TryHackMe Walkthrough: Governance & Regulations

Introduction

Cyber security is a rapidly evolving landscape wherein malicious actors relentlessly endeavour to exploit vulnerabilities in highly-sensitive systems, often with the intent of causing severe damage, disruption, and stealing of sensitive corporate data. To combat this evolving threat, a comprehensive approach to **information security governance & regulation** is necessary. Such an approach requires establishing robust policies and guidelines and implementing rigorous monitoring and enforcement mechanisms to ensure compliance. By adopting a proactive and strategic stance towards cyber security, organisations can mitigate the risks posed by malicious actors and safeguard their sensitive systems against potentially catastrophic breaches.

Why Is It Important?

Important Terminologies

- **Governance**: Managing and directing an organisation or system to achieve its objectives and ensure compliance with laws, regulations, and standards.
- **Regulation**: A rule or law enforced by a governing body to ensure compliance and protect against harm.
- **Compliance**: The state of adhering to laws, regulations, and standards that apply to an organisation or system.

Information Security Governance

Information security governance represents an organisation's established structure, policies, methods, and guidelines designed to guarantee the privacy, reliability, and accessibility of its information assets. Given the escalating complexity of cyber threats, the significance of information security governance is continually growing. It is essential for risk management, safeguarding confidential data from unauthorised intrusion, and adhering to pertinent regulations. Information security governance falls under the

purview of top-tier management and includes the following processes:

- **Strategy**: Developing and implementing a comprehensive information security strategy that aligns with the organisation's overall business objectives.
- **Policies and procedures**: Preparing policies and procedures that govern the use and protection of information assets.
- **Risk management**: Conduct risk assessments to identify potential threats to the organisation's information assets and implement risk mitigation measures.
- **Performance measurement**: Establishing metrics and key performance indicators (KPIs) to measure the effectiveness of the information security governance program.
- **Compliance**: Ensuring compliance with relevant regulations and industry best practices.

Information Security Regulation

Governance and regulation are closely linked in the information security paradigm but have distinct meanings. Information security regulation refers to legal and regulatory frameworks that govern the use and protection of information assets. Regulations are designed to protect sensitive data from unauthorized access, theft, and misuse. Compliance with regulations is typically mandatory and enforced by government agencies or other regulatory bodies. Examples of information security regulations/standards include the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Personal Information Protection and Electronic Documents Act (PIPEDA), and many more.

Key Benefits

The following are the benefits of implementing governance and regulation:

- **More Robust Security Posture**: Implementing a comprehensive security governance program and complying with relevant regulations can help an organisation reduce the risk of security breaches and protect sensitive information from unauthorised access, theft, and misuse
- **Increased Stakeholder Confidence**: Effective security governance and regulation can enhance stakeholder trust by demonstrating that an organisation takes cyber security seriously and has implemented measures to protect sensitive data.
- **Regulatory Compliance**: Compliance with relevant regulations, such as GDPR, HIPAA, and PCI DSS, can help organisations avoid legal and financial penalties and reputational damage resulting from non-compliance.
- **Better alignment with business objectives**: Security governance frameworks can help organisations align their information security strategies with their overall business objectives and ensure that security measures are cost-effective and contribute to the organisation's success.
- **Informed decision-making**: Security governance programs can provide decision-makers with the knowledge they need to make sophisticated decisions about information security risks and ensure that security measures are implemented where they are most needed.
- **Competitive advantage**: Effective security governance and compliance with relevant regulations can provide a competitive advantage by demonstrating an organisation's commitment to protecting sensitive data and enhancing stakeholder trust.

Relevant Laws and Regulations

Specific laws and regulations operate the security governance and regulatory ecosystem. They provide a structured framework for establishing minimum compliance standards, promoting accountability and trust, and fostering innovative approaches to safeguarding critical systems and data. By offering clear and concise rules, they reduce ambiguity and provide a common language for organisations to measure their security posture and ensure regulatory compliance. Following is an overview of some relevant laws and regulations:

Law/Regulation	**Domain**	**Description**
General Data Protection Regulation (GDPR)	Data Privacy & Protection	GDPR is a regulation propagated by the European Union that sets strict requirements for how organisations handle and protect and secure the personal data of EU citizens and residents.
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare	A US-based official law to maintain the sensitivity of health-related information of citizens.

Payment Card Industry Data Security Standard (PCI-DSS)	Financial	Set technical and operational requirements to ensure the secure handling, storage, processing, and transmission of cardholder data by merchants, service providers, and other entities that handle payment cards.
Gramm-Leach-Bliley Act (GLBA)	Financial	Financial companies must be sensitive to their customers' nonpublic personal information (NPI), including implementing information security programs, providing privacy notices, and disclosing information-sharing practices.

Answer the questions below

1. A rule or law enforced by a governing body to ensure compliance and protect against harm is called? **Regulation**
2. Health Insurance Portability and Accountability Act (HIPAA) targets which domain for data protection? **Healthcare**

Information Security Frameworks

The information security framework provides a comprehensive set of documents that outline the organisation's approach to information security and governs how security is implemented, managed, and enforced within the organisation. This mainly includes:

- Policies: A formal statement that outlines an organisation's goals, principles, and guidelines for achieving specific objectives.
- Standards: A document establishing specific requirements or specifications for a particular process, product, or service.
- Guidelines: A document that provides recommendations and best practices (non-mandatory) for achieving specific goals or objectives.
- Procedures: Set of specific steps for undertaking a particular task or process.
- Baselines: A set of minimum security standards or requirements that an organisation or system must meet.

Developing Governance Documents

Here are some generalised steps used to develop policies, standards, guidelines, etc.

- **Identify the scope and purpose:** Determine what the document will cover and why it is needed. For example, a password policy might be required to ensure robust and secure user passwords. In contrast, a baseline might be required to establish a minimum level of security for all systems.
- **Research and review:** Research relevant laws, regulations, industry standards, and best practices to ensure your document is comprehensive and up-to-date.

Review existing policies, procedures, and other documents to avoid duplicating efforts or contradicting existing guidance.

- **Draft the document:** Develop an outline and start drafting the document, following best practices for writing clear and concise policies, procedures, standards, guidelines, and baselines. Ensure the document is specific, actionable, and aligned with the organisation's goals and values.
- **Review and approval:** Have the document reviewed by stakeholders, such as subject matter experts, legal and compliance teams, and senior management. Incorporate their feedback and ensure the document aligns with organisational goals and values. Obtain final approval from appropriate stakeholders.
- Implementation and communication: Communicate the document to all relevant employees and stakeholders, and ensure they understand their roles and responsibilities in implementing it. Develop training and awareness programs to ensure the document is understood and followed.
- **Review and update:** Periodically review and update the document to ensure it remains relevant and practical. Monitor compliance and adjust the document based on feedback and changes in the threat landscape or regulatory environment.

Explanation through Real-world Scenarios

We will go through some real-world scenarios to fully understand the steps to develop these documents.

Preparing a Password Policy

- **Define password requirements:** Minimum length, complexity, and expiration.
- **Define password usage guidelines:** Specify how passwords should be used, such as requiring unique passwords for each account, prohibiting the sharing of passwords, and prohibiting default passwords.
- **Define password storage and transmission guidelines:** Using encryption for password storage and requiring secure connections for password transmission.
- **Define password change and reset guidelines:** How often passwords should be changed etc.
- **Communicate the policy:** Communicate the password policy to all relevant employees and stakeholders, and ensure that they understand the requirements and guidelines. Develop training and awareness programs to ensure that employees follow the policy.
- **Monitor compliance:** Monitor compliance with the password policy and adjust the policy as needed based on feedback and changes in the threat landscape or regulatory environment.

Making an Incident Response Procedure

- **Define incident types:** Unauthorised access, malware infections, or data breaches.
- **Define incident response roles and responsibilities:** Identify the stakeholders, such as incident response team members, IT personnel, legal and compliance teams, and senior management.
- **Detailed Steps:** Develop step-by-step procedures for responding to each type of incident, including initial response steps, such as containing the incident and preserving evidence; analysis and investigation steps, such as identifying the root cause and assessing the impact; response and recovery steps, such as mitigating the incident, reporting and restoring normal operations.
- **Report the incident to management and document the incident response process for future reference.**
- **Communicate the incident response procedures.**
- **Review and update the incident response procedures.**

Organisations only sometimes need to make a standard, frameworks, or baselines; instead, they follow and use already made documents related to their field or discipline, as the financial sector may follow PCI-DSS and GLBA; healthcare may follow HIPAA, etc. There are numerous factors upon which we decide which standard framework of baseline checklist should be used; these include regulatory requirements primarily related to the particular geographical areas, scope, objectives, available resources, and many more.

Answer the questions below

1. The step that involves monitoring compliance and adjusting the document based on feedback and changes in the threat landscape or regulatory environment is called? **Review and update**
2. A set of specific steps for undertaking a particular task or process is called? **Procedure**

Governance, Risk, and Compliance (GRC)

As we have studied, information security governance and compliance are necessary to maintain any organisation's overall security posture. But how to achieve it? Here comes the role of the Governance and Risk Compliance (GRC) framework. It focuses on steering the organisation's overall governance, enterprise risk management, and compliance in an integrated manner. It is a holistic approach to information security that aligns with the organisation's goals and objectives and helps to ensure that the

organisation operates within the boundaries of relevant regulations and industry standards. GRC framework has the following three components:

- **Governance Component**: Involves guiding an organisation by setting its direction through information security strategy, which includes policies, standards, baselines, frameworks, etc., along with establishing appropriate monitoring methods to measure its performance and assess the outcomes.
- **Risk Management Component**: Involves identifying, assessing, and prioritising risks to the organisation and implementing controls and mitigation strategies to manage those risks effectively. This includes monitoring and reporting on risks and continuously evaluating and refining the risk management program to ensure its ongoing effectiveness.
- **Compliance Component**: Ensuring that the organisation meets its legal, regulatory, and industry obligations and that its activities align with its policies and procedures. This includes developing and implementing compliance programs, conducting regular audits and assessments, and reporting on compliance issues to stakeholders.

How to Develop GRC Program - Generic Guidelines

A well-developed and implemented GRC program for cyber security provides an integrated framework for managing risks, complying with regulations and standards, and improving the overall security perspective of an organisation. It enables effective governance, risk management, and compliance activities, mitigating cyber incidents' impact and ensuring business resilience. In this section, we will explore how to develop and implement a GRC framework. Developing and implementing a GRC framework

involves various steps; we will explain each step with an appropriate example so that we can easily understand:

- **Define the scope and objectives**: This step involves determining the scope of the GRC program and defining its goals. For example, a company can implement a GRC program for its customer data management system. The objective might be to reduce cyber risks to 50% in the next 12 months while maintaining the trust of its customers.
- **Conduct a risk assessment**: In this step, the organisation identifies and assesses its cyber risks. For example, a risk assessment might reveal that the customer data management system is vulnerable to external attacks due to weak access controls or outdated software. The organisation can then prioritize these risks and develop a risk management strategy.
- **Develop policies and procedures**: Policies and procedures are developed to guide cyber security practices within the organisation. For example, the company might establish a password policy to ensure the usage of strong passwords. They might also implement logging and monitoring system access procedures to detect suspicious activity.
- **Establish governance processes**: Governance processes ensure the GRC program is effectively managed and controlled. For example, the organisation might establish a security steering committee that meets regularly to review security risks and make decisions about security investments and priorities. Roles and responsibilities are defined to ensure everyone understands their role in the program.
- **Implement controls**: Technical and non-technical controls are implemented to mitigate risks identified in risk assessment. For example, the company might implement firewalls, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), and Security Information and Event Management (SIEM) to prevent external attacks and impart employee training to improve security awareness and reduce the risk of human error.
- **Monitor and measure performance**: Processes are established to monitor and measure the effectiveness of the GRC program. For example, the organisation can track metrics and compliance with security policies. This information is used to identify areas for improvement and adjust the program as needed.
- **Continuously improve**: The GRC program is constantly reviewed and improved based on performance metrics, changing risk profiles, and stakeholder feedback. For example, suppose the organisation experiences a security incident. In that case, it might conduct a post-incident analysis to identify the root cause and make changes to prevent a similar incident from happening again.

An Example - GRC Framework in Financial Sector

To fully understand each component of GRC, it is necessary to understand it with real-world examples and scenarios. In the ensuing section, we will see how the financial industry implements each component of the GRC framework:

- **Governance-Related Activities:** Nominate the governance level executives, and make financial-related policies such as bank secrecy act, anti-money laundering policy, financial audit policies, financial reporting, crisis management, and many more.
- **Risk Management Activities:** Identify potential risks, their possible outcomes, and countermeasures such as financial fraud risks, fraudulent transactions through cyber-attack, stolen credentials through phishing, fake ATM cards, etc.
- **Compliance Activities:** Take measures to meet legal requirements and industry standards such as PCI DSS, GLBA, etc. Moreover, this also includes implementing correct methods like SSL/ TLS to avoid Man in the Middle (MITM) attacks, ensuring automatic patch management against unpatched software, creating awareness campaigns for users to protect them from phishing attacks, and many more.

Answer the questions below

What is the component in the GRC framework involved in identifying, assessing, and prioritising risks to the organisation? **Risk Management**

Is it important to monitor and measure the performance of a developed policy? (yea/nay) **yea**

Privacy and Data Protection

In every sector, such as financial, healthcare, government, and industry, privacy and data protection regulations are critical as they deal with citizens' Personally Identifiable Information (PII). Privacy regulations help ensure individuals' personal information is handled and stored responsibly and ethically. They also help to establish trust, protect personal information, and maintain regulatory compliance. Moving forward, we will go through essential cardinals of the most important privacy and data protection regulations and their purpose, which will help us to understand why data protection regulations are crucial.

General Data Protection Regulation (GDPR)

The GDPR is a data protection law implemented by the EU in May 2018 to protect personal data. Personal data is "*Any data associated with an individual that can be utilised to identify them either directly or indirectly*". Key points of the law include the following:

- **Prior approval** must be obtained before collecting any personal data.
- Personal data should be kept to a **minimum** and only collected when necessary.
- **Adequate measures** are to be adopted to protect stored personal data.

The law applies to all business entities that conduct business in the European Union (EU) and collect/store/process the personal data of EU residents and are required to comply. It is one of the most stringent data privacy regulations worldwide and safeguards personal data during collection. Companies can only collect personal data for a legitimate reason and must inform the owner about its processing. Moreover, this also includes penalties and fines based on non-compliance in the following two tiers:

- **Tier 1**: More severe violations, including unintended data collection, sharing data with third parties without consent, etc. Maximum penalty amounting to 4% of the organisation's revenue or 20 million euros (whichever is higher).
- **Tier 2**: Less severe violations, including data breach notifications, cyber policies, etc. The maximum fine for Tier 2 is 2% of the organisation's revenue or 10 million euros (whichever is higher).

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is focused on maintaining secure card transactions and protecting against data theft and fraud. It is widely used by businesses, primarily online, for card-based transactions. It was established by major credit card brands (Visa, MasterCard & American Express). It requires strict control access to cardholder information and monitoring unauthorized access, using recommended measures such as web application firewalls and encryption. You can learn more about the standard here.

Answer the questions below

1. What is the maximum fine for Tier 1 users as per GDPR (in terms of percentage)? **4%**
2. In terms of PCI DSS, what does CHD stand for? **Cardholder Data**

NIST SPECIAL PUBLICATIONS

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have created the ISO/IEC 19249. In this task, we will brush briefly upon ISO/IEC 19249:2017 *Information technology - Security techniques - Catalogue of architectural and design principles for secure products, systems and applications*. The purpose is to have a better idea of what international organizations would teach regarding security principles.

ISO/IEC 19249 lists five *architectural* principles:

1. **Domain Separation**: Every set of related components is grouped as a single entity; components can be applications, data, or other resources. Each entity will have its own domain and be assigned a common set of security attributes. For example, consider the x86 processor privilege levels: the operating system kernel can run in ring 0 (the most privileged level). In contrast, user-mode applications can run in ring 3 (the least privileged level). Domain separation is included in the Goguen-Meseguer Model.
2. **Layering**: When a system is structured into many abstract levels or layers, it becomes possible to impose security policies at different levels; moreover, it would be feasible to validate the operation. Let's consider the OSI (Open Systems Interconnection) model with its seven layers in networking. Each layer in the OSI model provides specific services to the layer above it. This layering makes it possible to impose security policies and easily validate that the system is working as intended. Another example from the programming world is disk operations; a programmer usually uses the disk read and write functions

provided by the chosen high-level programming language. The programming language hides the low-level system calls and presents them as more user-friendly methods. Layering relates to Defence in Depth.

3. **Encapsulation**: In object-oriented programming (OOP), we hide low-level implementations and prevent direct manipulation of the data in an object by providing specific methods for that purpose. For example, if you have a clock object, you would provide a method `increment()` instead of giving the user direct access to the `seconds` variable. The aim is to prevent invalid values for your variables. Similarly, in larger systems, you would use (or even design) a proper Application Programming Interface (API) that your application would use to access the database.
4. **Redundancy**: This principle ensures availability and integrity. There are many examples related to redundancy. Consider the case of a hardware server with two built-in power supplies: if one power supply fails, the system continues to function. Consider a RAID 5 configuration with three drives: if one drive fails, data remains available using the remaining two drives. Moreover, if data is improperly changed on one of the disks, it would be detected via the parity, ensuring the data's integrity.
5. **Virtualization**: With the advent of cloud services, virtualization has become more common and popular. The concept of virtualization is sharing a single set of hardware among multiple operating systems. Virtualization provides sandboxing capabilities that improve security boundaries, secure detonation, and observance of malicious programs.

ISO/IEC 19249 teaches five *design* principles:

1. **Least Privilege**: You can also phrase it informally as "need-to basis" or "need-to-know basis" as you answer the question, "who can access what?" The principle of least privilege teaches that you should provide the least amount of permissions for someone to carry out their task and nothing more. For example, if a user needs to be able to view a document, you should give them read rights without write rights.
2. **Attack Surface Minimisation**: Every system has vulnerabilities that an attacker might use to compromise a system. Some vulnerabilities are known, while others are yet to be discovered. These vulnerabilities represent risks that we should aim to minimize. For example, in one of the steps to harden a Linux system, we would disable any service we don't need.
3. **Centralized Parameter Validation**: Many threats are due to the system receiving input, especially from users. Invalid inputs can be used to exploit vulnerabilities in the system, such as denial of service and remote code

execution. Therefore, parameter validation is a necessary step to ensure the correct system state. Considering the number of parameters a system handles, the validation of the parameters should be centralized within one library or system.

4. **Centralized General Security Services**: As a security principle, we should aim to centralize all security services. For example, we would create a centralized server for authentication. Of course, you might take proper measures to ensure availability and prevent creating a single point of failure.
5. **Preparing for Error and Exception Handling**: Whenever we build a system, we should take into account that errors and exceptions do and will occur. For instance, in a shopping application, a customer might try to place an order for an out-of-stock item. A database might get overloaded and stop responding to a web application. This principle teaches that the systems should be designed to fail safely; for example, if a firewall crashes, it should block all traffic instead of allowing all traffic. Moreover, we should be careful that error messages don't leak information that we consider confidential, such as dumping memory content that contains information related to other customers.

In the following questions, refer to the ISO/IEC 19249 five design principles above. Answer with a number between 1 and 5, depending on the number of the design principle.

Answer the questions below

1. Which principle are you applying when you turn off an insecure server that is not critical to the business? **2**
2. Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices? **1**
3. While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying? **5**

Information Security Management and Compliance

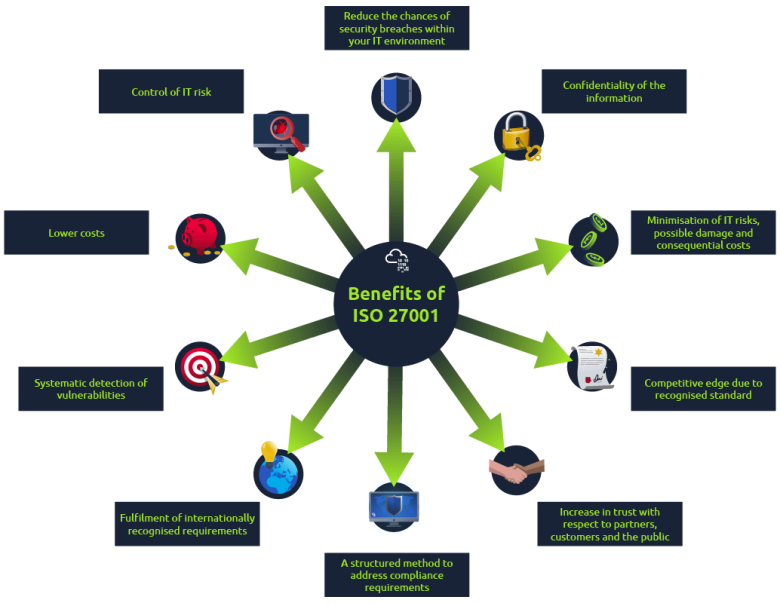
The strategic planning, execution, and continuous administration of security measures are all part of Information Security (IS) management, which **protects information assets from unauthorized access, use, disclosure, interruption, alteration, and destruction**. It involves risk assessment and identification, security controls and procedures development, incident response planning, and security awareness training. Contrarily, compliance refers to **observing information security-related legal,**

regulatory, contractual, and industry-specific standards. In IS management and compliance, we will go through two key standards.

ISO/IEC 27001

ISO 27001 is an internationally recognised standard for requirements to **plan, develop, run, and update** an organisation's Information Security Management System (ISMS). The official ISO/IEC 27001 documents are paid for and can be purchased from this link. It was developed by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has the following core components:

- **Scope**: This specifies the ISMS's boundaries, including the covered assets and processes.
- **Information security policy**: A high-level document defining an organisation's information security approach.
- **Risk assessment**: Involves identifying and evaluating the risks to the confidentiality, integrity, and availability of the organisation's information.
- **Risk treatment**: Involves selecting and implementing controls to reduce the identified risks to an acceptable level.
- **Statement of Applicability (SoA)**: This document specifies which controls from the standard are applicable and which are not.
- **Internal audit**: This involves conducting periodic audits of the ISMS to ensure that it is operating effectively.
- **Management review**: Review the performance of ISMS at regular intervals.



An ISMS built on the ISO 27001 standard requires careful design and execution. It entails exhaustively evaluating the **organisation's security procedures, detecting gaps, and conducting a thorough risk assessment**. Access control, incident response, etc., are just a few examples of the areas where clear rules and processes must be created and aligned with ISO 27001 requirements. **Leadership support and resource allocation** are also essential for the ISMS to be implemented successfully. **Regular monitoring, measurement, and continual development** are crucial to guarantee the efficacy and continued alignment of the ISMS with the organization's objectives.

Service Organization Control 2 (SOC 2)

SOC 2 was developed by the American Institute of Certified Public Accountants (AICPA) as a **compliance/auditing framework**. It focuses on assessing the efficacy of a company's data security based on the CIA triad. SOC 2 can reassure customers, stakeholders, and business partners that the company has put **sufficient controls in place to safeguard its systems, data, and sensitive information**.

The SOC 2 framework is essential for service providers interacting with client data or offering solutions that **process, store, or transmit sensitive data**. It assists businesses in demonstrating their dedication to upholding strict privacy and security standards. Customers frequently ask for SOC 2 reports or use them as a competitive advantage to guarantee clients that their information will be handled securely. You can learn more about it here.

Important Cardinals

- SOC 2 is an auditing standard that evaluates the usefulness of a service organisation's controls related to confidentiality, availability, integrity, and privacy.
- Independent auditors conduct SOC 2 audits to determine that security controls meet the relevant criteria.
- SOC 2 reports provide valuable information to customers, stakeholders, and regulators on a service organisation's security and privacy practices. They can be used to demonstrate that the service organisation has adequate controls to protect the data and systems it uses to process customers' information. For example, a cloud computing company that provides infrastructure services to other businesses may undergo a SOC 2 audit to demonstrate its adequate controls to protect customer data stored on its servers. The audit may cover physical security, network security, data encryption, backup and recovery, and employee training and awareness.

- The SOC 2 audit report will assess the controls in place at the cloud computing company and include any findings or recommendations for improvement. The information can be shared with customers and other stakeholders to ensure the company takes appropriate measures to protect its data and systems.

What Information Security Protection SOC 2 provides?

The primary purpose of the SOC 2 audit is to ensure that third-party service providers store and process sensitive information securely.

Planning and Undergoing a SOC 2 Audit

The following steps can be taken by an organisation's management team before and during an audit:

- **Determine the scope**: This may include specific systems, processes, or locations that are relevant to the security and privacy of customer data.
- **Choose a suitable auditor**: Select a qualified auditor with experience conducting SOC 2 audits for financial companies. Consider factors such as the auditor's reputation, experience, and availability.
- **Plan the audit:** Work with the auditor to plan the audit, including the audit timeline, the scope of the audit, and the audit criteria.
- **Prepare for the audit**: Prepare for the audit by reviewing your security and privacy controls, policies, and procedures. Identify any gaps or deficiencies and develop a plan to address them.
- **Conduct the audit**: The auditor will review your controls and conduct testing to assess their effectiveness. The audit may include interviews with key personnel, documentation reviews, and controls tests.
- **Receive the audit report**: Once the audit is complete, the auditor will provide a report detailing the audit results. The report may include a description of your controls, any deficiencies or gaps identified, and recommendations for improvement.

The above diagram shows the generic controls that will be checked during a SOC 2 audit for a financial company depending on the scope of the audit. Other than that, there are technical and specific controls, like ensuring data encryption in transit, network security, incident management, etc.

Answer the questions below

1. Which ISO/IEC 27001 component involves selecting and implementing controls to reduce the identified risks to an acceptable level? **Risk treatment**
2. In SOC 2 generic controls, which control shows that the system remains available? **Availability**

Conclusion

This room has provided a comprehensive overview of the importance of developing an effective **information security governance & regulation framework** to protect an organisation's valuable assets and sensitive information. We have learned about various **laws and regulations governing privacy and data protection**, such as GDPR and PCI DSS. The room has also introduced the Governance, Risk Management, and Compliance (GRC) Framework concept and explained how to develop an effective GRC program through real-world scenarios.

Furthermore, the room has highlighted different governance enablers, such as **ISO/IEC 27001, NIST 800-53, and NIST Special Publication 800-63B**, and explained how they provide information security protection to an organisation. Due to the ongoing emergence of new threats and vulnerabilities, information security is a relative concept. While achieving 100% security is

unrealistic, a proactive organisation understands the need to continuously implement robust security policies to mitigate risks and safeguard sensitive data.

Stay tuned for more exciting rooms on governing and regulating an organisation's security through policies.

Answer the questions below

Click the View Site button at the top of the task to launch the static site in split view.
What is the flag after completing the exercise? **THM{SECURE_1001}**