cybersecurity Controls are mandatory where all organizations, within the scope of these controls must implement whatever necessary to ensure continuous compliance with the controls.

NCA ECC

The National Cybersecurity Authority "NCA" has developed the Essential Cybersecurity Controls (ECC - 1: 2018) to set the minimum cybersecurity requirements based on best practices and standards to minimize the cybersecurity risks to the information and technical assets of organizations that originate from internal and external threats.

The Essential Cybersecurity Controls consist of 114 main controls, divided into five main domains:

- Cybersecurity Governance
- Cybersecurity Defense
- Cybersecurity Resilience
- Third-party and Cloud Computing Cybersecurity
- Industrial Control Systems Cybersecurity

.....

Unit Three : Information Security Management

At the end of the unit, the trainee will be able to:

- Explaining information security governance and its role in reducing the risks of electronic information systems.

- Explaining information security governance and its role in reducing the risks of electronic information systems.

- Explains the benefit of information security governance for companies that implement it and the benefits of using it.

- Shows the risks of electronic information systems.

Lesson1 : Scope and Charter of Information Security

Information Security Program Charter

Defines the principles and terms of the College's Information Security Management Program and the responsibilities of the members of the College community in carrying out the Information Security Program.

Owner: Information Technology

Short Description

Defines the principles and terms of the College's Information Security Management Program and the responsibilities of the members of the College community in carrying out the Information Security Program.

Purpose

In the course of carrying out Teachers College academic, research, and service missions, Teachers College's faculty, staff, and students collect many different types of information, including financial, academic, medical, human resources, and other personal information. The College values the ability to communicate and share information appropriately. Federal and state laws and regulations, as well as industry standards, impose obligations on the College and individual members of the TC community to protect the confidentiality, integrity, and availability of information relating to individuals including faculty, staff, students, research subjects, patients, contractors, and donors. Such information is an important resource of the College and any person who uses information collected by the College has a responsibility to maintain and protect this resource. In addition, certain contracts and policies require appropriate safeguarding of information.

This Charter and the College's more specific information security policies (collectively, the "Information Security Policies") define the principles and terms of the College's Information

Security Management Program (the "Information Security Program") and the responsibilities of the members of the College community in carrying out the Information Security Program. The current Information Security Policies are listed in Section 4 – Related Policies.

Scope

The "Information Resources" included in the scope of the Information Security Policies are:

- All Data (as defined in Section 3 below) regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, cloud-based storage) and regardless of form (e.g., text, graphic, video, audio);
- The computing hardware and software Systems (as defined in Section 3 below) that process, transmit and store data; and
- The Networks (as defined in Section 9 below) that transport Data.

This policy applies to all students, staff, faculty members, officers, employees, external users, and affiliates of Teachers College, Columbia University, including extended learning sites, guests, tenants, visitors, contractors, consultants, vendors, individuals authorized by affiliated institutions and organizations, and all others granted use of and/or access to Teachers College, Columbia University technology resources and data.

Because many of the information technology resources of the College are part of the Columbia University network, all College users must be familiar with and adhere to applicable University policies, and to the University's Acceptable Usage of Information Resources Policy.

Use of College information technology resources must also comply with college policies, regardless of whether they make explicit reference to electronic or other media. Relevant policies, including those related to professional conduct and protection from harassment, are available in the College's Policy Library.

Policy

1.1 General Statement

The mission of the Information Security Program is to protect the confidentiality, integrity, and availability of Data. We strive to maintain:

- Confidentiality - information is only accessible to authorized users for authorized purposes.
- Integrity - safeguard the accuracy and completeness of data and processing methods.
- Availability - ensure that authorized users have access to Data and associated Information Resources when required.

1.2 Specific Requirements

The Information Security Charter establishes the various functions within the Information Security Program and authorizes the persons described under each function to carry out the terms of the Information Security Policies. The functions are:

1.2.1 Vice President for Administration and Provost

The Teachers College Vice President for Administration (VPA) and Provost are responsible for oversight and compliance with all Information Security Policies. Such responsibilities include, but are not limited to:

- Assigning Data Stewards and Data Owners;
- Ensuring that each System Owner, Data Steward, and Data Owner appropriately identifies and classifies data in accordance with the Teachers College Data Classification Policy;
- Ensuring that each such System Owner, Data Steward, and Data Owner receives training on how to handle Sensitive Data and Confidential Data; and

- Ensuring that each IT Custodian in his/her area of responsibility provides periodic reports with respect to the inventory of Information Resources used in such areas to the Executive Director of Information Security.

1.2.2 Security, Policy and Compliance Governance

It is the College's goal to govern security, policy and compliance issues relating to the Information Security Program at the organizational level, through establishment of the Teachers College Information Security Advisory Committee (TC-ISAC). This committee will include two permanent members: the Chief Information Officer (CIO) and Executive Director of Information Security.

1.2.3 Security Management

The Executive Director of Information Security is responsible for the day to day management of the Information Security Program which includes

- Developing, documenting and disseminating Information Security Policies, in consultation with affected members of the TC community;
- Working with departments, faculty, and staff to inform them of the acceptable solutions and resolve discrepancies between Information Security objectives and priorities of the departments, faculty, and staff to determine workable solutions and if at an impasse refer the decision to VPA and Provost for resolution based on risk tolerance vs. cost;
- Educating and advising College personnel in information security matters;
- Communicating information regarding Information Security Policies;
- Developing and executing the Risk Management Program for Information Security;
- Collaborating with Data Stewards on any responsibility that may arise concerning information that needs to remain confidential;
- Collaborating with the College's Executive Director for Academic Affairs Compliance on the Family Educational Rights and Privacy Act (FERPA);
- Collaborating with the Office of General Counsel on the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Collaborating with the College's Controller's office on Gramm-Leach-Bliley Act (GLBA);
- Consulting with the College's Office of General Counsel on legal and regulatory issues;
- Translating the Information Security Policies into technical requirements, standards, and procedures;
- Working with the Office of General Counsel and other involved parties on litigation holds and other legally required exceptions to the document retention plan;
- Collaborating with Data Stewards, Custodians, and System Owners to determine the appropriate means of using Information Resources; and

- Authorizing any required exceptions to any Information Security Policy or any associated technical standards or procedures and recording such exceptions for remediation. In addition to the responsibilities listed above, the Executive Staff have granted the authority to the Executive Director to conduct the following activities:
    - Monitoring communications and Data that use the College Network or Systems for transmission or storage;
    - Monitoring use of the College's Digital Information Resources;
    - Conducting vulnerability scans of any Information Resources connected to the College Network;
    - Conducting security assessments of Systems and Data Centers;
    - Disconnecting Information Resources that present a security risk from the College Network;
    - Erasing all Data stored on personal Endpoints previously used for college business, as requested or required; and
- Supporting the College's Emergency Response Team, led by the VPA in connection with any breach or compromise of sensitive data, to the extent provided for in the Teachers College Electronic Data Security Breach Reporting and Response policy (Electronic Data Security Breach Reporting and Response).

1.2.4 Data Ownership and Stewards

Teachers College is the Data Owner of all its Enterprise Data and system assets and is the Security Authority of data classified according to Teachers College Security Classifications. Ownership and rights are governed by Teachers College policies on Intellectual Property.

Data Stewards are College faculty and staff assigned by the Provost and the VPA to define the appropriate level of security for the data and systems under their control in coordination with the Executive Director. This is primarily performed by informing the IT Custodians of the sensitivity of the data using the Data Classification schema so that it can be effectively protected. If the IT Custodian is a vendor, this requires involving the Executive Director in the contract negotiation to establish the appropriate security terms and conditions. Final implementation will be based on a risk assessment of the system and/or processes performed in conjunction with the Executive Director. Such responsibilities are summarized to include, but are not limited to:

- Maintaining the Data and the integrity of the information which supports the functions of their organization by managing data generation, access privileges and confirmation of the resultant stored information;
- Appropriately identifying and classifying Data in their respective areas of responsibilities in accordance with the Teachers College Data Classification Policy;

- Establishing and implementing security requirements for such Data in consultation with the Executive Director;
- Where possible, clearly labeling Sensitive Data and Confidential Data;
- Approving appropriate access to Data and Systems; and
- Ensuring information in all forms (e.g., paper, cloud-hosted data, and TC hosted data) is disposed of according to TC policy and procedure.

1.2.5 System Ownership

System Owners are College faculty and staff who are responsible for requesting or determining computing needs and applicable system hardware and software, to support their respective areas of responsibility and ensuring the functionality of each such system. System ownership is established during the TCIT New Application Assessment process. Such responsibilities include, but are not limited to:

- Identifying the functional requirements of the systems needed to support their area;
- Classifying each System in their respective areas of responsibility based on the identification and classification of Data by the applicable Data Steward;
- Ensuring that each such System that contains Sensitive Data or Confidential Data is scheduled for risk assessment by the Executive Director in accordance with the procedures mandated by the Registration of Systems policy;
- Establishing and implementing security requirements for each such critical system in consultation with the Executive Director, (e.g., encryption of data in transmission and storage, establishing and testing contingency plans for when systems are not available);
- Under guidance from the Executive Director, coordinating with vendors and/or TCIT to ensure that audit and logging mechanisms are in place for sensitive data, with respect to access to the systems or unauthorized changes;
- Maintaining an inventory of such Systems; and
- Ensuring that the IT Custodians follow the Teachers College Computer Lifecycle procedures and the Secure Computing and Information Management Guidelines are followed with electronic files and the department follows the guidelines for paper retention and disposal.

1.2.6 Technical Responsibility

IT Custodians are College staff or third-party service providers who are responsible for providing a secure infrastructure in support of Data and Systems, including, but not limited to, providing and/or ensuring physical security, backup and recovery processes, granting access privileges as authorized by Data Stewards or System Owners and implementing and administering controls over Data in their respective areas of responsibility. Such responsibilities include, but are not limited to:

- Maintaining an inventory of all Endpoints used in their respective areas of responsibility;

- Conducting periodic security checks of Systems and Networks, including password checks, in their respective areas of responsibility;
- Documenting and implementing audit mechanisms, the timing of log reviews and log retention periods;
- Performing self-audits and reporting metrics to the Executive Director and monitoring assessments and appropriate corrective actions; and
- Ensuring that the Teachers College Computer Lifecycle procedures and the Secure Computing and Information Management Guidelines are followed.

1.2.7 System or Data Usage

Users are persons who use Information Resources. Users are responsible for using such Resources properly in compliance with Teachers College policies and procedures including, but not limited to, the Teachers College Acceptable Use of Information Technology policy. Users should not make information available to unauthorized persons, and should ensure appropriate security controls are in place.

1.2.8 IT Security Incident Response Team

Roles and responsibilities for IT Security Incident Response are documented in the “IT Security Incident Response Team Roles and Responsibilities” protocol document.

2 Related Policies

Related Policies

Acceptable Use of Information Technology

Data Classification

Electronic Data Security Breach Reporting and Response

Email Use

Network and Communications Equipment Installation and Maintenance

Use of Social Security Numbers (SSNs), CU UPNs and TC ID Numbers

Computer Lifecycle

Network and Email Accounts

Evacuation Procedures

3 Enforcement

Violations of the Information Security Policies may result in corrective actions which may include: (a) the immediate suspension of computer accounts and network access, and (b) mandatory attendance at additional training as a condition of continued use of computer accounts and network access. Subject to the College’s other rules of conduct and disciplinary procedures, significant violations may also result in (c) a letter to the individual’s personnel or

student file; (d) administrative leave without pay; (e) other sanctions, up to and including termination or non-renewal of employment, faculty appointment or student status. Violations of the Information Security Policies may also result in civil or criminal liability under state, federal, or international laws.

4 Contact Information

TCIT Service Desk - servicedesk@tc.columbia.edu 212.678.3300

Executive Director of Information Security, Infosec@tc.columbia.edu

CIO, CIO@tc.columbia.edu

5 Definitions

As used in the Information Security Policies, the following terms are defined as follows:

Term	Definition
AES	The Advanced Encryption Standard adopted by the U.S. government.
Approved OHCA Email System	As defined in the Teachers College Email Use Policy
Teachers College, the College or TC	Teachers College, Columbia University
Confidential Data	Any information that is contractually protected as confidential information and any other information that is considered by the College appropriate for confidential treatment. See the Teachers College Data Classification Policy for examples of Confidential Data.
Covered Entity	As defined in HIPAA (45 CFR 160.163).
TCIT	Teachers College Information Technology
Data	All items of information that are created, used, stored, or transmitted by the College community for the purpose of carrying out the institutional mission of teaching, research, and educational service and all data used in the execution of the College's business functions.

Data Owner	Teachers College is the owner of all its Enterprise Data and system assets and is the Security Authority of data classified according to Teachers College Security Classifications. Ownership and rights are governed by Teachers College policies on Intellectual Property.
Data Steward	College faculty and staff assigned by the Provost and the VPA to define the appropriate level of security for the data and systems under their control in coordination with the Executive Director.
Email System	A System that transmits, stores, and receives emails.
Endpoint	Any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the College wireless or wired Network, access TC or Columbia email from any local or remote location or access any institutional (College, departmental or individual) System either owned by the College or by an individual and used for college purposes. This would include personal computers such as home computers.
Enterprise Data	Data that is collected and created through Teachers College's normal operations.
EPHI	Electronic Personal Health Information.
FERPA	The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99
GDPR	The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).
HIPAA	The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191
HITECH	The Health Information Technology for Economic and Clinical Health Act
IDEA	The International Data Encryption Algorithm.
Information Resources	All data; computing hardware and software systems that process, transmit, and store data; and networks that transport data.

Information Security Office	The information security resources assigned to support the Information Security Program.
Information Security Program	The TCIT policies, procedures, and resources put in place to protect the confidentiality, integrity, and availability of Data.
Internet of Things (IoT) Devices	Computing devices embedded in everyday objects, such as voice-activated smart speakers.
MAC	Media Access Control.
Mobile Device	A smart/cell phone (i.e., iPhone, Android, Windows phone), tablet (i.e., iPad, Windows, or Android based tablet) laptop or USB/removable drive.
Network	Electronic Information Resources that are implemented to permit the transport of Data between interconnected endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.
OHCA	An Organized Health Care Arrangement, which is an arrangement or relationship, recognized in the HIPAA privacy rules, that allows two or more Covered Entities who participate in joint activities to share PHI about their patients in order to manage and benefit their joint operations.
Payment Card	For purposes of PCI-DSS, any payment card/device that bears the logo of the founding members of PCI SSC (American Express, Discover, JCB International, MasterCard and Visa).
PCI	Payment card industry.
PCI-DSS	The PCI Data Security Standard produced by the PCI–SSC, which mandates compliance requirements for enhancing the security of payment card data.
PCI-SSC	The PCI Security Standards Council, which is an open global forum of payment brands, such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., that are responsible for developing the PCI-DSS.

Peer	A network participant that makes a portion of its resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.
Peer-to-Peer File Sharing Program	A program that allows any computer operating the program to share and make available files stored on the computer to any machine with similar software and protocol.
PHI	Personal Health Information as defined in the Teachers College Data Classification Policy
PII	Personal Identifiable Information as defined in the Teachers College Data Classification Policy
Public Data	Generally available information as defined in the Teachers College Data Classification Policy
Removable Media	CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, medical instrumentation devices, and copiers.
Risk Analysis	The process of identifying, estimating, and prioritizing risks to organizational operations, assets, and individuals. “Risk Assessment” is synonymous with “Risk Analysis”.
Risk Management Program	The combined processes of Risk Analysis, Risk Remediation and Risk Monitoring.
Risk Monitoring	The process of maintaining ongoing awareness of an organization’s information security risks via the risk management program.
Risk Remediation	The process of prioritizing, evaluating, and implementing the appropriate risk-reducing security controls and countermeasures recommended from the risk management process. “Risk Mitigation” or “Corrective Action Planning” is synonymous with “Risk Remediation”.
RSA	The Rivest-Shamir-Adleman Internet encryption and authentication system.
Security Authority	The entity accountable for establishing the policies, standards, and guidelines for the protection of information created by and/or managed by TC and setting the means by which these are enforced.

Sensitive Data	Any information protected by federal, state, and local laws and regulations and industry standards, such as HIPAA, HITECH, FERPA, the New York State Information Security Breach and Notification Act, NYS Shield Act, similar state laws and PCI-DSS. See the Teachers College Data Classification Policy for examples of Sensitive Data.
Server	Any computing device that provides computing services, such as Systems and Applications, to Endpoints over a Network.
SMTP	Simple Mail Transfer Protocol, an internet transportation protocol designed to ensure the reliable and efficient transfer of emails and is used by Email Systems to deliver messages between email providers.
SSL	The Secure Sockets Layer security protocol that encapsulates other network protocols in an encrypted tunnel.
Student Education Records	As defined in the Teachers College Data Classification Policy
System	Server-based software that resides on a single Server or multiple Servers and is used for College purposes. “Application” or “Information System” is synonymous with “System”.
System Owner	College faculty and staff who are responsible for requesting or determining computing needs and applicable system hardware and software, to support their respective areas of responsibility and ensuring the functionality of each such system.
UPS	Uninterruptible Power Supply.
User	Person who uses Information Resources.
User ID	A User Identifier or account name
VPN	Virtual Private Network

Lesson2 : Roles and Responsibilities

Roles and Responsibilities

What are Roles and Responsibilities?

A role is a position or function within an organization that defines the broader purpose and scope of an individual's contribution to the goals. Each role has its unique set of impact, authority, and challenges. Examples of roles include managers, team leaders, departmental executives, etc.

Responsibilities can be defined as the specific tasks and duties assigned to individuals that outline their expectations and how to achieve them. They can be either continuous or one-time tasks and involve activities like decision-making, problem-solving, and communication.

What are the importance of roles and responsibilities?

1. Clarity and direction: They provide clarity and direction to employees by reducing confusion and uncertainties, letting them focus on priorities that align with the overall objectives.

2. Improved productivity: When employees clearly understand their daily tasks and allocated resources, they can focus on their core responsibilities, boosting their productivity.

3. Accountability and ownership: Employees take ownership of their tasks and are accountable for their mistakes, leading to a higher output quality.

4. Conflict resolution: Employees are aware of their professional boundaries and are less likely to overlap with anyone else's efforts, minimizing conflicts.

5. Professional development: Managers find it easier to identify the performance gaps within the teams and take adequate me

asures to bridge them and facilitate the overall development of employees.

What are the different types of roles and responsibilities in an organization?

Many well-defined roles and responsibilities exist within an organization. The most common types are:

1. Manager's Roles and Responsibilities:

It includes guiding a department or a particular team toward achieving pre-defined goals. Their main responsibilities involve planning, organizing, coordinating the team's efforts and allocating adequate resources efficiently. Managers also make strategic decisions, provide feedback, resolve conflicts, and maintain a positive work culture within the team or department.

2. Employee Roles and Responsibilities:

They fulfill assigned tasks, meet management expectations, and contribute to goals and objectives. Employees' primary responsibilities include:

1. Executing routine tasks.
2. Collaborating with different team members.
3. Constantly upskilling oneself.
4. Effectively communicating with stakeholders.

Additionally, they must adhere to the company's policies, strict deadlines, and growth mindset to drive individual and organizational development.

3. Team Leader roles and responsibilities:

A team leader is responsible for guiding and coordinating a team's collective efforts toward achieving the organizational goals and objectives. Their key roles include setting objectives,

delegating tasks, fostering effective communication, motivating team members, and tracking the team's overall progress. They act as the connecting link between the team and higher management and provide regular updates and feedback to the team members.

4. IT roles and responsibilities:

The most prominent role of IT comprises of maintaining the organization's network and servers, providing technical assistance to employees, protecting sensitive data from cyber threats, creating software applications, and analyzing data to support decision- making. They are also responsible for ensuring the reliability and efficiency of the organization's various systems.

5. Business Analyst roles and responsibilities:

Business analyst analyzes business processes, systems, and data to identify gaps and improvement areas. They are responsible for documenting needs, improving stakeholder communication, and aligning departmental needs with business goals. They also assist in managing projects, training employees and leading change management activities to ensure organizational agility.

6. Project Manager roles and responsibilities:

A project manager's roles and responsibilities comprise of overseeing the planning, execution and completion of a project, managing allocated budget and resources, coordinating team members' efforts and minimizing risks. Ultimately, they are responsible for delivering the project on time, within the defined budget and with superior-quality results.

What are the key roles and responsibilities of various HR positions in a company?

In an organization, HRs have many functions with defined roles and responsibilities. Here are the key roles and responsibilities of various HR functions:

1. HR Executive roles and responsibilities:

An HR executive's key roles and responsibilities are assisting with the recruitment and onboarding process, managing employee documents, administering company and HR policies, managing grievances, and ensuring organizational compliance with industry standards and employee laws. They also assist in improving the overall HR department's effectiveness.

2. HR Generalist roles and responsibilities:

HR generalists are responsible for administering payroll and employee benefits, maintaining HR information systems, assisting in performance management process, and supporting organization-wide HR initiatives. They ensure the smooth functioning of the HR processes across the company and enhance employee satisfaction.

3. HR Manager roles and responsibilities:

HR managers are responsible for a wide range of activities like developing and executing HR strategies, overseeing recruitment and selection processes, managing employee grievances, supervising career development opportunities and managing HR budget and resources. HR

managers also play a vital role in driving employee engagement and cultivating a positive work environment.

4. HRBP roles and responsibilities:

The key roles and responsibilities of HRBP include acting as strategic partners to business leaders, aligning HR strategies with business objectives, talent management and workforce planning, and handling employee relations. They are critical players in aligning HR practices with the overall business objectives.

How to write roles and responsibilities?

The HR department is often assigned to define the specific roles and responsibilities for various positions in the organization. They need to be careful while crafting the roles and responsibilities, as they should be clear, concise and specific to the positions. Here is a step-by-step guide on how to write effective roles and responsibilities:

1. Identify the role: Clearly define the position for which the roles and responsibilities need to be written, as it helps set the context of the specific duties and obligations.

2. Understand the role: Identify the key functions and performance expectations by consulting subject matter experts and conducting extensive research on similar positions.

3. Start with action verbs: Starting each responsibility with an action verb like “manage”, “coordinate”, “develop” etc., conveys clear expected actions.

4. Use bullet points: Present the responsibilities in an “easy-to-read” format, making it easier for individuals to gain clarity on the role expectations.

5. Consider the level of responsibility: Tailor the responsibilities based on the impact of the job role and align them with the overall business objectives.

6. Review and refine: Proofread the roles and responsibilities to avoid shortcomings and then gather feedback from various stakeholders to refine them further.

Roles and Responsibilities

Bring clarity to your team with the Roles and Responsibilities Play, a structured practice designed to define team members' roles within a project.

This practice helps reduce confusion, avoid duplication of effort, and ensure that everyone understands their specific contributions to the team's objectives by defining who is responsible for what.

Atlassian teams run this Play at the start of a project or when integrating new team members to help foster better collaboration and alignment.

Lesson3 : Security Organization and Management Styles

What is security management?

Security management is the high-level process of cataloguing enterprise IT assets and developing the documentation and policies to protect them from internal and external threats and cyberthreats. Although the types of identified assets will vary from organization to organization, they will often include people, physical facilities, technology and data. Beyond categorization, this exhaustive analysis helps identify potential security risks and inform procedures for managing, responding and resolving threats, especially as they relate to cybersecurity.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) co-published a series of requirements and recommendations that help inform and certify security management systems, called ISO/IEC 27001. First created in 2003 in the Netherlands and later updated in 2013, it's now often used as the standard for developing IT and data security strategies.

Why is security management important?

Security management is important because it gives enterprises and organizations a proven, reliable groundwork for protecting their infrastructure from loss, theft and disruption – primarily for cybersecurity purposes. For companies, especially ones working with massive amounts of data, applications and other workloads across distributed networks and multiple locations, thorough risk analysis and assessment can help prevent cyberattacks from happening, minimize downtime during and after an attack and improve recovery time.

Related HPE Solutions, Products or Services

Security Risk Compliance

HPE Security Solutions

Project Cosigno

Enterprise Security Services

Security management also establishes IT roles and procedures through formal documentation, helping eliminate role confusion, human errors and miscues as well as ensuring compliance with industry standards and regulations. Thorough security management can even standardize the process of adding new components and infrastructure.

Related Topics

Infrastructure Security

IT Security

Security Monitoring

How does security management work?

The security management process can be broken down into three general phases: assessment, awareness and activation.

Assessment

During this stage, security leaders establish the policy framework for their IT. The first step is conducting an in-depth itemization of all IT assets – every device, piece of hardware and software, and beyond – and comparing it to an organization's business and compliance needs, as well as vetting existing IT for any vulnerabilities or gaps and assigning credential protocols. Once completed, IT leadership can use those findings to inform policy and procedure creation.

Awareness

With the security management structure in place, the next step involves sharing the results and educating not only the IT team but all employees in the organization. The education portion can include anything from basic cybersecurity best practices to detailing roles and responsibilities with third-party providers.

Activation

The final phase consists of several important actions, namely strategy enforcement for compliance, comprehensive monitoring and response, and routine maintenance. And while, in some respects, this phase represents a final set of actions, it also includes ongoing revisions as needed, whether for adapting to new business needs, incorporating new technologies or responding to new threats.

What are the risks of forgoing security management?

Not accounting for or protecting your IT structure from end to end can have costly – and catastrophic – consequences. Not only will cyberattacks and other cyberthreats find ways to infiltrate your network and damage, steal and destroy data and resources virtually at will, but those compromises can impact people outside of the organization. For example, a hacktivist could disrupt an oil and gas producer’s operations, setting off a series of events that could include lost revenue, interrupted supply chains, higher gas prices and, in extreme situations, compromised safety functions that could lead to employees being injured or worse. What’s more, having a reputation for haphazard security measures can hurt your public image, you're standing within the industry and your potential for future growth.

Internally, security management makes managing your IT environments more efficient and proactive. Without it, you risk lapses in security oversight that could lead to slower threat

identification and response times, unclear protocols and responsibilities, an inability to adapt to evolving cybersecurity issues and, ultimately, stymied innovation potential.

What is cloud security management?

Cloud security management is a sub-specialization of security management. While developing cloud security policies follows a similar path (e.g. assessment, awareness and activation), it focuses on cloud-specific infrastructure rather than physical assets, with the ultimate goal of securing digital assets via rigorous access controls, data encryption and analysis, and proactive monitoring.

Strong cloud security management enables lots of IT flexibility and opportunities for automation. Like traditional security management, it can help maintain compliance, protect reputations and reduce demand on IT teams. With monitoring and other tasks offloaded to artificial intelligence (AI) and machine learning (ML), IT teams can spend less time on mundane, labor-intensive workloads.

HPE and security management

HPE is well known for its high-performance and secure portfolio of products and services, from powerful hardware to end-to-end solutions. These services are designed for enterprise-level deployments that can reinforce existing security strategies and transform security from a time-consuming obstacle to an accelerator of innovation.

Options such as **HPE Security and Digital Protection Services** provide edge, cloud and data protection using adaptive models and industry expertise to keep pace with new cyberthreats and technology initiatives, with risk and security management solutions that include modern approaches like Zero Trust security and DevSecOps with industry standards such as NIST. For more infrastructure-specific security, **HPE Security Solutions** offers silicon-to-cloud defenses across distributed networks.

Other HPE security offerings such as **Project Cosigno** focus specifically on identity authentication. Rooted in Zero Trust protocols, it provides security and infrastructure engineering teams with a web-scale, unified platform to broker and issue service identities. Unlike other approaches, the solution provides scalable, cryptographic, platform-agnostic identities based on open standards (SPIFFE). As a result, it enables companies to boost security operations and developer productivity, reduce application on-boarding and accelerate cloud or container adoption while strengthening overall security.

What is Security Management?

Security management covers all aspects of protecting an organization’s assets – including computers, people, buildings, and other assets – against risk. A security management strategy begins by identifying these assets, developing and implementing policies and procedures for protecting them, and maintaining and maturing these programs over time.

Below, we discuss what security management means to organizations, types of security management, and review some considerations for security management when choosing a cyber security solution

uprose of Security Management

The goal of security management procedures is to provide a foundation for an organization's cybersecurity strategy. The information and procedures developed as part of security management processes will be used for data classification, risk management, and threat detection and response.

These procedures enable an organization to effectively identify potential threats to the organization's assets, classify and categorize assets based on their importance to the organization, and to rate vulnerabilities based on their probability of exploitation and the potential impact to the organization.

Types of Security Management

Security management can come in various different forms. Three common types of security management strategies include information, network, and cyber security management.

#1. Information Security Management

Information security management includes implementing security best practices and standards designed to mitigate threats to data like those found in the ISO/IEC 27000 family of standards. Information security management programs should ensure the confidentiality, integrity, and availability of data.

Many organizations have internal policies for managing access to data, but some industries have external standards and regulations as well. For example, healthcare organizations are governed by the Health Insurance Portability and Accessibility Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) protects payment card information.

#2. Network Security Management

Network security management is a vital component of a network management strategy. The network is the vector by which most cyberattacks reach an organization's systems and its first line of defense against cyber threats. Network security management includes deploying network monitoring and defense solutions, implementing network segmentation, and controlling access to the network and the devices connected to it.

#3. Cybersecurity Management

Cybersecurity management refers to a more general approach to protecting an organization and its IT assets against cyber threats. This form of security management includes protecting all aspects of an organization's IT infrastructure, including the network, cloud infrastructure, mobile devices, Internet of Things (IoT) devices, and applications and APIs.

Security Management Architecture

A scalable and sustainable security management strategy is one that is built using an integrated framework and the right tools rather than a disconnected set of standalone policies and strategies. A security management architecture enables an organization to consistently enforce its security policies across its entire IT ecosystem. This requires an array of integrated security solutions that enable centralized management and control of an organization's entire security infrastructure.

Impact of DevSecOps on Security Management

A shift is on to automate security management using DevOps. There are many security tasks that are repetitive and take time to complete when using a management user interface. Security automation is a valuable tool for reducing the time spent completing tasks.

Examples of security management tasks that could benefit from automation include:

- Adding rules and objects to a security policy to complete a new project.
- Responding to a security incident by validating threat indicators, mitigating the threat by isolating the infected host, and searching logs for other infected hosts using Indicators of Compromise (IoC) returned from the security incident analysis.
- Provisioning new cloud infrastructures, including the firewalls and the security policy for the firewalls protecting the new infrastructure.
- Cloud applications of DevSecOps include container image scanning, code scanning, Infrastructure as a Code (IaC) scanning, and scanning for credential exposure.

Security Management with Check Point

Effective security management requires having the right tools for the job. One critical tool for security management is a cybersecurity platform that enables an organization to maximize the effectiveness and efficiency of its security team. Without proper monitoring and management, even the best security solutions cannot protect an organization against cyber threats.

Security management has always been one of Check Point's core competencies, and we continually work to evolve security and management capabilities to meet the evolving needs of the market and our customers. Check Point security management can be deployed on the platform of your choice; turn-key security management appliances, open server hardware, in public and private cloud environments, and as a hosted cloud service. Check Point's security management solutions are based on four key pillars, including:

- **Security Automation into CI/CD Pipelines**: Integrating security into CI/CD pipelines via automation reduces configuration errors, makes rapid deployments possible, and allows operational processes to be orchestrated.

Security Consolidation: Consolidated security improves efficiency, reduces capital and operational expenditure (CAPEX and OPEX), and achieves improved visibility and context by integrating security policy and events management within a single solution.

- **Solution Agility**: Security management solutions must be agile and dynamic to keep up with the evolving cyber threat landscape. An example is an object in the security policy that defines private or public cloud addresses or users. As these external entities change, so does the security policy.
- **Efficient Operations**: Security should be a business enabler, not a roadblock. Security management solutions must be efficient to not inhibit security innovation. For example, easy to use management that unifies security and event management and enables delegated access to multiple admins at the same time enables security staff to do more in less time.

We invite you to download our whitepaper on security management and read more about the Check Point security management solution.

Lesson4 : Security Investments

What Are Investment Securities?

Investment securities are a category of securities-tradable financial assets such as equities or fixed income instruments-that are purchased with the intention of holding them for investment. As opposed to investment securities, in general, securities are purchased by a broker-dealer or other intermediary for quick resale.

Investment securities are subject to governance via Article 8 of the Uniform Commercial Code (UCC).

Key Takeaways

- Investment securities are a category of securities-tradable financial assets such as equities or fixed income instruments-that are purchased with the intention of holding them for investment.
- Banks often purchase marketable securities to hold in their portfolios; these are usually one of two main sources of revenue, along with loans.
- Investment securities held by banks as collateral can take the form of equity (ownership stakes) in corporations or debt securities.

Understanding Investment Securities

Banks often purchase marketable securities to hold in their portfolios; these are usually one of two main sources of revenue, along with loans. Investment securities can be found on the balance sheet assets of many banks, carried at amortized book value (defined as the original cost less amortization until the present date).

The main difference between loans and investment securities is that loans are generally acquired through a process of direct negotiation between the borrower and lender, while the acquisition of investment securities is typically through a third-party broker or dealer. Investment securities at banks are subject to capital restrictions. For example, the number of Type II securities or securities issued by a state government is restricted to 10% of the bank's overall capital and surplus.

Investment securities provide banks with the advantage of liquidity, in addition to the profits from realized capital gains when these are sold. If they are investment-grade, these investment securities are often able to help banks meet their pledge requirements for government deposits. In this instance, investment securities can be viewed as collateral.

Types of Investment Securities

Equity Stakes

As with all securities, investment securities held by banks as collateral can take the form of equity (ownership stakes) in corporations or debt securities. Equity stakes can be in the form of preferred or common shares-although it is critical that they provide a measure of safety in this case. High-risk, high-reward securities, such as initial public offering (IPO) allocations or small gap growth companies, might not be appropriate for investment securities. Some companies offer dual-class stock, which provide distinct voting rights and dividend payments.

Debt Securities

Debt securities can take the common forms of secured or unsecured corporate debentures. (Secured corporate debentures can be backed by company assets, such as a mortgage or company equipment). In this scenario, secured debt (also called investment-grade) would be preferred. Treasury bonds or Treasury bills and municipal bonds (state, county, municipal issues) are also options for a bank’s investment securities portfolio. Again, these bonds should be investment-grade.

While securities, in general, include derivative securities-such as mortgage-backed securities, whose value is derived from the asset(s) underlying the financial instrument-these are higher risk and not often encouraged to be part of a bank’s investment securities portfolio.

Money Market Securities

Other types of investment securities can include money-market securities for quick conversion to cash. These generally take the form of commercial paper (unsecured, short-term corporate

debt that matures in 270 days or less), repurchase agreements, negotiable certificates of deposit (CDs), bankers' acceptances, and/or federal funds.

Sponsored

Receive 80% Trading Profits + Refundable Fees*

For a one-time fee, join the Vantage Elite Challenge today and receive up to $200,000 in simulated funds to trade through CFDs. Earn up to 80% of your trading profits upon successful completion. Use these funds to test your strategies, hone your skills, and maximize your earnings potential.*

Investment Securities

The links in this section primarily cover money market mutual fund investments and securities purchased by banks for their own accounts. Money market generally refers to the markets for short-term credit instruments, such as commercial paper, bankers' acceptances, negotiable certificates of deposit, repurchase agreements, and federal funds.

.....

Unit Four : Information Security Strategy

At the end of the unit, the trainee will be able to:

- Distinguish between internal and external risks faced by electronic information systems.

- Analyzes the role of external risks to information systems, including hacking, data and information theft, malware, viruses, and network sabotage.

- Identify threats in information security (information security threats)

- Mentions the importance of data governance for institutions and companies.

Lesson1 : Information Security Strategy

The information security strategy is one component of a defensible program

Effective cybersecurity, also referred to here as information security, requires a complete and defensible security program that ensures a balance between protecting and running the business. It includes five key components:

1. **An enterprise information security charter: Executive mandate**

This is a short document written in plain language that establishes clear owner accountability for protecting information resources, and provides a mandate for the CISO to establish and maintain the security program.

This charter document must be read, understood, signed off, visibly endorsed and annually reaffirmed by the CEO and board of the organization.

2. **Terms of reference: Reference model**

A key element of a defensible program is the ability to demonstrate that the organization is in line with accepted practices and standards. With respect to the security program, this means using one or more taxonomical reference models, based on accepted industry standards (such as the NIST cybersecurity framework [CSF], ISO/IEC 27001/2 or CIS Controls [formerly known as Critical Security Controls]) to guide strategic and tactical decisions.

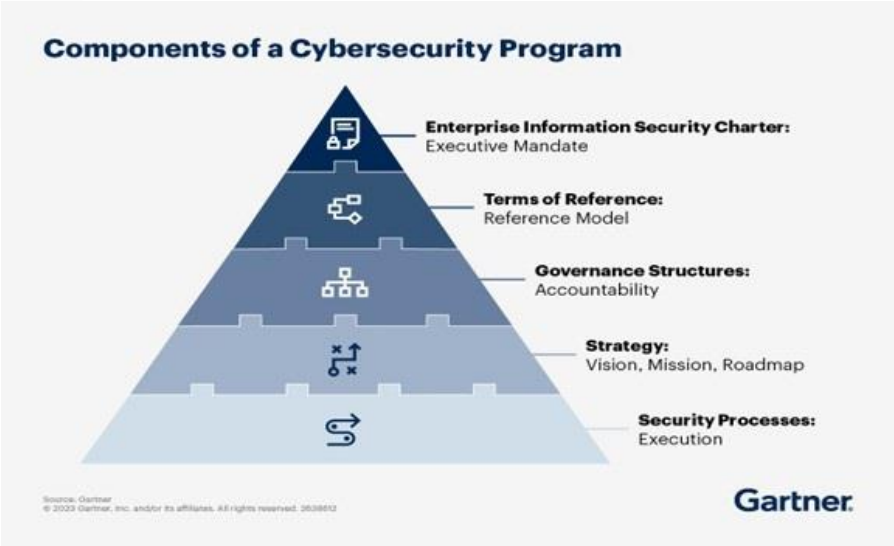
3. **Governance structures: Accountability**

Many regulations require organizations to have a CISO with appropriate independence from information resource and control owners. A virtual CISO can be an acceptable compromise in some situations. The CISO function ideally reports outside the office of the CIO to avoid certain conflicts of interest.

As for decision making, an enterprise security steering committee can be an effective forum for discussing security challenges, proposed policies and investment plans. This forum should include representatives from information-owning business units and staff functions (IT, legal, HR and privacy office). Executive reporting frameworks and processes should also be defined.

4. **Strategy: Vision, mission and roadmap**

Getting business support for the security program requires a clear vision that explains its components and objectives and how they relate to business goals. The vision should align with proven practices and standards, and be grounded in current state assessments for the organization, as well as peer benchmarks on level of spend, number of staff, program maturity or levels of compliance with generally accepted standards. See the vision, current state and prioritization tabs for more details.



5. **Security processes: Execution**

The security program must be geared toward anticipating and reacting to frequent, unexpected changes in the business, technology and operating environments. It should also drive continuous improvement in the effectiveness and efficiency of security controls.

The ability to continuously improve while simultaneously reacting to change requires the information security program to agree on a set of principles that guide security implementation and operations on a day-to-day basis, such as:

- Making control decisions based on specific risk and risk appetite rather than on check-box compliance
- Supporting business outcomes rather than solely protecting the infrastructure
- Always considering the human element when designing and managing security controls

Experience IT Security and Risk Management conferences

Join your peers for the unveiling of the latest insights at Gartner conferences.

Lesson2 : Strategy Development Methodologies

The Top 5 Strategic Planning Methodologies

Strategic planning is an integral part of any business' success, and it will ensure your business is heading in the right direction. Furthermore, it helps outline your objectives as it's crucial to helping business owners make their everyday decisions.

With the best strategic planning methodology in place, your business will be proactive as opposed to being reactive. You will seamlessly increase your operational efficiency with proper strategic planning and projects. Your profitability and market share will increase significantly. Your business will be more relevant in its respective industry since you will serve your customer base better. However, as important as strategic planning is, many businesses have yet to emulate this opportunity. Also, a single strategic model isn't better than other models.

So, we've come up with the 5 best strategic planning methodologies that will help make your business thrive. But first, let's see what a strategic planning model is and why it's important.

What Is a Strategic Planning Model?

It refers to how a business creates a plan and implements it to make its operations better and further meet its business goals. Your business can benefit a great deal by having a well-defined strategic planning model in place.

For instance, a good strategic planning model will ensure all departments of a business work harmoniously. Moreover, it allows businesses to achieve their targets in the long-run.

Every business leader should know the basics of strategic planning to enable them to come up with an appropriate strategic planning model. Such basics include developing your business' strategic goals, as well as their potential impacts. You have to define your goals while creating your plan. Factor in defining your key goals, long-term goals, operational goals, and company goals. The basics further include crafting strategies for the development of your strategic planning model.

Top 5 Strategic Planning Methodologies

Below are some suitable strategic methodologies you should emulate in your strategic planning process:

Basic Planning Methodology

The strategic planning methodology is also referred to as the simple strategic planning model. Businesses that utilize this structure include startups or businesses that have little knowledge in strategic planning. Moreover, the model is ideal for smaller companies that lack resources to execute complex strategic planning methodologies.

It also focuses on developing your business' mission, vision statement and core values. Business leaders can use the model to outline the steps they should take to achieve their business goals. Basic strategic planning methodology can further enable business leaders to monitor the progress of their businesses.

The main advantage of using this strategic planning model is that it helps you create a solid mission statement that perfectly describes why your business exists. Furthermore, you can use it as a resource to select your company's intermediate goals in regard to what you should accomplish first.

The basic strategic planning methodology helps you create actionable plans that outline the elaborate steps your business should take to implement certain strategies. You can effectively monitor your progress while using this model.

Goal-based Strategic Planning Methodology

Businesses that start with using basic strategic planning methodology shift to goal-based strategic planning methodology over time. The model is suitable for established organizations or businesses seeking for more complex strategic planning methodologies. It is the most frequently used strategic planning model.

It starts with an analysis of a business' weaknesses, threats and opportunities. Goal-based strategic planning methodology also focuses on your business' internal and external factors and threats and competition. Next, you can use the strategic planning model to identify issues and goals which you can use to prioritize your business objectives.

Alignment Strategic Planning Methodology

The methodology helps you craft a strong relation between your business' mission and resources. The model can be a perfect tool for your business, especially if you are striving to fine tune your objectives and identify why you aren't achieving your goals.

This model helps you outline your business' resources. It further helps business owners establish the specific aspects of their businesses that are working appropriately, and which aspects need some adjustments. Finally, you can include these adjustments in your business plan. This step is the most important step in making an effective business plan.

Organic Strategic Planning Methodology

The strategic planning methodology doesn't use linear methodological approaches, unlike other strategic planning models. Organic strategic planning methodology uses an approach that strategic planning experts call story boarding. This approach allows business owners to develop unique business ideas. It can prompt you to be active on matters that affect your business.

The planning models start with clarifying your business' cultural values through dialogues and storyboarding techniques. Next, the strategic planning methodology focuses on articulating a business' vision. The accomplishments of this methodology translate into a business' goals.

Scenario Strategic Planning Methodology

This is another common strategic planning methodology to consider. It is more of a strategic planning technique rather than a strategic planning methodology. The methodology is highly effective in identifying issues, goals and external environments. It is useful for businesses that are preparing for a variety of scenarios that are the result of external forces of changes in the business environment.

The strategic planning model starts with establishing vulnerabilities that could possibly affect a business. After identifying possible vulnerabilities , you can look into strategies you can use for responding to the prevailing vulnerabilities.

Balanced Scorecard

The strategic planning methodology entails considering your business' objectives, initiatives and measures. You can develop this model by using programs such as Google Sheets, PowerPoint and Excel. The strategic planning methodology gives you comprehensive details into your business' initiatives and measures.

Strategy Mapping

The strategic planning methodology is a tool that is used for communicating a strategic plan. The tool is suitable for achieving high-level business goals. It helps communicate-high-level details across your business in an easy-to-understand model. The strategic planning model offers an array of benefits including:

- A simple and straightforward visual representation that is easy for organization and businesses to refer to during the development process
- It helps unify all company goals into one business strategy and comprehensive plan
- It can help you determine your key basic steps and goals
- It helps you establish how your business objectives affect others in real time

Other strategic planning tools

There are many strategic opportunities and complaints you can implement to accomplish your business objectives. Whether you are seeking to reduce complaints in your store by providing better purchase and return policies, or you would like to reduce your production manufacturing costs by implementing better processes and detailed action plans, these strategic planning tools will work for you.

SWOT Analysis

A SWOT analysis is a strategic planning model that businesses can use in the beginning of their strategic planning process.

The strategic planning methodology helps analyze your business' weaknesses, threats, strengths, and opportunities. Conducting a SWOT analysis is vital to helping you identify your

business' progress and the specific areas you should improve. At the end of the day, managers and staff from human resources need to be on-board with their strategic plan in its entirety for it to be effective, including their SWOT strategy. Here is a breakdown on how to do a SWOT analysis:

- Decide on the objectivity of your SWOT analysis
- Research your market position and industry
- List your company's strengths
- List your business's weaknesses
- List potential external opportunities and repeatable processes
- List potential threats and major issues
- Establish the priorities from your SWOT analysis

Lesson3 : Information Security Strategy Elements

10 Key Elements of Information Security Policy

One of the inevitable outcomes of growth that doesn't get the attention it deserves is security risk. As the organization grows, technologies and third-party systems become mainstay. This directly increases the probability of risk. Information security policy is the glue that holds everything together in a way that nothing falls apart.

Let us understand what information security policy is, its importance, and the key elements.

Table of Content

What is information security policy?

Information security policy is a set of rules, practices, guidelines, and processes that governs the management, protection, and access of information. It ensures the confidentiality, integrity, and availability of networks, applications, systems, programs, and data across the infrastructure.

An effective information security policy helps to document security policies, respond to incidents, protect sensitive client data, and comply with regulatory frameworks like ISO, SOC, or HIPAA.

10 Most Important Elements of Information Security Policy?

Information security policy combines several elements to create a holistic approach to protection against threats. This includes:

1. Purpose

Program policies are actionable strategies that define the goals and scope. It should include your approach to information security, preventive measures, threat detection systems, legal compliance, and data transparency to clients.

2. Audience

Clarity on each policy, its clauses, and subsets help end users understand their roles and responsibilities. Employees, top management, third parties, and consultants should be aware of what they are accountable for.

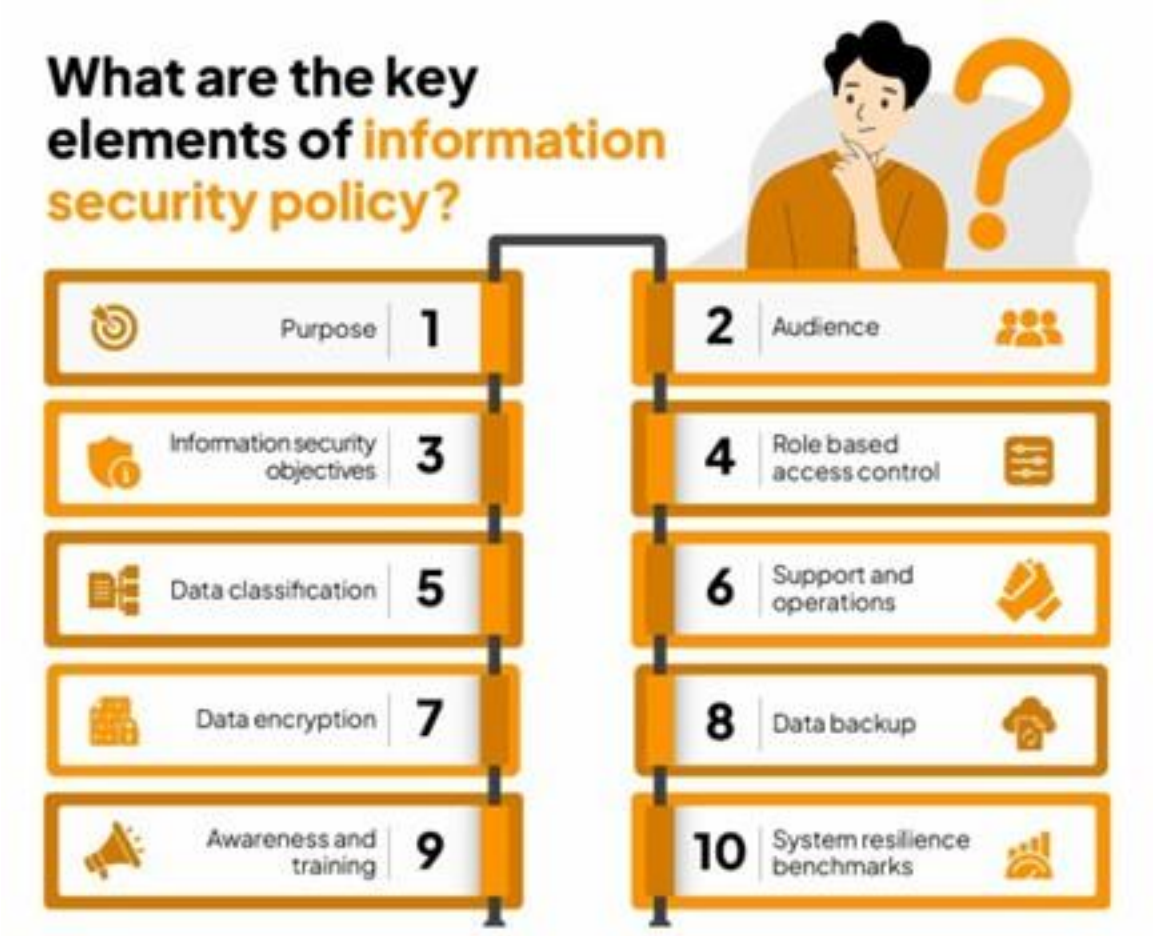
3. Information security objectives

Refers to the trinity of information security; integrity, confidentiality, and availability.

- Integrity means that the data is complete, accurate, and fully operational.
- Confidentiality refers to protecting data from unauthorized access by implementing privileged or role-based access.
- Availability allows privileged users to access information required to carry out their functions as and when required.

4. Role-based access control

Every business infrastructure comprises heterogeneous data. Your policy should be set up to allow each function and subfunction to access data needed for their tasks – also known as the principle of least privilege. This helps to reduce data loss or accidental disclosure.



5. Data classification

Data classification is a good practice that helps organizations prevent intentional or accidental disclosure. You can conduct a risk assessment to categorize data into the following levels:

- Publicly available information.
- Confidential data that would cause zero or little damage is disclosed.
- Confidential data that would potentially cause substantial harm if leaked to the public.
- Confidential data that would undoubtedly cause substantial harm if leaked to the public.

6. Support and operations

Comprises three types of measures to protect all levels of data.

- Data protection regulation: Its systems that store, process, or manage sensitive data should be compliant with industry standards and best practices. These include but are not limited to data encryption, incident response plan, backup and recovery, anti-malware, firewalls, password management, and protection against insider threats.
- Data backup: Ransomware, a type attack where malicious actors hack into a system, encrypt the data, and render it inaccessible till a ransom is paid has become the most common threat. You can avoid this by regularly backing up data in multiple locations.
- Data movement: Data in transit via electronic means should be secured through encryption and Data Loss Prevention (DLP) methods.

7. Data encryption

Whether you deploy data on the cloud or on-premise, it is transmitted electronically. To secure this data, you can use end-to-end protection measures such as:

- Advanced encryption standard (AES) to protect the online data transfer. It is an industry-standard encryption protocol that uses the same key to encrypt and decrypt. AES encryption keys are of three lengths – AES-128, AES-192, and AES-256. AES-256 is the strongest of the three, as the number of possible key combinations is the highest.
- Transport layer security (TLS) to safely transfer data via HTTPS. This method uses cryptography to secure email, payment card details, messaging, and VOIP.

8. Data backup

A strong backup and business contingency plan to ensure data integrity is crucial to retrieve information in case an incident occurs. Ensure this by

- Create backups as often as needed. You can do that manually or automate it.
- Encrypt your data while creating backups.
- Monitor the backed up data, keep track of changes, and maintain an audit log.

9. Awareness and training

Your employees are on the front lines of defense against a number of security threats. They should be familiar with the policies adopted by your organization along with industry-specific regulations or framework requirements. Basic knowledge to identify threats, know what constitutes good security practices, and steps to take against potential threats should be prioritized as a part of your training and awareness program.

10. System resilience benchmarks

Include security benchmarks such as Windows server, Linux, AWS, Kubernetes, and others in your security policy.

Easy Automated Risk Insights

Importance of information security policy

When you implement information security policies, it makes a huge impact on the overall security posture. Most organizations don't chalk out a budget for security until they face a compromise. This is a bad practice, as ISP is no longer optional for the following reasons:

The accelerated rate of digitization has increased the volume of assets deployed on the cloud—there is more sensitive data on devices than ever before.

This shift turned the cloud into a magnet for malicious actors. For businesses that store sensitive information, a security policy helps to identify and contain breach attempts should be a priority.

After May 2020, there was a 176% spike in use and installation of collaboration tools. As business dependency on third-party solutions increases, more risks add to the ecosystem.

Between 2020 and 2021, third-party breaches rose by 17%. With IPS, you can efficiently manage third-party risks and vendor risks by thoroughly evaluating and assessing them.

Regulatory compliance is compulsory for some businesses and a survival strategy for others, depending on the type of information they process.

For example, healthcare services in the US must be HIPAA compliant. Businesses that process payment must be PCI DSS compliant. If you manage sensitive customer information, SOC 2 or ISO 27001 are recommended.

When you have an information security policy, you can identify and address security gaps as mandated by the applicable framework.

How to build a strong information security policy

Building policies and processes from scratch takes an immense amount of time, cooperation, planning, and resources. Even then small to medium sized businesses with no prior security experience fail to bring it all together with success.

Sprinto brings policies, processes, and people together from a single automated platform so you don't have to break a sweat or worry about compliance failure. It scans your system for non-compliance, alerts users against vulnerabilities, and trains your employees to improve the overall posture. Talk to our experts now about your needs.

What are the objectives of information security policy?

Information security policy seeks to preserve the principles of good security; integrity, availability, and confidentiality of tools and technologies used by members of an organization.

What are the three types of information security policies?

Three common security policies include program policies, system-specific policies, and issue-specific policies.

What is the purpose of information security policy?

A strong information security policy helps to create an efficient process to manage and monitor data assets, document vulnerabilities, changes, and updates, mitigate security threats, and build customer trust.

The 12 Elements of an Information Security Policy

What is an information security policy?

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges. An information security policy makes it possible to coordinate and enforce a security program and communicate security measures to third parties and external auditors.

To be effective, an information security policy should:

- Cover end-to-end security processes across the organization
- Be enforceable and practical
- Be regularly updated in response to business needs and evolving threats
- Be focused on the business goals of your organization

About this Explainer:

This content is part of a series about information security.

The importance of an information security policy

Information security policies can have the following benefits for an organization:

- **Facilitates data integrity, availability, and confidentiality** – Effective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.
- **Protects sensitive data** – Information security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).
- **Minimizes the risk of security incidents** – An information security policy helps organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.
- **Executes security programs across the organization** – Information security policies provide the framework for operationalizing procedures.
- **Provides a clear security statement to third parties** – Information security policies summarize the organization's security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.
- **Helps comply with regulatory requirements** – Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

12 Elements of an Information Security Policy

A security policy can be as broad as you want it to be, from everything related to IT security and the security of related physical assets, but enforceable in its full scope. The following list offers some important considerations when developing an information security policy.

1. Purpose

First state the purpose of the policy, which may be to:

- Create an overall approach to information security., especially as touches standards, security requirements, and best practices adopted by the organization.
- Detect and preempt information security breaches such as misuse of networks, data, applications, and computer systems.
- Maintain the reputation of the organization, and uphold ethical and legal responsibilities and applicable governance.
- Respect employee and customer rights, including how to react to inquiries and complaints about non-compliance.

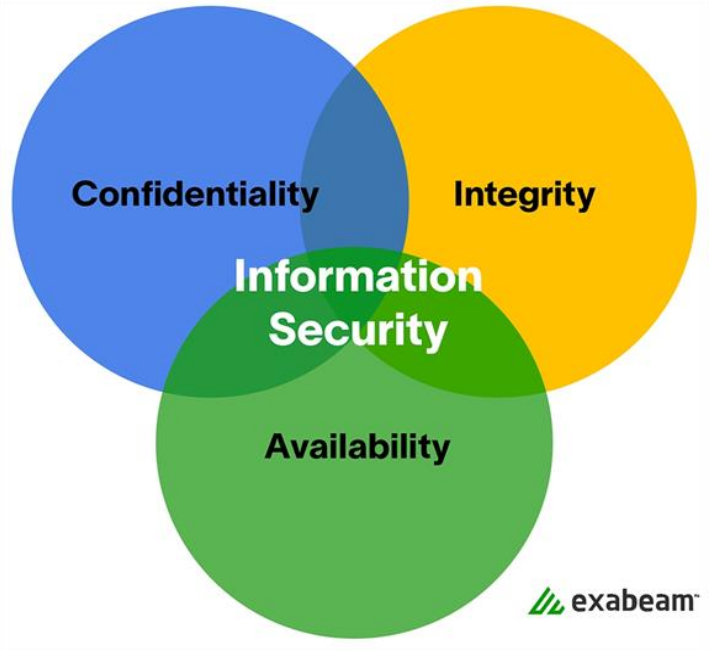
2. Audience

Define the audience to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit which manages security separately may not be in the scope of the policy).

3. Information security objectives

Guide your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives:

- **Confidentiality** - Only authenticated and authorized individuals can access data and information assets.
- **Integrity** - Data should be intact, accurate and complete, and IT systems must be kept operational.
- **Availability** - Users should be able to access information or systems when needed.



4. Authority and access control policy

- **Hierarchical pattern** – A senior manager may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee or contractor. The policy should outline the level of authority over data and IT systems for each organizational role.
- **Network security policy** – Critical patching and other threat mitigation policies are approved and enforced. Users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts.

5. Data classification

The policy should classify data into categories, which may include “top secret,” “secret,” “confidential,” and “public.” The objectives for classifying data are:

- To understand which systems and which operations and applications touch on the most sensitive and controlled data, to properly design security controls for that hardware and software (see 6.)
- To ensure that sensitive data cannot be accessed by individuals with lower clearance levels
- To protect highly important data, and avoid needless security measures for unimportant data

6. Data support and operations

- **Data protection regulations** – systems that store personal data, or other sensitive data — must be protected according to organizational standards, best practices, industry compliance standards, and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection.
- **Data backup** – Encrypt data backup according to industry best practices, both in motion and at rest. Securely store backup media, or move backup to secure cloud storage.
- **Movement of data** – Only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

7. Security awareness and behavior

Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification.

- **Social engineering** – Place a special emphasis on the dangers of social engineering attacks (such as phishing emails or informational requests via phone calls). Make all employees responsible for noticing, preventing, and reporting such attacks.
- **Clean desk policy** – Secure laptops with a cable lock. Shred sensitive documents that are no longer needed. Keep printer areas clean so documents do not fall into the wrong hands.
- Work with HR to define how the internet should be restricted both on work premises and for remote employees using organizational assets. Do you allow YouTube, social media websites, etc.? Block unwanted websites using a proxy.

8. Encryption policy

Encryption involves encoding data to keep it inaccessible to or hidden from unauthorized parties. It helps protect data stored at rest and in transit between locations and ensure that sensitive, private, and proprietary data remains private. It can also improve the security of client-server communication. An encryption policy helps organizations define:

- The devices and media the organization must encrypt
- When encryption is mandatory
- The minimum standards applicable to the chosen encryption software

9. Data backup policy

A data backup policy defines rules and procedures for making backup copies of data. It is an integral component of overall data protection, business continuity, and disaster recovery strategy. Here are key functions of a data backup policy:

- Identifies all information the organization needs to back up
- Determines the frequency of backups, for example, when to perform an initial full backup and when to run incremental backups
- Defines a storage location holding backup data
- Lists all roles in charge of backup processes, for example, a backup administrator and members of the IT team

10. Responsibilities, rights, and duties of personnel

Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

11. System hardening benchmarks

The information security policy should reference security benchmarks the organization will use to harden mission-critical systems, such as the Center for Information Security (CIS) benchmarks for Linux, Windows Server, AWS, and Kubernetes.

12. References to regulations and compliance standards

The information security policy should reference regulations and compliance standards that impact the organization, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the Health Insurance Portability and Accountability Act (HIPAA).

9 best practices for successful information security policies

1. **Information and data classification** – helps an organization understand the value of its data, determine whether the data is at risk, and implement controls to mitigate risks
2. **Developers, security, and IT operations** – should work together to meet compliance and security requirements. Lack of cooperation between departments may lead to configuration errors. Teams that work together in a DevSecOps model can coordinate risk assessment and identification throughout the software development lifecycle to reduce risks.

3. **Security incident response plan** – helps initiate appropriate remediation actions during security incidents. A security incident strategy provides a guideline, which includes initial threat response, priorities identification, and appropriate fixes.
4. **SaaS and cloud policy** – provides the organization with clear cloud and SaaS adoption guidelines, which can provide the foundation for a unified cloud ecosystem and standards of configuration, especially for development environments. This policy can help mitigate ineffective complications and poor use of cloud resources.
5. **Acceptable use policies (AUPs)** – helps prevent data breaches that occur through misuse of company resources. Transparent AUPs help keep all personnel in line with the proper use of company technology resources.
6. **Identity and access management (IAM) regulations** – let IT administrators authorize systems and applications to the right individuals and let employees know how to use and create passwords in a secure way. A simple password policy can reduce identity and access risks.
7. **Data security policy** – outlines the technical operations of the organization and acceptable use standards in accordance with all applicable governance and compliance regulations.
8. **Privacy regulations** – government-enforced regulations such as GDPR and CCPA protect the privacy of end users. Organizations that don't protect the privacy of their user's risk fines and penalties, and in some cases court action.
9. **Personal and mobile devices** – Nowadays, most organizations have moved business processes to the cloud. Companies that permit employees to access company software assets from any location from any device risk introducing vulnerabilities through personal devices such as laptops and smartphones. Creating a policy for proper security of personal devices can help prevent exposure to threats via employee-owned assets.

Learn more about information security:

- Information security (InfoSec): The Complete Guide
- The 8 Elements of an Information Security Policy
- PCI Security: 7 Steps to Becoming PCI Compliant
- Cloud Security 101
- Threat Hunting: Tips and Tools
- IT Security: What You Should Know
- Machine Learning for Cybersecurity: Next-Gen Protection Against Cyber Threats
- Penetration Testing: Process and Tools

Unit Five : Current State and Desired State of Security

At the end of the unit, the trainee will be able to:

- Shows data governance policies (access-preservation-exchange-protection-security) of data.

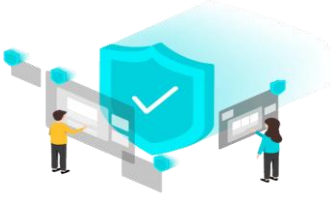
- Explains the most prominent challenges in the cybersecurity governance program

- Distinguish between “information security and protection” and “cyber security”

- Explains cyber security governance

Lesson1 : Current State and Desired State of Security

Desired & Current States



This section of the Dashboard encourages you to visualize what will need to change in order for you to reach your project Goal. What do you want your institution to look like as a result of your change project? How will your project impact your institution, college, department/unit, and individual faculty and students? Filling out these parts of the Dashboard will help you solidify your goal as a concrete vision and identify the gap between where you are and where you want to be.

Desired State

The Desired State represents specific changes in conditions rather than project goals or outcomes. It requires specific descriptions of things that will be different. For example, a goal might be that students in introductory STEM courses feel that they are part of a community. A Desired State would be the concrete things that
you will create with your project in this community, such as student cohorts in introductory STEM courses (institution level), welcoming study spaces within each STEM department (department level), and instructors of introductory STEM courses using collaborative group work (individual level).

Desired States can occur at different levels of the system. For the sake of simplicity, the Dashboard identifies five basic levels: External, Institution, College, Department/program, Individual. These basic levels are relevant to a wide variety of higher education institutions. There is nothing particularly special about these levels and they can be changed to match the levels that are relevant to your institution or change project. The important thing about explicitly showing a variety of levels is to understand the different elements of your particular system, and the important impacts of each level on your change project.

Many change initiatives fail because they focus on a single level and do not account for the barriers imposed by other levels nor build on the affordances provided by other levels.

Current State

Once you have identified the Desired State for your project, it is now time to identify the Current State. What is the actual condition of each area you listed in the Desired State? What do those things look like right now? Answering this question will help you identify the gap between your Current and Desired States.

Also, when thinking about the Current State, it is important to identify aspects of the system that you don't expect to change during your project (that is, the Current and Desired States will be the same), but that will likely support or impede reaching the desired state. For example, your Desired States might align with your institutional strategic plan. On the other hand, your institution could be in a difficult financial situation with budget deficits and, thus, have little appetite for new programs. You cannot expect to change these things, but they will certainly impact your project.

Failure to recognize the affordances offered by the current state can lead to missed opportunities. Failure to recognize the constraints imposed by the current state can lead to overoptimistic plans that do not reflect reality and are likely to fail.

Levels of the system Consider desired conditions and current conditions at these levels	Possible target issues What specific things exist (current) or do you want to exist (desired) at each level of the Dashboard? (adapted from Eckel & Kezar, 2003)
External Institution College Department/program Individuals	Structures: Curriculum (e.g., types of knowledge presented through the curriculum, organization of the curriculum) Pedagogy (e.g., use of particular teaching methods or new technologies) Student learning practices Student assessment practices Policies (key institutional policies such as those regarding scheduling) Budgets Non-financial resources (e.g., allocation of space or equipment towards particular projects) Departmental structures (e.g., organizational hierarchy, relevant centers) Institutional structures

	Decision-making structures (e.g., formal governance processes, ad hoc structures such as task forces) Cultures: Language used at the institution (i.e., to talk about itself, etc.) and types of conversations (e.g., topics, priorities) Stakeholder relationships Norms of interaction between individuals and groups

Tip: Structures vs. Cultures

There are two basic types of Desired States that can occur at each system level: structures and cultures.

Structures are more concrete things that can be directly measured or observed.

For example, you can directly observe whether an undergraduate lounge exists in a department where students are able to hang out, study, and interact with one-another.

Cultures can be more difficult to define. The literature contains careful definitions of culture (e.g., Burke, 1992; Burnes, 1996). However, for the purposes of the Dashboard, the careful definitions of culture are not particularly important. We simply think of culture as the more subtle aspects of the Desired and Current States that tend to be harder to directly measure or observe.

For example, a department may have a culture where students in introductory courses do not feel welcome to enter the undergraduate lounge. This is different from a structural issue, such as a policy that restricts the lounge to upper-level students. Such a culture could even conflict with a formal policy that invites and encourages introductory students to use the lounge.

When structures and cultures conflict, it is usually the culture that dominates (Groysberg, Lee, Price, & Cheng, 2018). Table 1 identifies common aspects of structures and cultures in academic institutions based on the work of Eckel & Kezar (2003). This can be a useful place to start and trigger ideas relevant to your project.

Current State of Usable Security
Security threats arising from the interaction between humans and computer systems

Cyberspace is not only the setting for business, it is also an important part of people's lives. With this increased exposure to threats comes increased expectations of safe and secure ICT. There are many different types of security measures to fight these threats, but this time we will be examining usable security; a type of security that protects against threats arising from interactions between humans and computer systems, and in particular threats to one’s privacy.

What is "Usable Security?"

In recent years, the word "cyber-attack" has become more and more commonplace in various forms of media. Whether the attackers' motive is fun, craving the limelight, social and political

claims, espionage, or just for monetary gain, these attacks put state institutions, private companies and individual users at risk on a daily basis.

Usable security refers to the practice of preventing threats to user security and privacy that arise from the interaction of humans (users) with computer systems. Unlike traditional system and network security, it focuses on users, analyzing their behavior, mental models and decision-making processes. It then uses these findings to provide feedback on computer system design, implementation, and operation, thereby improving user security and privacy. Our main focus is threats caused by online services. Rather than addressing software vulnerabilities or account hijacking, our usable security research focuses on security and privacy from the user's personal perspective. As introduced in the first article, according to "10 Major Security Threats 2020," compiled by the IPA (Information-Technology Promotion Agency, Japan), "Personal Information Theft from Services on the Internet" was the 12th biggest threat for individuals and the 8th biggest for organizations, so it is clearly a major security threat.

Privacy threats on online services from a usable security perspective

Let's take a look at the threat in detail. As an example, let’s think about logging in to a specific online service using a pair of a user ID and password.
This service is configured to display either the message "This User ID does not exist" if the User ID is input incorrectly, or "Incorrect password" if the password is input incorrectly. At first glance, there seems to be no issue with this, and there are likely to be plenty of people who have seen a lot of messages just like this.
But there are potential threats to privacy here.

What if we suppose that there is a person close to you with malicious intent?
Many online services use email addresses as user IDs. So, they might decide to try inputting the email addresses of people they know at random, such as those of their partner, their family, their friends, or their colleagues. As a result, they know that if the message "This User ID does not exist" displays, their target is not using the online service, but if "Incorrect password" displays, their target is using the service.
The main problem is that this attack can be performed by anyone who knows the email address in question.

Examples of privacy breaches that could be caused by error messages

Let's dig a little deeper into what kind of privacy breach could be caused by this attack.
So, let's use an online based career change service as an example. Based on the knowledge that the person in question holds an account, the attacker might guess that the account holder is planning to change jobs in the near future.
In the case of the financial loans service, they might guess that the person in question is currently experiencing financial difficulties.
Someone close to you who knows your email address might be able to breach your privacy by using these different condition-specific error messages for malicious purposes.

According to our online survey of over 600 people, over 82% of participants answered that there are certain sensitive services they would not want other people to know they have an

account with, such as services geared toward people of specific sexual orientations, adult content, and financial loan services. That means that for this 82%, the attack could be a breach of their privacy.
On the other hand, 25% of participants responded "Yes" to the question "Have you ever wanted to know if someone whose email address you know has an account on a particular online service?" This means that one in four people is a potential perpetrator.
In addition, our measurement study of around 100 types of online services revealed that almost all of the services displayed revealing error messages; thus, an attacker can deduce whether their target has an account on almost any of these services.
From these findings we can see that this issue is a practical threat from people close to us.

Examples of Secure Error Messages

Examples of Secure Error Messages

So, what measures are valid against the attack? Figure 4 shows examples of secure and insecure messages in each login-related function.

Function	Input	Insecure Messages	Secure Messages
Login	A registered user ID and an incorrect password	"Incorrect password"	"Incorrect user ID or password"
	An unregistered user ID and arbitrary password	"This user ID does not exist"	
Password Recovery	A registered user ID	"We have sent you a link to reset your password."	"If the email address you input exists in our database, we will send you a link to reset your password."
	Unregistered user ID	"This is not a registered email address."	
Account Creation	Registered user ID	"This user ID has already been registered."	"We have sent an account creation link to the input email address."

Function	Input	Insecure Messages	Secure Messages
	Unregistered user ID	"Account created successfully."	

Figure 4: Examples of Secure Error Messages

NTT's Usable Security Initiatives

NTT has been conducting research on usable security in order to design systems that encourage users' secure behavior as part of efforts to understand user security and privacy awareness and behavior on systems and services; a core part of the field of cyber-security. NTT Secure Platform Laboratories, which have conducted research into usable security as introduced here, have made the public aware of security threats and notified various stakeholders of countermeasures.
Specifically, we worked with IPA (Information-technology Promotion Agency, Japan) and JPCERT (Japan Computer Emergency Response Team Coordination Center) to notify potentially affected service providers of the threat and countermeasures, and also discussed with OWASP (the Open Web Application Security Project), an international open-source community for web security, to revise its web-security guidelines.

Looking Ahead

In recent years, as ICT and other societal systems have become more advanced, security-related decisions and actions required on the part of users are becoming increasingly complex. While everyone should be able to equally reap the benefits of ICT, there is a concern that this situation will leave some users behind. For example, it is now more difficult to understand the risks and take appropriate action when a browser displays a security warning.
At NTT, we aim to create an ICT society in the truest sense of the word, receptive to all kinds of people. To achieve this, our goal is to create security technology that absolutely everyone can understand, select, and use accordingly. Usable security will no doubt be a major theme in achieving this. One of NTT's strengths is that we develop full-stack (covering a wide range of fields; from infrastructure construction to applications) and full life-cycle (covering the entire life-cycle, from consulting through to maintenance and operations) services.

Humans are the central element in the relationship between humans, computer systems and ICT, and our relationship with computer systems and ICT is unlikely to change in future. However, it is thought that as ICT develops and becomes more complex, human awareness will be unable to keep up, and we will continue to see people exploiting this gap to launch cyber-attacks.

No matter how ICT evolves in future, NTT will continue to work with users to improve their awareness of ICT while also continuing to improve system designs such that users are enabled to make better decisions and use ICT safely and with confidence.

Reference

1. (1)"Usable Security" (Business Communication 2020 Vol. 57 No. 4)

2. (2)Ayako Akiyama Hasegawa, Takuya Watanabe, Eitaro Shioji, and Mitsuaki Akiyama, I know what you did last login: inconsistent messages tell existence of a target's account. ACSAC 2019.

What is a desired state for security?

A defined value, list, or rule (specification) that a) states or b) allows the computation of the state that the organization desires in order to reduce information security risk. Desired state specifications are generally statements of policy.

What is the desired state?

Desired State

The Desired State represents specific changes in conditions rather than project goals or outcomes. It requires specific descriptions of things that will be different. For example, a goal might be that students in introductory STEM courses feel that they are part of a community.

Lesson2 : Business Case and Value Realization

Business Value Realisation

Business value realisation is about achieving and demonstrating the actual business value resulting from a deployment of a new or improved product, solution or service. Projects and programmes that implement new capabilities often involve significant organisation changes, requiring a shift of mindset and significant investments by the organisation.

A key success factor of these transformations is the ability to measure the adoption of the new capabilities, products or solutions by the organisation and its customers. A poor adoption will result in the benefits and value not being realised. The business value realisation process therefore aims at measuring and maximising adoption and success of business transformation over time.

Figure 5.5.1 *Business value realization process*

The business value realization process relies on early stage work relating to the creation of a business benefits plan linked to the requested business case:

- **Business objectives** must be clearly identified and measurable (number of users, revenue contribution, savings, etc.)
- **Targets** must be associated to a timeline (deployment +3 months, +6 months, etc.) to provide a timeframe for the Business Value Realization
- **Conditions of success and failure** must be described in order to facilitate an assessment at the end of the business value realization period
- **Roles and responsibilities** to measure the business value realization must be attributed to identified resources.

There are four types of tasks associated with the business value realization process:

- **Business and customer feedback**: Capturing the comments and improvement suggestions of the business or customers, undertaking a lessons-learned exercise and feeding the demand process with improvements suggestions where appropriate
- **Post deployment communication**: In coordination with the service delivery and service owners, prepare and communicate to the target audience in a timely manner in order to promote the new capability or solution
- **Metrics measurement**: Periodically measure, in a consistent way, the success factor metrics defined in the business case
- **Incentive programs**: Create incentive programs and strategy to promote the new capability or solution to the organization or the customers (retirement of previous capability or service, etc.).

For sequential developments, some of the business benefits may be achieved before the rollout happens, for example in the pilot, although in most cases they materialize after the rollout.

For incremental developments however, the business value realization must be measured from the first increment.

Figure 5.5.2 *Sequential and incremental business value realization*

The business value realization process runs for a period set within the business case. At the end of the period, an assessment has to be made as to whether the transformation is successful, has reached some success and must improve, or is a failure.

In the case of a failure, where the business benefits are not realized as expected or realized too slowly, a root cause analysis should be conducted to support decision making on initiating possible corrective actions. The most common causes of failure include the following reasons:

- Lack of business readiness to use the new capabilities or solutions
- Organizations not incentivized to change
- Misalignment between business requirements and development delivery

- Divergences (priorities changed over time, original business case no longer valid, etc.).

If the initiative is only partially successful, improvement requests can be raised and fed back into the demand process.

If the business benefits are realized as expected, it is good practice to communicate this success to all relevant stakeholders.

It is also good practice for the benefits to be continually managed and assessed throughout the whole investment lifecycle, which includes incremental updates and amendments to any product or service.

What is Value Realization in SaaS and Why Does It Matter?

Value realization can make the difference between a customer who unsubscribes and a customer who becomes a brand advocate.

If you want to build a loyal customer base and nurture product growth, your focus should be spent on making users realize the value of your product as soon as possible—which might be trickier than you think.

So, let's talk about value realization and what you can do to improve it.

Summary of value realization in SaaS

- Value realization is when a customer experiences and recognizes the value of your product or service.
- Value expectation is when a customer has an "AHA moment" and thinks your product can bring the results they need. While value realization happens when the customer experiences value that exceeds those expectations.
- Value realization is key for product growth. As it allows you to convert free trial users into paying customers, it unlocks upsell opportunities and drives long-term customer retention.
- There are four metrics you can use to measure value realization:

1. Time to value (TTV)
2. Time to live
3. Return on investment (ROI)
4. Net promoter score (NPS)

- The value realization process has five stages:

1. Definition. Where you need to determine the meaning of your customers' success by creating user personas.
2. Delivery. Which involves the implementation of your product through in-app onboarding and self-service support.
3. Realization. When the customer starts getting results from your product and getting hyped through gamification.
4. Validation. When you have to keep providing actual business value throughout the journey through secondary onboarding and account expansions.
5. Optimization. It involves adapting your product to your customer's ever-changing expectations through in-app surveys and review gathering, making it timeless.

What is value realization?

Value realization is when a customer experiences and recognizes the value of your product or service. This can be achieved by aligning your output with the customer's unique strategic or personal objectives.

Value expectation vs. value realization

Although "value realization" and "value expectation" are closely related, they're different.

Value expectation is when a customer has an "AHA moment" and thinks your product can bring the results they need and then continues their journey with that expectation in mind.

Value realization is a later stage, and it happens when the customer experiences the value they were expecting face-to-face. It's the moment a customer has finally reached the activation stage.

Why is value realization important?

If you think value realization isn't worth paying attention to, you're missing out.

Ensuring that your customers find real value in your product is essential for multiple reasons:

Convert users into customers

If your SaaS offers a demo or a free trial, value realization can be the decisive moment when a user decides to convert into a paying customer.

The reason is simple. Most people will only pay for a product when they recognize the benefits of your product and experience the promised value directly.

Unlock upsell and cross-sell opportunities

After realizing the value of your product, customers are now convinced that it's worth investing in your brand. Making them more likely to accept upsells, upgrade, and buy additional services.

Drive long-term retention and loyalty

If you ensure that your customers are experiencing value throughout their journey (and not just during the free trial), you'll retain them and maximize customer lifetime value (LTV).

Not only that, but if you exceed their expectations, they'll eventually become brand advocates and share your product through word-of-mouth. Slowly cultivating customer loyalty.

Important value realization metrics to track

Now that you know the importance of value realization, you might wonder how to track it.

And while you can't read your user's minds, there are some key performance indicators that can give you an idea of what's going on:

Time to Value

As the name indicates, time to value (TTV) refers to the time it takes for a user to realize the expected value of your product.

If you want free trial users to convert into paying customers and reduce any churn risk, you want this metric to be as short as possible.

How to decrease time to value?

To reduce time to value, you can show a personalized empty state.

An empty state is what users see when they sign-up, and all they see is a blank dashboard, which puts barriers to value realization and hurts time to value.

However, when you replace the white space with personalized messages, templates, guides, and onboarding checklists, you can help users get a head start when they sign up and accelerate their journey.

Userpilot replaces the empty space with checklists that drive users to value realization.

Time to live

Time to live is the time it takes for a customer to implement your solution. In short, it measures how long the value delivery lasts (as you'll learn later), so you can shorten it.

Return on investment

Return on investment (ROI) is the most famous KPI. It measures how much income you get from your investment.

Since most businesses use ROI as their primary metric for success, you can use it to measure your customer's success with your product and make them realize its value easier.

Net promoter score

Net promoter score (NPS) shows how willing customers are to recommend your product to others by comparing the number of promoters and detractors.

If NPS scores are high, it means customers are realizing your value since they are willing to advise others to use your product.

What are the stages of the value realization process?

If you want to improve time-to-value and make sure that more users realize the value of your product, then you need to pay attention to the five stages of the value realization framework, which include:

1. Definition
2. Delivery
3. Realization
4. Validation
5. Optimization

So let's go over each stage while sharing some practices you can implement to optimize each stage.

1. Value definition

For value realization to happen, there must be an alignment between outcomes and expectations.

For this reason, the definition of value you communicate with customers is indispensable during this process. This way, your sales and marketing teams can set up the right expectations that will lead to value realization as customers start using your product.

Here's what you can do to create a clear definition of value:

Know your target audience and define what value means to them

Before communicating value to prospects, you must determine what's valuable for your user personas in the first place.

For this, you can create a user persona that goes deep into what your customers find valuable, such as getting their job done quickly and effectively, saving time, achieving business objectives, alleviating pains, etc. And you can only create a detailed persona through direct customer research such as interviews, surveys, chats, sales recordings, etc.

For example, you can quickly identify what's valuable for a product manager when looking at the example below, as it clearly shows its pain points, JTBDs, and goals that you can satisfy with your product.

2. Value delivery

Value delivery is about implementing the solution so both the customer and your team can get ready for success. It can involve installations, integrating software, high-touch guidance, and a lot of support throughout the process.

The goal here is to get through this process with as little investment of resources as possible. And here are some tactics you can apply to accomplish it:

Onboard users and provide in-app guidance

User onboarding is essential for customer success and basically covers the whole value delivery process.

Making the onboarding process as smooth and pleasant as possible is a big task, but you can start with implementing in-app guidance when your users first sign-up.

Think of interactive walkthroughs and tooltips that appear on the screen just at the right time before the user starts wondering how to use a specific feature.

Communicates interactive walkthrough created with User pilot.

Offer ongoing customer support and education with a resource center

Customer education is part of value delivery. But what if a user faces an obstacle and needs answers fast?

Users don’t enjoy waiting in line to get support, and we’re sure your customer service agents are not looking forward to repeatedly responding to the same questions.

As a win-win solution, create and organize self-help resources in-app. Include diverse content formats such as articles, video tutorials, and webinars that caters to everyone’s learning style.

When users know they can find answers in a few clicks, delivery will happen quicker and with less friction.

Provide in-app support with a knowledge base. Create one code-free with Userpilot.

3. Value realization

After everything has been implemented and your customers start executing their tasks using your product, it’s up to your product and customer to make value realization happen.

Whether it happens or not depends on the expectations you set at the beginning, if your product works as intended, and if you educate your customers properly so they can get real-life results with it. So what can you do to improve at this stage?

Here’s one tactic:

Celebrate customer wins

With UX gamification and emotional design, you can add badges, points, and levels for a more fun product experience.

Celebrating milestones not only reduces the friction to adopt features but also encourages them to feel good whenever they accomplish a task—making them more likely to recognize your product's value.

For example, here's how Calendly celebrates when you schedule your meeting:

How Calendly celebrates your first meeting.

4. Value validation

Although the value realization stage is important, value validation is the stage that brings ROI.

So after the customer has recognized the value of your product, don't sleep on it! You must ensure they'll keep receiving the same level of value throughout the customer journey and achieve their goal.

Here's what you can do about it:

Introduce users to more advanced features

As said earlier, your job doesn't stop at value realization. At the validation stage, you must engage users with secondary onboarding so they can finally adopt your product.

For this, provide value to the user repeatedly by introducing secondary features relevant to their use case.

Think of triggered tooltips, secondary checklists, or webinars to encourage users to try new features, just like this one:

Highlight secondary features to users with tooltips.

Drive account expansion through upsells and cross-sells

To experience the full value of your product, users have to upgrade their plan and buy upsells at this stage.

But it doesn't mean you should try to upsell something at every touchpoint. Instead, prompt users to upgrade their plan only when you're sure they will benefit.

Are your users constantly reaching the limits of their plans? Or doing a task the hard way when they could technically automate it with a premium feature?

Then ask them to upgrade with a personalized message.

For example, see how Loom teases you to upgrade when you reach the 5-minute recording limit on their freemium plan (which indicates that you'd benefit from unlimited recording).

5. Value optimization

Industries and technologies change rapidly, and so do your customer expectations.

At the value optimization stage, you must safeguard your acquired customers by ensuring that your value is timeless and evergreen.

Here are two key practices that will help you optimize the value of your product constantly:

Check-in with customers and collect feedback

At the optimization stage, you need to collect to understand how your customers feel about your brand and do your best to keep providing value.

You can automate customer feedback and trigger in-app surveys at different touchpoints to measure how your customers feel across the customer's journey and find opportunities for improvement.

There are different types of customer satisfaction surveys you can use such as CES (customer effort score), CSAT, NPS, and so on.

But it doesn't stop there. To make sure your customers feel heard and realize the value of your brand, you must close the feedback loop by acting on it. For example, implementing a highly-requested feature, solving a common bug, integrating your product with other apps, etc.

Gather qualifying evidence of value from your customers

To get evidence of your product's value to your customers, you can ask for reviews on 3rd-party review platforms, referrals, and testimonials to get social proof and understand what makes your product valuable.

For example, you can ask users to leave a testimonial after they've reached a specific milestone. Or you can also do some social listening and find people actively sharing your product with their network, then reach out to them to thank them and ask them to write a G2 review.

Speaking of which, you can even check review sites like G2 or Capterra and see how many users are actively recommending your product without you knowing—maybe there are some gold nuggets you haven't found.

Send a personalized modal to ask for reviews. Create modals code-free with User pilot.

Wrapping up

Although it seems very subjective, you can foster value realization when following the right practices.

Some of these practices can be easily implemented using a customer success tool like User pilot. So why not book a demo to see how you can enhance your success process without coding?

Lesson3 : Information Security Governance Metrics

Information security governance metrics

"A few well-chosen metrics can be a huge help in monitoring controls and measuring their effectiveness"
Clint Kreitner, SANS

Summary

It is not necessarily obvious how to measure information security governance. This paper describes potential metrics for measuring and improving information security governance. We are not suggesting that all of these metrics are necessary or appropriate for any organization, rather that management should consider the suggestions and then select 'a few good metrics' to use as part of the overall corporate governance framework.

Introduction In its free booklet "Information security governance: guidance for boards of directors and executive management" (2 nd edition), the IT Governance Institute (ITGI) describes information security governance in terms of the following key elements:

1) Desired outcomes of information security governance such as strategic alignment of information security with business strategy, risk management, resource management, performance measurement and value delivery;

2) Knowledge and protection of information assets - information and the knowledge based on it have increasingly become recognized as business-critical assets without which most organizations would simply cease to function. Knowledge is a business enabler, requiring organizations to provide adequate protection for this vital resource;

3) Benefits of information security governance such as increased share value, increased assurance by bringing information security under management control, better compliance and protection against liabilities; and

4) Process integration - integration of management assurance processes regarding security to improve overall security and operational efficiencies.

We'll use these four elements to derive more than four types of information security governance targets and metrics.

Information security governance metrics

If we accept that it is important to make our employees (and indeed those employed by third parties who work on our behalf) responsible for information security and especially if we intend to hold them personally accountable for their actions, so it makes sense for management to check how effective this process is and, where necessary, make adjustments to improve the governance of information security.

notice Bored information security awareness Information security governance metrics

1. Desired outcome metrics

Clarity of expectations

If we are going to measure the organization against some desired outcomes, the requirements should be made clear. Some might for example claim that information security roles and responsibilities must be "fully documented" if fulfilling such roles and responsibilities is desirable

but this is difficult if not impossible to achieve in practice. Job descriptions are inevitably quite generic and are not meant to define absolutely everything that employees are meant to do. Just like the laws of the land, information security policies, standards, procedures and guidelines also have to be interpreted to some extent depending on the particular circumstances. However, it is generally accepted good practice to document key information security roles and responsibilities,

policies, standards etc. This leads to the first group of metrics around the extent to which the requirements are defined and their suitability.

The organization's information security policy manual is an excellent place to start since (hopefully!) it defines a number of roles and responsibilities and allocates them to the applicable departments, teams/functions or individual employees. It is feasible to work systematically through the policy manual, drawing up a roles and responsibilities matrix along the following entirely absent (0%). Significant gaps corresponding to extreme low values would naturally suggest improvement opportunities.

The level of detail in this process is optional. It might be sensible to start, for instance, at the level of whole sections of the policy manual, or to work down particular columns of the matrix (e.g. just within IT). The experience gained by this initial run should make a more detailed assessment slightly easier to stomach.

Fulfillment of expectations

A second group of metrics reflects the need to assess compliance with or fulfillment of the defined roles and responsibilities. "Complete compliance" is an idealistic if naïve goal since limited noncompliance may be acceptable and even desirable under some circumstances, provided this is in the organization's best interests. This target is itself a policy matter that applies across all policies etc. It tends to be determined more by the organization's culture than by written edicts notice Bored information security awareness Information security governance metrics from management but, that said, management does set the tone from the top. The target seems likely to evolve as the measurement process matures – no bad thing.

Assuming that people have been told what they should or should not be doing in relation to information security, the next problem is to figure out how well they comply in practice. The key here is to focus on non-compliance since, for the most part, people tend to comply.

The 'number of non-compliance incidents in the previous period' seems relatively simple but ignores the importance of each incident. An alternative approach might be for someone to assign each non-compliance incident a 'score' (e.g. 0 meaning trivial or insignificant to 5 meaning extremely serious leading to dismissal or legal action) and present both the number of incidents and the mean score. Once the metrics bed down, management may well push back on the scoring process so it is probably worthwhile making the scoring process as open and well defined as possible, perhaps using examples of incidents at each level. You will of course need access to the source information about non-compliance incidents, ideally by close cooperation with HR and other management functions.

Be aware of the iceberg problem: you are very unlikely to find out about all non-compliances, primarily those that result in significant incidents and are clearly visible. There will always be a larger hidden body of non-compliances, but the hope is that they are insignificant so really don't matter to the organization.

2. Knowledge and protection of information asset metrics
Potential metrics in this category are described in the metrics discussion papers provided every month as part of the awareness program. There is a huge array of things that could be measured but it is far more difficult to pick out ‘a few good metrics.
A key metric that strikes a chord with some is based on the old “Days since a lost time accident” display boards common outside factories in the 1970s and 80s. The modern-day equivalent is “Days since a significant security incident”, typically displayed on the corporate intranet. Clicking on the headline number pulls up details on the breakdown of incidents by type, significance and/or business unit/department. The lowest level of detail may include brief descriptions of actual incidents, ideally accompanied by explanations of the controls that were fixed or improved to prevent recurrence.
3. Benefits of information security governance metrics
Here we seek to measure the financial control elements of governance as they apply to information security management. Information security raises legitimate management questions such as:
• How much is ‘enough’ information security? Are we investing too much or too little in managing our information security risks (and by the way, do we even track all the costs)?
• Are our information security investments being applied wisely, achieving both efficiency and effectiveness?
Financial controls are commonly measured so the metric ideas in this section are also just brief suggestions:
• Matching expenditure to budget, accounting for any under or over-spend;
• Annual expenditure on information security, expressed as a simple value (with caveats around the distributed nature of information security controls), a proportion of income or of some other
major expense (e.g. proportion of the IT budget), or a trend;
• Matching risk and reward, achieved by measuring the recovery of procurement or development and implementation costs for information security controls through reduced impacts and risks (i.e. increased assurance and confidence). Business cases for significant security control investments should contain metrics.
Notice Bored information security awareness Information security governance metrics
4. Information security process integration metrics
It may seem counterintuitive but “the inverse of the number of people employed in information security management” is potentially a metric for this governance goal – the idea being that most information security activities should ideally be performed by people working in other corporate functions. Many organizations that are mature enough to understand and adopt the “information
security” rather than “IT security” approach take the line that information security is a distributed
function, spread throughout the organization, albeit one led/directed by a specialist advisory function (“Information Security Management”) which requires a certain number of competent and experienced workers in order to be effective. As information security knowledge and skills

permeate the organization, there is potentially less and less need for a large core team of

dedicated information security managers in a centralized function, but conversely someone needs to maintain the policies, compliance activities, awareness programs and so forth on behalf of the entire organization.

A more pragmatic metric, therefore, might measure the proportion of information security man-days expended within versus without the Information Security Management department. This is not an easy metric to measure since accounting for information security management man-days outside the ISM function requires the cooperation of all departments doing ISM work.

5. Confidence metrics

A rather different style of metric involves surveying managers, for example:

How confident are you our information security governance meet the organization's needs?

Please mark the following percentage scale at the appropriate point, in your opinion.

0% 50% 100%

Not at all. Not quite enough | Just about enough Absolutely!

It is simple to measure percentage values from each response and calculate the mean score (indicating the perceived level of confidence) and variance (showing the range of opinions). Provided sufficient survey forms are completed and measured, the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials, as well as worthwhile ideas for improvement. The mere fact that people are being asked their opinions in this manner itself supports greater awareness of, if not interest in, information security governance.

Management reporting the numbers themselves are generally less important than what they mean or imply about the organization's information security governance. It is worthwhile analyzing and explaining the numbers – for instance, a written management report and executive summary with key recommendations for governance improvements, backed up with appendices containing the actual numbers. Consider repeating the measurements periodically (e.g. every year or two) to assess progress towards your governance objectives. Consider also preparing an interim 'status report' a Comments e.g. what led you to this score? Are you aware of information security governance failures or issues, or conversely what makes you think we are world-class?

Notice Bored information security awareness Information security governance metrics few months before the full presentation to senior management, giving middle managers and staff an opportunity to address the worst metrics before it's too late.

Conclusion The metrics and reporting methods noted in this paper have hopefully stimulated you to derive creative and useful measures for your own situation. Do not neglect the value of having someone present and discuss metrics and reporting with management, especially on a topic such as governance. The dialogue that ensues can be very effective at teasing out any underlying issues and concerns on both sides.

For more information Please visit Information Security's intranet Security Zone for more on information security governance. Additional awareness materials and advice on this topic are available from the CISO or Information Security Manager.

NIST SP 800-55 (Rev 1, July 2008) Performance Measurement Guide for Information Security

(new title - formerly Security Metrics Guide for Information Technology Systems) is “a guide to assist in the development, selection, and implementation of measures be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs.” Take a look also at SP 800-80 (DRAFT, May 2006) Guide for Developing Performance Metrics for Information Security. This is a more useful than the original SP 800-55 but still rather over the top for most organizations (it is intended for large US government departments subject to FISMA).
Andrew Jaquith’s book Security Metrics is a pragmatic guide and the classic 1998 paper by Hauser
and Katz “Metrics: You Are What You Measure is also highly recommended.

2. Knowledge and protection of information asset metrics
Potential metrics in this category are described in the metrics discussion papers provided every month as part of the awareness program. There is a huge array of things that could be measured but it is far more difficult to pick out ‘a few good metrics.
A key metric that strikes a chord with some is based on the old “Days since a lost time accident” display boards common outside factories in the 1970s and 80s. The modern-day equivalent is “Days since a significant security incident”, typically displayed on the corporate intranet. Clicking on the headline number pulls up details on the breakdown of incidents by type, significance and/or business unit/department. The lowest level of detail may include brief descriptions of actual incidents, ideally accompanied by explanations of the controls that were fixed or improved to prevent recurrence.
3. Benefits of information security governance metrics
Here we seek to measure the financial control elements of governance as they apply to information security management. Information security raises legitimate management questions such as:
• How much is ‘enough’ information security? Are we investing too much or too little in managing our information security risks (and by the way, do we even track all the costs)?
• Are our information security investments being applied wisely, achieving both efficiency and effectiveness?
Financial controls are commonly measured so the metric ideas in this section are also just brief suggestions:
• Matching expenditure to budget, accounting for any under or over-spend;
• Annual expenditure on information security, expressed as a simple value (with caveats around the distributed nature of information security controls), a proportion of income or of some other
major expense (e.g. proportion of the IT budget), or a trend;
• Matching risk and reward, achieved by measuring the recovery of procurement or development and implementation costs for information security controls through reduced

impacts and risks (i.e. increased assurance and confidence). Business cases for significant security control investments should contain metrics.
Notice Bored information security awareness Information security governance metrics
4. Information security process integration metrics
It may seem counterintuitive but “the inverse of the number of people employed in information security management” is potentially a metric for this governance goal – the idea being that most information security activities should ideally be performed by people working in other corporate functions. Many organizations that are mature enough to understand and adopt the “information
security” rather than “IT security” approach take the line that information security is a distributed
function, spread throughout the organization, albeit one led/directed by a specialist advisory function (“Information Security Management”) which requires a certain number of competent and experienced workers in order to be effective. As information security knowledge and skills permeate the organization, there is potentially less and less need for a large core team of dedicated information security managers in a centralized function, but conversely someone needs to maintain the policies, compliance activities, awareness programs and so forth on behalf of the entire organization.
A more pragmatic metric, therefore, might measure the proportion of information security man-days expended within versus without the Information Security Management department. This is not an easy metric to measure since accounting for information security management man-days outside the ISM function requires the cooperation of all departments doing ISM work.
5. Confidence metrics
A rather different style of metric involves surveying managers, for example:
How confident are you our information security governance meet the organization’s needs?
Please mark the following percentage scale at the appropriate point, in your opinion.
0% 50% 100%
Not at all. Not quite enough | Just about enough Absolutely!
It is simple to measure percentage values from each response and calculate the mean score (indicating the perceived level of confidence) and variance (showing the range of opinions). Provided sufficient survey forms are completed and measured, the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials, as well as worthwhile ideas for improvement. The mere fact that people are being asked their opinions in this manner itself supports greater awareness of, if not interest in, information security governance.
Management reporting the numbers themselves are generally less important than what they mean or imply about the organization’s information security governance. It is worthwhile analyzing and explaining the numbers – for instance, a written management report and executive summary with key recommendations for governance improvements, backed up with appendices containing the actual numbers. Consider repeating the measurements periodically (e.g. every year or two) to assess progress towards your governance objectives. Consider also preparing an interim ‘status report’ a Comments e.g. what led you to this score? Are you aware of information security governance failures or issues, or conversely what makes you think we are world-class?
Notice Bored information security awareness Information security governance metrics

few months before the full presentation to senior management, giving middle managers and staff an opportunity to address the worst metrics before it's too late.

Conclusion The metrics and reporting methods noted in this paper have hopefully stimulated you to derive creative and useful measures for your own situation. Do not neglect the value of having someone present and discuss metrics and reporting with management, especially on a topic such as governance. The dialogue that ensues can be very effective at teasing out any underlying issues and concerns on both sides.

For more information Please visit Information Security's intranet Security Zone for more on information security governance. Additional awareness materials and advice on this topic are available from the CISO or Information Security Manager.

NIST SP 800-55 (Rev 1, July 2008) Performance Measurement Guide for Information Security (new title - formerly Security Metrics Guide for Information Technology Systems) is "a guide to assist in the development, selection, and implementation of measures be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs." Take a look also at SP 800-80 (DRAFT, May 2006) Guide for Developing Performance Metrics for Information Security. This is a more useful than the original SP 800-55 but still rather over the top for most organizations (it is intended for large US government departments subject to FISMA).

Andrew Jaquith's book Security Metrics is a pragmatic guide and the classic 1998 paper by Hauser

and Katz "Metrics: You Are What You Measure is also highly recommended.

.....

Unit Six : Case Study

At the end of the unit, the trainee will be able to:

- Explains the steps that the organization must follow in the information security governance program.
- Mention the most prominent challenges in the information security governance program.
- Identify the steps that contribute to the information security governance program.- Mention the components of the cyber security strateg

معهد التدريب الإداري العالي
Management Training Higher Institute

Lesson1 : Case Study: Implementing Information Security Governance

Information Security Governance: A Case Study of the Strategic Context of Information Security

Completed Research Paper

Terrence Tan
The University of Melbourne
Australia
t.e.tan80@gmail.com

Sean B Maynard
The University of Melbourne
Australia
seanbm@unimelb.edu.au

Atif Ahmad
The University of Melbourne
Australia
atif@unimelb.edu.au

Tobias Ruighaver
The University of Melbourne
Australia
tobias@ruighaver.net

Abstract

Security governance influences the quality of strategic decision-making towards ensuring that investments in security are not wasted. Security governance involves a range of activities including adjusting organisational structures, designating roles and responsibilities, allocating resources, managing risks, measuring results, and gauging the adequacy of security audits and reviews. We draw on a case study to identify three security issues in an organisation around strategic context. These are (1) limited diversity in decision-making; (2) lack of guidance in corporate-level mission statements to security decision-makers; (3) a bottom-up approach to security strategic context development. We further argue that instead of an approach that is based on risk and controls, organisations should address objectives and strategies through developing depth in their security strategic context.

Keywords: Security Culture, Decentralized Decision Making, Security Strategic Context, Business Security Strategies, Information Security Governance.

Introduction

In today's dynamic information security environment, organisations, even those where security controls and state-of-the-art technical security are implemented, are struggling to develop strategies to address the increases in security attacks (Park et al. 2012; Ahmad et al. 2014). Most of these organisations base their information security initiatives on the ISO 27000 series of standards, but are still struggling to cope with increases in threats and vulnerabilities.

While ISO 27000 and related standards introduce a lifecycle model for security management, the emphasis is still on the controls needed in information security. Little information is given about security objectives, potential implementation strategies for these objectives or about the key aspect of accountability arrangements. Also, other than risk assessment, there are few suggestions on how organisations should develop security objectives and strategies as part of their security governance processes. While this emphasis on controls works well in a reasonably static security environment, in today's ever changing security environment, organisations need to encourage and promote innovation in their approach to security management, moving beyond what is prescribed in the current standards (Ruighaver, 2008).

Corporate security governance focuses on "setting the responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly" (ITGI, 2009). Understanding how certain characteristics of security governance, at the enterprise level and below, influence the quality of strategic decision-making in information security is an essential step to ensuring that investments in security are not wasted. The ability to make well-informed decisions about the many important components of

governing for enterprise security, such as adjusting organisational structures, designating roles and responsibilities, allocating resources, managing risks, measuring results, and gauging the adequacy of security audits and reviews is crucial. Efforts to improve decision making in these areas is mostly focusses on corporate security governance (Tan et al., 2003; Carcary et al. 2016).

Unfortunately, this emphasis fails to effectively address the need to ensure that decision making at the lower levels of the enterprise is improved, i.e. the need to establish security governance at the business unit level and below. From this point, we will refer to this level of governance as "enterprise-wide security governance", or "security governance", while referring to "corporate security governance" when discussing issues related to board level governance issues. Hence, while there is evidence of reasonable efforts to develop corporate security governance guidelines and frameworks, there is little known about enterprise-wide security governance. In particular, about how organisations develop their security strategic context, how they decide on security objectives and strategies and how they use these to develop their policies and security infrastructures, and the part accountability plays in ensuring a streamlined and effective process. Subsequently, this paper addresses the following research question: *How does information security governance influence the depth of strategic context in enterprise information security?*

This case paper reports on one of several case studies of IT services organisations conducted in the area of enterprise-wide security governance. Cases were selected on the basis that they were actively undertaking security efforts, were relatively stable, were large enough so that governance was an issue, and had high reliance on their information systems. This particular case examines the information security function in a business unit of a privately owned, Small-to-Medium Enterprise (SME), with security governance decentralized to the IT group. This paper will discuss several of the major issues related to 'enterprise wide security governance' that we discovered in our in-depth case study as well as how these issues affect the security strategic context for this particular organisation.

Background

Modern organisations are facing a more complex threat environment. Even though information security professionals are aware of, and defend these complex attacks, there are still many high profile security incidents. Several experts state that a cause of these incidents is that security personnel are too narrowly focused (Wright et al, 2006). For example, in 2013, Vudu, a streaming service in California, had customer names, addresses and encrypted passwords stolen. Whilst digitally their systems were secure, with firewalls and such installed and working correctly, the data was physically stolen when thieves broke into their headquarters and purloined multiple hard drives (Kumparak 2013).

Organisations however, are slowly realising the importance of preparedness for these new attacks (Tan et al., 2010), by conducting strategic planning around security. Despite this increased emphasis, many organisations tend to aim for compliance of standards, hoping that that will be enough to protect them from security incidents (Shedden et al., 2010). This approach, however, indicates severe shortcomings in the strategic planning of the organisation and points to organisations requiring better governance around information security.

Governance

For organisations operating in complex and highly dynamic environments, the importance of effective governance (how decisions are made) and management (what decisions are made) cannot be understated (Peppard, 2007). The traditional view of corporate governance sees the responsibility falling to the board and senior executives, with the focus being on the financial well-being of the organisation (Konczal, 2011). This is however, not sustainable due to the highly dynamic business environment. Organisations must devolve governance activities down to all levels of the organisation, and even to outside entities (ITGI, 2009). From a security perspective, this means that responsibilities for governance fall to all employees of the organisation, and to external stakeholders such as auditors (Pultorak, 2005; Bergeron 2015). This devolves responsibility to the lower levels of the organisation as well as to the senior executives.

However, having responsibility and feeling responsible are two different issues. With responsibility comes accountability. Therefore, an important aspect of any effective governance is how the organisation handles accountability for decisions in security management (Borck, 2000). Lack of even the simplest accountability processes is a fairly common deficiency in security governance, such as

simple feedback loops in which decisions on security are discussed with higher levels of management, and the focus is on how the decisions are made (Burke, 2005; Straub et al., 2008).

Importantly, the delegation of responsibility to those at the lower levels does not preclude the need for executive level management support. Knapp et al. (2006) found that top management support for information security is a significant predictor of the direction and success of an organisation's information security. Therefore, whereas operational responsibility and accountability primarily lies with those at the middle management and lower levels, top/executive management still has clear responsibility to visibly demonstrate their support and a high prioritization of information security.

Security governance should be viewed as a larger management issue that revolves around understanding how decisions are made and making consistently good decisions in a complex and dynamic environment characterized by distributed decision making (Koh et al., 2005; Ribbers et al., 2002). Decision makers should be given the right information and the right guidance to be able to make quick, decisive and accurate decisions in real time (Dhillon & Torkzadeh, 2006).

Summary

From this discussion it is clear that current security practice and compliance with standards is not enough to protect organisations. Much research has been completed in the information security domain in areas such as policy (Alshaikh et al. 2015; Sommestad et al., 2014; Ifinedo, 2014; Ruighaver et. al., 2010; Maynard & Ruighaver, 2006), risk management (Webb et al., 2014; 2016) security culture (Okere et al., 2012; Lim et. al., 2010; Da Veiga & Eloff, 2010; Ruighaver et al., 2007), and incident response (Ahmad et al., 2015; Ahmad et al., 2012; Shedden et al., 2010). Despite this research, organisations are still suffering from incidents.

Also, there is evidence that organisations are happy with complying with standards and are doing "what everyone else is doing." Given that this is not working, they now must answer the question of "what else can we do?"

Enterprise-wide Security Governance

For this case study, it is important to make a clear distinction between corporate security governance and enterprise-wide security governance as introduced in this paper. From the previous section, it can be appreciated that corporate security governance can be understood as governance at a board or executive level (Brown & Nasuti, 2005) with its main aims to ensure that security governance is promoted and controlled enterprise-wide. Its focus is ensuring controls and reducing or avoiding risks. Enterprise-wide security governance as discussed in this paper refers to the controls, arrangements, processes or structures that are exercised over the organisation's security. Specifically, these controls, arrangements, processes and structures are focused on improving decision making through providing decision makers at all levels with the right information and the right guidance, at the right time, to make good decisions about security (Gantz, 2008).

The field of Information Security is a complex and critical component to an organisation's success. A strategic approach to Information Security aims to transform the IT security function from a set of ad-hoc activities with an emphasis on technology, to a coordinated approach of principles, behaviours, and adaptive solutions that map to business requirements (Whitman & Mattord 2013). As such, those responsible are not just senior management but also middle management and others involved with the implementation of security strategies. As the practices and methodologies behind Corporate Governance and IT Governance are somewhat reliable and time tested and seen to be successful in dealing with various organisational issues, it is plausible to suggest that improving Security Governance throughout the enterprise may be the key to improving the level of security in organisations.

Frameworks

The focus of this study is to improve information security decision-making through enterprise-wide security governance. The execution of security strategies and timely decisions around these strategies occurs at the operations level of the organisation. Subsequently this study is interested in how people that implement security perform decision making, with or without organisational guidance. Tan and Ruighaver (2005a) point out however, that for decision makers to make quality decisions, guidance must be effectively communicated to them in the form of the organisation's security strategic context,

which is contained within artefacts such as security objectives, strategies, tactics and mission statements.

These artefacts are crucial as they outline for decision makers the intent or motivation behind what the organisation is trying to achieve with security and the desired end state. For instance, soldiers in battle, given a mission, need to understand their commander's intent. In the military context, the commander's intent is understood as 'a concise expression of the purpose of the operation and the desired end state that serves as the initial impetus for the planning process' (Shattuck, 2000: 66). With this understanding, only then can soldiers be proactive, innovative, flexible and aggressive in their decisions to achieve mission success. With these artefacts effectively developed, it is then vital that they be communicated enterprise-wide, as far down to even the lowest levels. Consequently, this will encourage and allow better, more concise and effective decisions to be made.

Trying to quantify what a good security strategic context is and how one can improve it is a complex problem that cannot be adequately answered in a single study. Importantly, however, Peterson et al. (2000) and Ribbers et al. (2002) argue that good security strategic context "requires active participation and a shared understanding among stakeholders if they are to coordinate activities and adapt to changing circumstances". By developing security strategic context exclusively at the top management level, it is likely to result in a lack of diversity across the security strategic context. Hence, good security strategic context needs to be developed by different people/committees at different levels of the organisation, similar to the development of IT strategic context (Weill & Woodham, 2002).

In this case study we specifically focus on a key aspect of security governance, strategic context (see Tan & Ruighaver 2004). Notably, strategic context is also identified as a key component of successful IT governance (Weill & Ross, 2004). We also adopt a strategic context model (Broadbent, 2002) which we expand so that we look at both the depth and coverage of the security strategic context. Depth focuses on the extensiveness of the organisation's strategic context and encompasses 5 domains: Security Objectives (mission statements), Security infrastructure, Security architecture, Security application needs, and Security investment and prioritization. Coverage focuses on the comprehensiveness of the organisational strategic context and includes the security areas defined by Tan and Ruighaver (2005b): Network Security, Systems and Data Security, Physical Security, Personnel Security, Operations Security, and Miscellaneous Security aspects (Eg. a focus on eCrime, and incident handling).

A matrix of the depth and coverage dimensions helps to determine the strategic context in which an organisation is operating in. In the analysis of the case data we use this matrix to assess the scope of the organisation's security strategic context (see Appendix 1 for the analysis).

The Case Study

This case study reports on an Australian organisation: MicroComps Limited (MCL). MCL is a commercially successful organisation who are market leaders in supply chain management and business-to-business e-Commerce solutions. Privately owned, the management structure within MCL consists of a management group that reports to a private ownership board (see Figure 1).

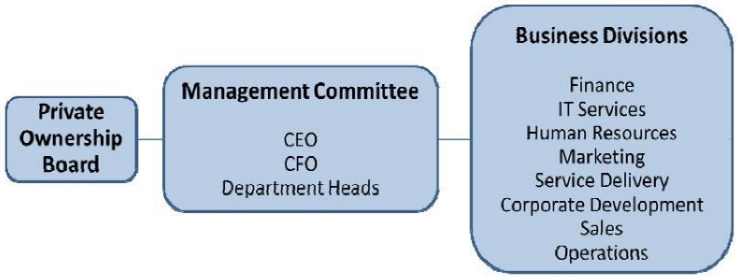


Figure 1: MCL's Organisational Structure

This board has the final say on the operations of the organisation. In the early days of operating, the management group consisted wholly of the ownership board, with the CEO of the organisation being the primary owner. Over time, and as the organisation grew, it became necessary to set up a

معهد التدريب الإداري العالي
Management Training Higher Institute

management committee that answers to the board. At this time, the ownership board of MCL took on a supervisory role. The CEO, the CFO and senior leadership from each department within the organisation together comprise the management committee.

Department heads report to the ownership board through the CEO and CFO. With regards to the day-to-day operations of the business, the ownership board has a hands-off approach. However, the board still maintains and is actively involved with influencing the strategic direction of the organisation. From a governance perspective, the decision-making structures at MCL delegates decision making to the division level, allowing each head to formulate and develop their own strategy, as long as it is within the organisation's strategic context (strategic plan). Thus, the responsibility for all security in the organisation falls to the IT Manager, who is responsible for the security governance in the organisation.

Dealing largely with the transaction, processing and ordering systems of other businesses, MCL's role is to receive files (such as orders and payments), translate them into an understandable, common language, then deliver the order (as many businesses operate their own backend systems and generally not one backend system can talk with every other backend system). A simple way of thinking about this process is to visualise what is involved, think the Postal system: receiving, sorting (translating), storage and delivery.

The participants targeted in this case were specifically selected due to their likely involvement in the development of security strategies, decision making and in providing input to security decisions. As MCL is a SME, the three selected participants were the only personnel within MCL that have security responsibilities. The participants were the IT Manager (ITMngr), the Systems Administrator (SysMngr) and the Network Administrator (NetMngr). These personnel were intimately involved with the implementation of security controls and highly relied upon to make decisions about security and to react to security incidents. Of the three, one respondent held the most senior position in the IT and information security area while the others reported directly to them. In addition to gaining data form the participants the researchers sought documents (such as policies, security strategy etc) and were able to observe members of the organisation across a 1-week period with respect to security. The main reason for this was to triangulate data for the research.

From a security perspective, none of the participants had any exposure or formal training on security standards because security had never been something pushed strongly by the organisation. Therefore, inconsistencies are evident from the participants' views on the importance of security to the operations of MCL, with some participants stating that security was not important apart from being able to cover vulnerabilities, whilst others stated that security was extremely important to the ongoing running of the organisation. In MCL security was set up and managed by ITMngr and SysMngr, and has a technical focus.

Overall, ITMngr's responsibilities are to provide a functional and robust infrastructure, equipment and framework for the organisation to enable employees to do their jobs and to allow customers to receive their services. ITMngr, like the rest of the organisation is incredibly customer focused, and only on very few occasions (and when probed) did he discuss the importance of security and threats to his organisations, rather talking about the importance of the customer. Security initiatives at MCL have been 'organically' grown and ad hoc. Without formal standards or guidance from the organisation on how and what to do about security, ITMngr had to formulate his own strategies and his objectives (security strategic context), based largely on the wider objectives of availability and reliability of systems given to him by the organisation.

ITMngr acknowledges that security to him (and the organisation) is not so much a priority but a necessity and that his approach to security in many ways is reactive. He addresses security through the implementation of technical controls and adjusts these in response to security threats and incidents.

NetMngr, is new to the job and has had security delegated to him by ITMngr. Having only just joined the organisation, NetMngr is representative of the problem that could arise from the organisation's lack of corporate governance and focus on security. The consequence of a lack of organisational guidance on security on the participants is clearly demonstrated in NetMngr. Not only does he have little experience with security, he does little regarding security and views security to be less important compared to other business functions. Similarly, he is unaware of what goes on concerning security in general at MCL. Without formal standards, guidelines, documents, mandates or guidance from the corporate governance to inform NetMngr of his responsibilities relating to security, like ITMngr, he is left to his own devices.

Fortunately for NetMngr, although the organisation has not provided much, if any, formal guidance, NetMngr receives sufficient on-the-job guidance from ITMngr, within the team. This ad hoc training, is analogous with someone working as an apprentice through a hands-on, learn from experience, on-the-job mentoring process. NetMngr looks after the local network. Accordingly, he monitors the network performance and services, making sure that everything is working as it should and that all resources are running at optimum levels.

MCL has its data centre and all its data, servers and backups outsourced and located off-site. Responsibility for that data centre and all external business centres lies with SysMngr. Coming from a strong technical background and with previous experience in technological support, administrative roles and limited security, SysMngr possesses a great deal of technical knowledge. Like the other participants, SysMngr too does not receive much, if any, formal guidance from the organisation on what to do, what to secure or how to prioritise security. Like NetMngr, SysMngr gets direction from ITMngr, supplemented by his past experiences.

However, relying on past experiences as a guide for future actions and decisions can also be dangerous. In the first place, most people do not recognise the underlying reasons for their mistakes or failures. In the second place, the lessons of experience may be inapplicable to the new problems. This is where effective security governance to understand how decisions are made and to improve decision making is very important. Good decisions must be evaluated against future events, while experience belongs to the past (Koontz & Weihrich, 2008).

Case Analysis and Discussion

As stated earlier, the analysis of the case data produced a matrix to assess the scope of the organisation's security strategic context (see Appendix 1 for the analysis). From the analysis three main themes were identified. These are discussed in this section.

Diversity in Decision Making is Limited

At MCL, security does not follow any single security standard, rather, security initiatives were improvised and ad hoc, and almost all decisions about the security strategic context have been made by the IT Manager. Little or no formal guidance on decision-making rights have ever been explicitly expressed or delegated by the organisation. According to participants, the organisation is not concerned about what decisions are made, nor about how participants went about their jobs, as long as they achieved the availability and reliability of systems and networks. Whilst SYSMngr and NETMngr had unwritten guidelines around security there were no formal policies provided.

At MCL, security governance is mostly decentralised to the IT group by default. Almost all decisions and input into decisions, from almost every level of security strategic context is developed and decided by the IT Manager with input coming from his team. Unfortunately, inputs are only from his team, thus creating an environment of limited social participation and limited diversity in decision making.

These settings then create the situation where participants rely heavily on their own ingenuity, particularly that of the IT Manager to drive security initiatives and to develop security strategies. Interestingly, all these actions and initiatives are undertaken without the knowledge and understanding that they are actually developing security strategic context.

Unfortunately, with the lack of formal guidance from executive levels and from other functional areas, any discussions, dialogues or consultations, including feedback loops, are internalised within the IT department. The input given and received is very insular within the IT department and is limited to the experiences of the team members (mainly in systems and networks) and does not adequately cover the wider range of security concerns and imperatives. For instance, areas such as physical and environmental security and personnel security are lacking in strategies and attention.

Depth in the technical aspects of security (in network security, systems security and data security) is excellent. All levels of depth in the security strategic context matrix (see appendix 1) are adequately addressed. This implies that participants at MCL would have good diversity in decision making for these specific areas.

Our analysis of MCL's security strategic context identifies that the objectives, strategies and certain controls developed, employed and actioned at MCL, differ from those recommended by security standards such as the ISO 27002 Standard. Whereas the ISO 27002 Standard recommends strategies such as:

- Control access to critical data and/or servers to ensure availability and reliability
- Monitor access to directories
- Real time protection
- Up-to-date anti-virus software

MCL has customized these recommendations and developed strategies such as:

- Maintain a flexible approach to security. Adjust and move in response to things
- Automatically delete all .exe files on mail server
- Alerts to be sent when any inconsistencies are noticed
- Maintain tight and dedicated roles for every server, machine and process so that redundancy can be achieved (double up on everything)
- Training and mentoring.

Although performed on an ad hoc basis and not through any formal instruction or direction, these strategies are specific, customised and flexible to the needs and functions of MCL allowing the organisation to view security not as an individual quantified function, but rather as being integrated into what they do by necessity. In this sense, as security objectives clarify focus and provide a frame of reference for every important aspect of security activity, these objectives and strategies become appropriate as high-level statements that would inform the organisation about how security will be used to create business value.

Little Guidance Provided By Corporate Level Security Mission Statements

The initial setup of security at MCL was ad hoc, fragmented and unplanned with the executive management paying scant attention to security, and lacking a holistic perspective of their security governance posture. Security is not regarded as being an issue of executive management, until something goes wrong. However, even without acceptable levels of formal guidance and assistance, participants were delegated the responsibility for security and security decision-making, hence a culture of accountability was evident. Consequently, the participants, with the understanding that they are held accountable, are in a sense, driven to develop their own security strategic context based on their own experiences and always looking to the IT Manager for guidance, which as explained earlier has its own pitfalls.

Further, the participants at MCL were held responsible not only for what decisions were made but also on how they made those decisions. For instance, did they seek advice? Participants at MCL were not held accountable for compliance to security or of a specific implementation of security. Instead, they were held accountable for the effectiveness of security. This is particularly so for ITMngr. As the IT Manager, this was his responsibility and he is fully aware that, 'if you want to lose your job, lose data'. As such, ITMngr takes full ownership of security, and in a sense, controls security in an almost authoritarian fashion. Given their own inadequacies, the other participants accommodate this dictatorship.

The participants knew they were held accountable by the company's director for their role in information security. Although there was really only one accountability loop between the IT Manager and the CEO with active discussions on the state of the company's security and on how to improve it, a secondary feedback and accountability loop existed between the IT Manager and the other participants. These accountability and feedback loops, although existent, are about what decisions are being made and not about how the decisions are made. Essentially, we believe that the participants were actually afraid of losing their jobs, which can be considered more as a 'motivational influence' than an accountability aspect.

Without appropriate formal guidance, this scenario could potentially explode and result in many 'catastrophic' decisions being made by the participants. The serious question to consider is whether the organisation can ultimately hold the participants responsible if something goes wrong bearing in mind that the organisation, due to the lack of formal guidance and attention to security, has never told the participants as to how to make good decisions? Or for that matter, what good decisions are.

Security Strategic Context Development From The Bottom Up

Many organisations see Security Governance as a small part of Corporate Governance. While IT Governance has become a recognized focus area in larger organisations, these organisations often do not give Security Governance the same attention. Hence, organisations still need to realize that just like IT, the field of Information Security is a complex and critical component to their organisation's success. As such, those responsible for security are not just senior management but also middle management and others involved with the implementation of security strategies (those at the operations level of the organisation), and they will similarly need a governance framework for making informed decisions about Information Security.

At MCL, culturally, the focus of security is on the physical systems and network security, an environment conducive to bottom-up participation. Participants did not have a framework to work with and their experiences were limited. However, whether due to the 'motivational' fear of potentially losing their jobs, or due to their positive disposition towards security, unbeknown to them, the participants have developed their own security strategic context as they were forced to come up with their own objectives and controls.

Their experiences being limited to mainly the technical areas drove them to a narrow focus. Thus, frivolity about certain risks and controls exist with certain areas having a heavier focus than others do. Areas such as personnel security and physical and environmental security are missing in MCL's security strategy context. However, other areas such as network and systems security are focused on heavily. This is indicative of a highly IT-driven, porous security with the security focus and initiatives purely on the technical aspects.

At MCL, due to limited corporate governance support and understanding of the importance of security, the participants regarded security as totally unplanned and ad hoc. This attitude was inherent across all levels in the organisation, be it at the executive or middle management, business unit or lower levels. Coupled with the second imperative of an emphasis on executive controls, the significant lack of strategic direction imparted by the organisation has led to a mediocre effort in its security strategy development. We submit that this then results in deficiencies in their depth of security strategic context.

Conclusions

Previous research in Information Security Management highlighted the need for security governance as a means to guide decision-making at the level of middle-management and below. This paper presents a revelatory case study that identifies three significant shortcomings in the security governance of SMEs. These are limited diversity in decision-making, lack of guidance in corporate-level mission statements to security decision-makers, and a bottom-up approach to security strategic context development. From a theoretical perspective, these shortcomings explain how poor security governance influences strategic context in enterprise information security.

Most current information and academic papers on security governance at the enterprise wide level promote a centralized decision making model based on, in our experience, an ineffective and old-fashioned risk management approach to security. The old-fashioned centralized approach is relatively simple to manage: It needs almost no security governance enterprise wide (business unit or operations levels) as most decisions are made at the corporate level.

In the current dynamic security environment, this centralized approach does have a major drawback. Centralized decision-making will reduce the flexibility and adaptability of an organisation's security posture, making it difficult for the organisation to respond quickly/timely to changes in its security environment.

Further, the lack of input from people at the operations level in the predominantly centralized security-planning ethos has stifled innovation in security. This study suggests that organisations should empower decision makers at the middle and lower management levels and improve the timeliness and effectiveness of security decisions by ensuring that all the governance practices identified in the security governance framework are effectively addressed.

Additionally, this study is about how organisations can transform their approach to security. Instead of an approach that is based on risk and controls, the researchers advocate for organisations to address objectives and strategies through developing depth in their security strategic context. With this alternative approach, it is expected that security policies and guidelines developed will enable

decision makers to understand the rationale for controls, rather than simply performing the function of security controls. Further, unlike current studies that focus primarily on oversight, our emphasis is to understand how decisions are made and not focus on what decisions are made. Therefore, to understand how, one needs to know the purpose and rationale for the decision.

More significantly, with MCL's security philosophy, the same employee(s) or committee(s) that decide on security infrastructure and applications also decide on objectives and security strategies. Hence the rationale is that there is no need to communicate those objectives and strategies to the rest of the organisation. While accountability arrangements exist, these are still mainly focused on what decisions are made and not on how decisions are made, which is what governance is about.

To create a dynamic, flexible and agile security posture, a more decentralized approach to security decision-making is needed. A decentralized approach will need good security governance at all levels. To attain this, it is important that the necessary enterprise-wide security governance structures and processes are developed and put in place. This ensures that adequate security objectives and security strategies are developed and effectively communicated to the decision makers. This, in itself, is expected to promote innovation and effective security.

References

Ahmad, A., Maynard, S.B., Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses", *International Journal of Information Management* 35(6), 717-723.

Ahmad, A, Maynard, SB, Park, S 2014. "Information Security Strategies: Towards an Organisational Multi-Strategy perspective", *Journal of Intelligent Manufacturing*, 25 (2), pp 357-370.

Ahmad, A., Hadjkiss, J., Ruighaver, A.B. 2012. "Incident Response Teams - Challenges in Supporting the Organisational Security Function". *Computers & Security*. 31(5). 643–652.

Alshaikh, M., Maynard, S, B., Ahmad, A. 2015. "Information Security Policy: A Management Practice Perspective". *The 26th Australasian Conference on Information Systems*, Adelaide, Australia.

Bergeron, F., Croteau, A. M., Uwizeyemungu, S., & Raymond, L. 2015. "IT Governance Theories and the Reality of SMEs: Bridging the Gap". In *48th Hawaii International Conference on Systems Sciences (HICSS)*, pp. 4544-4553. IEEE.

Borck, J 2000. "Advice for a Secure Enterprise: Implement the Basics and See That Everyone Uses Them", *InfoWorld*, 22(46), p. 90.

Broadbent, M. 2002. "CIO Futures – Lead With Effective Governance", *ICA 36th Conference*, Singapore.

Brown, W & Nasuti, F 2005, "Sarbanes-Oxley and Enterprise Security: IT Governance – What it takes to Get the Job Done", *The EDP Audit, Control and Security*, 33(2), pp. 1-20.

Burke, J 2005. "Closing the Accountability Gap for Public Universities: Putting Academic Departments in the Performance Loop", *Planning for Higher Education*, 34(1), pp. 19-28.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. 2016. "A Framework for Information Security Governance and Management". *IT Professional*, 18(2), 22-30.

Da Veiga, A., & Eloff, J. H. 2010. "A framework and assessment instrument for information security culture". *Computers & Security*, 29(2), 196-207.

Dhillon, G & Torkzadeh, G 2006. "Value-Focused Assessment of Information Systems Security in Organizations", *Information Systems Journal*, 16(3), pp. 293-314.

Gantz, S 2008. "Redefining Governance to Improve Security", in *CSI 2008 - Security Reconsidered.*

Ifinedo, P. 2014. "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition". *Information & Management*, 51(1), 69-79.

Information Technology Governance Institute (ITGI). 2009. "An Executive View of IT Governance," (*www.itgi.org*; accessed Feb 25, 2011)

Knapp, K, Marshall, T, Rainer, R & Ford, F 2006. "Information Security: Management's Effect on Culture and Policy", *Information Management & Computer Security*, 14(1), pp. 24-36.

Koh, K, Ruighaver, A, Maynard, S & Ahmad, A 2005. "Security Governance: Its Impact on Security Culture", in *Proceedings of 3rd Australian Information Security Management Conference*, Perth, Australia, pp. 1-13.

Kumparak, G. 2013. "Vudu Headquarters Robbed, Hard Drives with Private Customer Data Stolen, http://techcrunch.com/2013/04/09/vudu-headquarters-robbed-hard-drives-with-private-customer-data-stolen/, accessed 19/1/17.

Konczal, E 2011. "Corporate Governance 2.5 A New Focus", viewed 16 August 2011, <http://www.corporate-eye.com/blog/2011/07/corporate-governance-2-5/>.

Lim, J., Ahmad, A., Chang, S., and Maynard, S.B. 2010. "Embedding Information Security Culture Emerging Concerns and Challenges". *PACIS 2010 Proceedings*. Paper 43, pages 463-474.

Maynard S. and Ruighaver, A.B. 2006. "What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality". *5th Annual Security Conference*, Las Vegas, Nevada USA, 19-20 April 2006.

Okere, I., Van Niekerk, J., & Carroll, M. 2012. "Assessing information security culture: A critical analysis of current approaches". In *Information Security for South Africa (ISSA)*, 2012 (pp. 1-8). IEEE.

Park, S; Ruighaver, A.B.; Maynard, S.B. and Ahmad, A. 2012. "Towards Understanding Deterrence: Information Security Managers' Perspective". *Proceedings of the International Conference on IT Convergence and Security 2011*, Suwon, Korea, p 21-37.

Peterson, RR., O'Callaghan, R. & Ribbers, PMA. 2000. "Information Technology Governance by Design: Investigating Hybrid Configurations and Integration Mechanisms", *Proceedings of the 20th International Conference on Information Systems*, Australia.

Peppard, J. 2007. "The Conundrum of IT Management", *European Journal of Information Systems*, vol. 16, no. 4, pp. 336-45.

Pultorak, D. 2005. "IT Governance: Toward a Unified Framework Linked to and Driven by Corporate Governance". *CIO Wisdom II*, Prentice Hall.

Ribbers, PMA, Peterson, RR & Marylin, MP 2002. "Designing Information Technology governance processes: Diagnosing contemporary practices and competing theories", *Proceedings of the 35th Hawaii International Conference on System Sciences*, IEEE Computer Society, pp. 1-12.

Ruighaver, A.B., Maynard, S.B. and Chang, S. 2007. "Organisational security culture: Extending the end-user perspective". *Computers & Security*, 26(1), February 2007, Pages 56-62,

Ruighaver, A.B., Maynard, S.B., Warren, M 2010. "Ethical Decision Making: Improving the Quality of Acceptable Use Policies", Computers and Security, 29:7, October 2010, Pages 731-736.

Ruighaver, A.B. 2008. "Organisational Security Requirements: An agile approach to Ubiquitous Information Security". In *Proceedings of the 6th Australian Security management Conference,* Australia (2008)

Shattuck, LG 2000. "Communicating Intent and Imparting Presence", *Military Review*, March-April, p. 66.

Shedden, P., Ruighaver, A.B., Ahmad, A., 2010. "Risk Management Standards – The Perception of Ease of Use". *Journal of Information Systems Security*. 6(3).

Shedden, P., Ahmad A., Ruighaver, A.B., 2010. Organisational Learning and Incident Response: Promoting Effective Learning Through the Incident Response Process. *Proceedings of the 8th Information Security Management Conference* (pp.139-150), Perth, Australia: Edith Cowan University. 30 Nov – 2nd Dec, 2010.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. 2014. "Variables influencing information security policy compliance: a systematic review of quantitative studies". *Information Management & Computer Security*, 22(1), 42-75.

Straub, D, Goodman, S & Baskerville, R 2008. "Information Security: Policy, Processes and Practices", *Advances in Management Information Systems*, M E Sharpe Inc, Armonk, NY.

Tan, T.C.C., Ruighaver, A.B., Ahmad, A. 2003. "Incident Handling: Where the Need for Planning is often not Recognised". In *Proceedings of the Ist Australian Computer Network, Information & Forensics Conference*, Australia

Tan, T.C.C., Ruighaver, A.B. 2005a. "Understanding the Scope of Strategic Context in Security Governance", In: *Proceedings of the 2005 IT Governance Int. Conf*, New Zealand

Tan, T.C.C., Ruighaver, A.B. 2005b. "A Framework for investigating the development of Security Strategic Context in Organisations", In *Proceedings of the 6th Aust Information Warfare & Security Conference: Protecting the Australian Homeland*. pp. 216-226. Australia

Tan, T.C.C., Ruighaver, A.B. 2004. "Developing a framework for understanding Security Governance". In *Proceedings of the 2nd Australian Information Security Management Conference*, Australia (2004)

Tan, T., Ruighaver, A.B., & Ahmad, A. 2010. "Information Security Governance: When Compliance Becomes more Important than Security". In *24th IFIP TC-11 International Information Security Conference*. Brisbane, Australia. pp. 55-67.

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G. 2016 "Foundations for an Intelligence-Driven Information Security Risk Management System", *Journal of Information Technology Theory and Application*, 17(3), pp25-51.

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management". *Computers & Security*. 44(1), July 2014, p 391-404.

Weill, P & Woodham, R. 2002. "Don't Just Lead, Govern: Implementing Effective IT Governance", *Massachusetts Institute of Technology*, Cambridge, Massachusetts (2002).

Weill, P., Ross, J.W. 2004. "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results", *Harvard Business School Press*.

Whitman, M. E., & Mattord, H. J. 2013. *Management of information security*. Nelson Education.

Wright, PD, Liberatore, MJ, Nydick, RL 2006. "A survey of operations research models and applications in Homeland Security", *Interfaces*, 36(6), Nov/Dec, pp.514-529.

Appendix 1: Detailed Analysis of the Breadth and Coverage of The Strategic Context

green and italicized text = activities performed by participants at MCL in accordance with what is suggested in the ISO 27002 Security Standard.
red and bolded text = activities performed by participants additional to those activities suggested in the ISO 27002 Security Standard.
black underlined text = activities proposed by the ISO Security Standard, but no evidence was found that would indicate MCL was performing these activities.

		Depth	
Coverage		Security Objectives	Security Strategies & Infrastructure
	Network Security	• *Ensure availability and reliability of network services (general access, authentication and access to information systems).* • **Compartmentalise and define roles.**	• *Control access to critical data and/or servers to ensure availability and reliability.* • *Manage incoming files.* • **Maintain a flexible approach. Adjust and move in response to events.** • **Lockdown of servers via tightening of roles.**
	Systems Security	• *Prevent unauthorized activities.* • *Detect unauthorized activities.* • **Compartmentalise and define roles.**	• Regular monitoring of sys and events. • Define a security policy outlining unauthorised activities. • Implement organisational wide use of company approved encryption. • *Provide means for authentication.* • **Maintain a flexible approach.** • **Adjust in response to things.** • **Ad hoc monitoring of network, processes**

			and systems. **• Informal control of access rights.** **• Lockdown servers, tighter roles.**
	Physical & Environ-mental Security	• Prevent damage and interference to business premises and information. • Prevent loss, damage or compromise of assets and interruption to business activities. **• Outsourced to third party.**	• Defined security perimeter erected. • Security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. • Computer and information equipment are secured to reduce unauthorised physical access.
	Personnel Security	• Reduce risks of human error, theft, fraud or misuse by employees. • Ensure users are aware of security threats & concerns. *• Minimise damage, monitor & learn from incidents (limited).*	• Ensure that incidents affecting security be reported. • Define and establish formal disciplinary processes. • Ensure that employees are aware of security threats. *• Address security responsibilities at the recruitment stage.*
	Communic-ations & Operations Security	• Define procedures for securing communications and operations facilities. *• Ensure correct & secure operation of information processing facilities.* *• Minimize risk of systems failure.* *• Maintain integrity & availability of info processing & communication.*	• Establish strategy for advanced planning and preparation to ensure availability. • Establish routine procedures for housekeeping. • Establish responsibilities & (informal) procedures for management on of all information processing facilities. **• Maintain a flexible approach. Adjust and move in response to things.** **• Ensure systems have redundancy in event of failure.**
	Data Security	*• Maintain appropriate protection of organisational assets.* *• Ensure that information assets receive an appropriate level of protection.*	• Identify areas of risk in processing cycle. • Define protection of company records. *• All major info assets should be accounted for and have an owner.* *• Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. This accountability ensures appropriate protection.* **• Maintain a flexible approach. Adjust and move in response to events.**
	Miscellan-eous Security	• Comply with legal requirements. • Ensure compliance of systems with security policies and standards. *• Business continuity management to counteract interruptions to business activities and to protect critical processes from the effects of major failures or disasters.*	• Ensure that the design, operation, use & management of systems be within statutory, regulatory and contractual requirements. • Ensure regular review of Information Systems security. *• Implement a business continuity management process to reduce disruption to an acceptable level.*

		Depth	
Coverage		Security Architecture	Security Application(s) Needed
	Network Security	• Evaluate policies for information dissemination & authorisation. • *Authentication mechanisms.* • *Control of user access to information.* • *Alerts sent when monitoring software flags anything.* • **Monitor unauthorised access.** • **Automatic deletion of .exe files on mail server.** • **Dedicated role for each server and machine.**	• *Encryption and certificates.* • *Monitor access to directories.* • *Firewalls.* • *Proxy servers.* • *Home grown monitoring software.* • *Up-to-date anti-virus software.* • **Controls to delete .exe files on mail server automatically.** • **SMS and Email alerts.** • **Informal policy determining role for every server/machine.**
	Systems Security	• Security and Acceptable use policies to be disseminated organisation wide. • Systems should be monitored to detect deviation from access control policy and record monitor able events to provide evidence in case of incidents. • *Identify & verify identity of users.* • **Monitor access to directories by unauthorised software/programs.** • **Home-grown monitoring but only of things that would disrupt services (predominantly software or programs, not users).** • **Alerts sent when monitoring software flags anything.**	• Monitoring software to monitor employee activity on system. • *Access Control Software (password managers & policies to ensure complex passwords).* • *Up-to-date anti-virus software.* • *Real time protection.* • *Monitor access files.* • **Monitoring software to monitor system and processing health.** • **SMS and email alerts.** • **Informal policy determining role for every server/machine.**
	Physical & Environ-mental Security	• Secure areas need to be protected by a defined security perimeter, with appropriate security barriers and entry controls. • Special controls may be required to protect against hazards or unauthorised access & to safeguard support facilities. • *Protection equipment to reduce the risk of unauthorised access to data and to protect against loss or damage.*	• Surveillance Technology. • *Access Control (door entry technology, proximity card access, photo identification, and biometrics).* • *Monitoring Software with reviewable access control logs.* • *Data centre provides redundant power supply, air conditioning, secure environment.*
	Personnel Security	• Any breach of security policies will cause an initiation of formal disciplinary action. • Users should be informed in security procedures and correct use of information processing facilities. • *Users made aware of their responsibilities at recruitment (security in job responsibilities, personnel screening and terms of employment).*	• Personnel security policies. • Disciplinary policies. • Accepted Use Policies. • Character Checks. • Maintaining personnel security files. • Security education & training. • Visitor Control. • **Regular emails sent out to employees about laptop security, updating antivirus definitions, etc.** • **Personal, hands on, 1 to 1 mentoring programs.**
	Communic-ations & Operations Security	• Develop appropriate operating instructions and incident response procedures. Disseminated organisation wide. • Segregation of duties established to reduce risk of negligence or misuse. • Users should be made aware of dangers of unauthorised/malicious software.	• Monitoring software to flag errors or procedural breeches. • Security education & training. • *All servers and systems have redundancy.* • *Secure backup facilities.* • **Hourly Online backups.**

		• *Routine checks on back-up strategy (take back-up copies of data & rehearse timely restoration, logging events and faults).* • **Routine checks to make sure all security updates are installed.**	
	Data Security	• Important records are identified. • Controls are allocated depending on nature of application and business impact of any corruption of data. • Delegate specific responsibilities for developing and implementing security controls. • *Responsibilities for the protection of individual assets is clearly defined.*	• *Disk Encryption.* • *Security Tokens and PINs.* • *Backups.* • *Data Masking.* • *Copy protection.* • *Single sign-on.* • **User groups set.** • **File management processes.** • **Informal policy on data security set.**
	Miscellan-eous Security	• Reviews performed against appropriate security policies & technical platforms. • Information systems should be audited for compliance with security implementation standards and legal requirements. • *Business continuity management process must be implemented to deal with disruption through a combination of preventative and recovery controls.*	• *Security audits and assessments (limited and ad hoc).* • *Backup strategies.* • *Monitoring strategies.*

A note on Security Investment & Prioritisation

As an SME, resource allocation for security initiatives is scarce and limited. MCL does not have an individually allocated budget for security. Security initiatives are drawn out of the IT Budget. Security is not prioritised but is seen as an aspect of things that need to be done. Suggestions for investments can be made any one of the members of the Managed Services Team as they are responsible for security. However, the decision is made by the IT Manager. Although in certain circumstances, the IT Manager brings these suggestions up to higher management, this is in no means an attempt to get verification. Rather it is more about communication and an effort to keep the executive levels of the organization involved in what is happening.

معهد التدريب الإداري العالي
Management Training Higher Institute

View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 7-19-2017

Information Security Governance: A Case Study of the Strategic Context of Information Security

Terrence Tan
The University of Melbourne, t.e.tan80@gmail.com

Sean Maynard
The University of Melbourne, seanbm@unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Tobias Ruighaver
The University of Melbourne, tobias@ruighaver.net

Follow this and additional works at: http://aisel.aisnet.org/pacis2017

Recommended Citation
Tan, Terrence; Maynard, Sean; Ahmad, Atif; and Ruighaver, Tobias, "Information Security Governance: A Case Study of the Strategic Context of Information Security" (2017). *PACIS 2017 Proceedings*. 43.
http://aisel.aisnet.org/pacis2017/43

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2017 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Lesson2 : Summary

Information security governance is similar to a blueprint for safeguarding valuable data in businesses and organizations. It outlines the rules, responsibilities, and processes required to keep information protected from cyber threats.

Understanding this framework enables companies to secure their information and uphold trust with customers and partners. Exploring the fundamentals of information security governance highlights its significance in today's digital world.

Let's get started!

Definition of Information Security Governance

Information security governance is about the framework of policies, procedures, and controls that organization's use to protect their information. It involves collaboration between security leaders, managers, executives, and employees to assess risks effectively. By having strong governance policies, organizations can evaluate risks and ensure information is secure. They also maintain integrity and control accessibility.

Through risk management and compliance, organizations can handle security issues and incidents promptly. Governance committees and boards oversee the security program.

For example, federal agencies like CISA focus on cybersecurity governance frameworks to help organizations manage security risks. Tools like Central eyes can help organizations streamline governance, move away from manual processes, and add value to managing security incidents.

Importance of Information Security Governance

Information security governance in an organization involves setting up policies, procedures, and controls to protect sensitive information.

This helps manage risks, threats, and incidents that could impact systems.

Information security governance focuses on risk assessment and compliance to meet regulatory requirements and industry standards.

Benefits of information security governance include enhancing business continuity and disaster recovery practices by identifying and managing risks.

By replacing manual processes with automated controls, organizations can improve resilience to security issues and incidents.

Challenges may arise, especially in compliance across federal agencies and in dealing with the complexities of state cybersecurity governance.

The involvement of executive teams and directors in developing governance policies can impact the overall strategy.

Leaders and managers need to navigate these challenges by building a strong information security programmer that offers immediate value and adapts to cybersecurity governance changes.

Key Components of Information Security Governance

Risk Management

Organizations can identify and assess risks in their information security governance framework by conducting a comprehensive risk assessment.

Information security leaders and managers evaluate risks and threats in the organization's technology infrastructure.

Involving the executive team, board of directors, and governance committee helps ensure alignment of governance policies with security issues.

Implementing controls such as manual processes or spreadsheets aids in monitoring and managing incidents.

Building a strong information security program with policies and procedures provides immediate value to the organization.

To mitigate cybersecurity risks and ensure compliance with regulations, organizations can implement strategies like state cybersecurity governance policies and federal agencies' guidelines.

Enhancing information accessibility and focusing on data integrity help organizations effectively manage risks and protect their information from threats.

Mitigating Cybersecurity Risks

Organizations can improve cybersecurity by:

- Having strong security governance policies.
- Implementing effective risk management strategies.
- Conducting thorough risk assessments.
- Involving the executive team in cybersecurity governance.
- Developing clear policies, procedures, and controls.
- Ensuring compliance with regulations like CISA.
- Building a comprehensive risk assessment framework.
- Aligning with state cybersecurity guidelines.
- Involving the board of directors and governance committee.
- Demonstrating leadership commitment to data integrity.

- Automating processes through a central platform for immediate value.

BOD 23-01 Compliance

Compliance with BOD 23-01 has a big impact on an organization's ability to reduce cybersecurity risks. It ensures that the right security policies and procedures are in place.

When the executive team takes an active role in governance committees, they lead the way for the information security program. This involvement helps in conducting a thorough risk assessment to find potential threats.

Implementing controls such as technology infrastructure and management processes enables organizations to handle these risks effectively.

BOD 23-01 Compliance also requires boards of directors to supervise cybersecurity governance, safeguarding information for authorized personnel only.

In cybersecurity governance at the state level, including federal bodies, maintaining information integrity and compliance is crucial. By actively participating in risk assessment and management, organizations can tackle security issues proactively, adding value to their overall security strategy.

Security Policies and Procedures

Effective security policies and procedures in organizations include:

- Risk assessment
- Governance policies
- Technology infrastructure
- Incident management strategies

A strong information security program, led by security leaders and the executive team, helps organizations mitigate risks. Compliance and audit processes involve controls, manual processes, and spreadsheets for risk assessment.

The governance committee and board of directors oversee security issues and make informed decisions. Tools like the Central eyes platform can help manage cybersecurity governance effectively.

Building a robust security governance framework enables organizations to address threats, incidents, and risks while safeguarding information integrity and accessibility. State cybersecurity governance for federal agencies and state cybersecurity guidelines enhance information security management within organizations.

Governance Policy Support

Organizations can support governance policies effectively by implementing a comprehensive risk assessment.

This helps in identifying and mitigating security risks.

Information security leaders and managers play a key role in this process.

They assess risks, threats, and compliance requirements to develop robust governance policies.

These policies should align with the organization's information security program.

Involving the executive team, board of directors, and governance committee is essential.

This ensures that security issues are promptly addressed.

Regularly reviewing and updating technology infrastructure and controls is crucial.

This helps in maintaining the integrity of the system and data accessibility.

Replacing manual processes and spreadsheets with automated tools like the Central eyes platform streamlines governance procedures.

It provides immediate value in managing security incidents.

Building a strong cybersecurity governance strategy is important.

This helps in proactively addressing security issues affecting federal agencies and state cybersecurity governance.

Compliance and Audit Processes

Compliance and audit processes in an organization help maintain effective information security governance. It's important for security leaders to establish policies and procedures to ensure compliance with regulations and audit requirements.

Regular risk assessments are conducted, both manually and automatically, to identify potential security issues. Audits then evaluate the effectiveness of these compliance measures.

The executive team, board of directors, and governance committee oversee the information security program. They ensure that controls are in place to protect information integrity.

Incidents are managed promptly, with learnings used to improve the overall strategy continuously. Technology infrastructure like the Central eyes platform is key in providing immediate value through comprehensive risk assessment and management.

These measures help organizations mitigate risks, threats, and vulnerabilities while building a strong cybersecurity governance framework meeting federal and state requirements.

Implementing Information Security Governance

Asset Visibility and Protection

Organizations need strong information security governance practices for asset visibility and protection.

By setting clear governance policies, security leaders can oversee technology security effectively.

Regular risk assessments and compliance checks help identify potential risks.

Implementing risk management strategies improves data security and protects assets.

To enhance protection, organizations need an information security program supported by executives and the board.

Automation tools like Central eyes platform can detect vulnerabilities and incidents.

Up-to-date security procedures strengthen system integrity.

Collaboration with cybersecurity committees and federal agencies enhances asset protection.

Improved Data Security

To improve data security in an organization, information security leaders can:

Develop and apply strong security governance policies.

Ensure alignment with relevant compliance standards and best practices.

Conduct risk assessments.

Establish clear governance policies.

Regularly engage with the executive team and board of directors to address emerging security issues.

Implement secure file transfer methods to maintain data integrity during transit, reducing the risk of breaches and unauthorized access.

Detect and respond to vulnerabilities promptly to uphold data security standards.

Identify potential weaknesses in the technology infrastructure to prevent security incidents.

Build a comprehensive risk management strategy to proactively mitigate risks affecting the information security program.

Safeguard against cybersecurity threats.

Implementing state cybersecurity governance, involving federal agencies and technology solutions like Central eyes Platform.

Provide immediate value in enhancing overall security controls

Replace outdated spreadsheets with automated tools for improved accessibility and integrity.

Vulnerability Detection and Response

When it comes to finding vulnerabilities in a system, organizations have different methods:

- Conduct regular risk assessments
- Implement security controls
- Monitor system logs for unusual activities
- Use technology tools to scan for weaknesses

Once vulnerabilities are found, organizations should act fast:

- Implement security patches
- Update system configurations
- Revise policies to reduce risks

Information security leaders, managers, and employees should work together:

- To follow security governance policies
- To prevent incidents that could harm the organization's technology

By creating a detailed risk management strategy, organizations can:

- Address security issues quickly and proactively
- Protect their systems and data

Cybersecurity governance, federal agencies, and board of directors are important:

- They oversee security controls
- Ensure the organization's security program is in line with governance directives

By centralizing security governance, organizations can:

- Simplify processes
- Eliminate manual tasks
- Provide instant value in addressing security threats

Secure Content Communications

Secure content communications within an organization involve several key components. They need to be carefully managed through information security governance. This includes:

- Having robust security policies
- Ensuring compliance with regulations

- Conducting regular risk assessments
- Having incident response procedures

Organizations need to empower their security leaders and managers. They should implement effective security governance policies. This ensures that technology infrastructure is secure. Additionally, employees are trained on secure communication protocols.

To ensure secure file transfer methods, organizations should implement:

- Encryption technologies
- Access controls
- Secure data storage practices

Security leaders can implement comprehensive risk assessments. This helps identify potential vulnerabilities affecting communication channels. By building a strong information governance program, organizations can protect sensitive information from external threats and insider risks.

Information security governance is essential for ensuring the integrity and confidentiality of communications within an organization. Having strong governance policies and controls in place allows organizations to effectively manage their technology infrastructure. It also helps respond to security incidents promptly. This approach is crucial for both federal agencies and state cybersecurity governance. It provides immediate value in protecting information and maintaining trust with stakeholders, including the board of directors and executive team.

Secure File Transfer Methods

When it comes to information security governance, organizations must consider several factors when choosing secure file transfer methods to protect data.

Firstly, governance policies must be in place to ensure that the chosen method aligns with the organization's security framework. Security leaders should conduct a risk assessment to identify potential risks and threats to the system.

Managers need to establish clear policies and procedures for secure file transfer, following regulations and standards like CISA. Additionally, investing in technology infrastructure supporting secure transmission and accessibility of information is crucial.

Manual processes or spreadsheets may pose security risks, highlighting the need for controls and automation in file transfer procedures.

Building a robust information security program involving the executive team and the board of directors in cybersecurity governance can help mitigate risks and prevent compromising data integrity.

Federal agencies and state cybersecurity governance bodies increasingly focus on secure file transfer methods to safeguard sensitive information.

Benefits of Information Security Governance

Compliance with Regulations

Organizations can ensure compliance with regulations in information security governance by:

- Implementing robust governance policies and procedures.
- Working closely with the executive team and board of directors to establish comprehensive risk assessment and management strategies.
- Regularly assessing risks, threats, and vulnerabilities within the technology infrastructure.
- Identifying and addressing potential security issues affecting the organization.
- Training managers and employees on policies and procedures to maintain information integrity and accessibility.
- Having mechanisms in place to address and rectify non-compliance incidents promptly.

It's also important to consider state cybersecurity governance requirements, such as those outlined by CISA, when building an information security program. By centralizing controls and moving away from manual processes and spreadsheets, organizations can achieve immediate value and demonstrate compliance with federal agencies and state cybersecurity governance initiatives.

Improved Business Continuity and Disaster Recovery

Businesses can improve their business continuity and disaster recovery plans by implementing strong information security governance. This involves:

- Establishing clear governance policies that outline roles and responsibilities within the organization.
- Equipping security leaders and managers to assess risks and threats effectively.
- Adopting a comprehensive risk assessment strategy to identify vulnerabilities in technology infrastructure.
- Developing robust incident response procedures.
- Ensuring compliance with regulations like CISA and state cybersecurity governance requirements to enhance data security and communication channels.
- Focusing on integrity and accessibility of information to mitigate security issues and achieve immediate value in business continuity and disaster recovery efforts.

This approach helps in building stronger security controls and aligning the organization's information governance with federal agencies and the board of directors' expectations.

Challenges in Implementing Information Security Governance

Ensuring Compliance Across Federal Networks

Federal agencies can make sure they follow rules and standards on their networks. They can do this by having strong information security policies. This means top leaders in the organization work together to create clear security rules. Leaders in information security need to check for risks that could harm the organization's technology. With a good cybersecurity plan, organizations can deal with risks before they cause problems.

There are some challenges in making sure federal networks meet the rules. Using manual methods like spreadsheets can take a lot of time and have mistakes. Technology tools like Central eyes Platform can help automate the process. These tools give managers a quick look at security problems and help them act fast. State cybersecurity rules are important for keeping federal networks safe and accessible.

Central eyes is a Security Governance Framework. It ensures organizations comply with regulations like BOD 23-01. The platform helps in mitigating cybersecurity risks and ensuring compliance. It does this through risk assessment, management, and incident response capabilities.

Central eyes supports governance policies, compliance, and audit processes. It does this by providing a comprehensive risk assessment. This builds a strong foundation for information security governance. It helps security leaders and managers to identify and address risks and threats. These affect the organization's technology infrastructure.

By automating manual processes and eliminating spreadsheets, Central eyes enhance governance efficiency. It offers immediate value to organizations. This enables them to establish controls, ensure system integrity, and enhance access to critical information.

With Central eyes, organizations can effectively manage security issues. They can align their information security program with regulations like CISA. This helps meet requirements set by federal agencies and state cybersecurity governance.

Key takeaways

Information security governance is all about guiding an organization's strategy for managing and protecting its information assets. This includes frameworks, policies, processes, and structures that help ensure information security aligns with goals and complies with regulations. It also involves managing risks effectively. To do this well, clear roles and responsibilities are essential.

Regular assessments and continuous improvement efforts are necessary to safeguard information and support business objectives.

Readynez offers a large portfolio of Security courses, providing you with all the learning and support you need to successfully prepare for a role as Chief Information Security Officer. All our Security courses, are also included in our unique Unlimited Security Training offer, where you can attend 60+ Security courses for just €249 per month, the most flexible and affordable way to get your Security Certifications

Please reach out to us with any questions or if you would like a chat about your opportunity with the Security Certifications and your journey towards becoming a CISO.

FAQ

What is information security governance?

Information security governance is the framework of policies, procedures, and processes that ensure an organization's information assets are adequately protected. It involves setting objectives, assigning responsibilities, and regularly monitoring and managing risks. For example, establishing access control measures to safeguard sensitive data.

Why is information security governance important?

Information security governance is crucial for protecting sensitive data, ensuring compliance with regulations, managing risks, and maintaining trust with stakeholders. Examples include setting policies and procedures, conducting regular audits, and implementing security controls to prevent data breaches.

What are the key components of information security governance?

Key components of information security governance include policies and procedures, risk management, compliance, and incident response. For example, creating and enforcing a strong password policy, conducting regular risk assessments, ensuring compliance with regulations, and having a robust incident response plan in place.

How can an organization implement effective information security governance?

An organization can implement effective information security governance by establishing clear policies and procedures, conducting regular risk assessments, providing ongoing training for employees, and monitoring compliance with regulations such as GDPR.

What are the common challenges faced in information security governance?

Common challenges faced in information security governance include lack of adequate resources, compliance issues, ineffective communication, and keeping up with evolving threats. Examples include limited budget for cybersecurity measures, difficulty in ensuring all employees adhere to security policies, and difficulties in staying compliant with industry regulations.