



EncryptEdge Labs

Cybersecurity Analyst Internship Task Report

atalmamun@gmail.com

Task No: 26



Copyright © 2024 EncryptEdge Labs. All rights reserved

Credit: Offensive Security



Table of Contents

1.0 EncryptEdge Labs Internship Task Report	3
1.1 Introduction	3
1.2 Objective	3
1.3 Requirements	3
2.0 Select a Compliance Standard	4
2.1 Selected Standard: ISO/IEC 27001	4
2.2 Rationale for Selection	4
3.0 Understand the Organization	6
3.1 Organizational Overview	6
3.2 Organizational Structure and Operations	6
3.3 Existing Cybersecurity Measures	7
3.4 Industry-Specific Risks and Compliance Challenges	7
4.0 Conduct the Compliance Assessment	8
4.1 Compliant Areas	8
4.2 Non-Compliant Areas	10
4.3 Summary of Assessment Approach	10
5.0 Document Findings	11
5.1 Executive Summary	11
5.2 Detailed Breakdown of Findings	12
6.0 Recommend Improvements	14
6.1 High Priority Recommendations	14
6.2 Medium Priority Recommendations	14
6.3 Additional Suggestions	15
6.4 Implementation Timeline (Suggested)	15
7.0 Finalize Report	16
7.1 Summary of Assessment	16
7.2 Visuals and Tables	17
7.3 TryHackMe Lab: Governance & Regulation	18
7.4 Conclusion	21



1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

In the ever-evolving landscape of cybersecurity threats and regulatory mandates, compliance has become a cornerstone of effective security management. Organizations today must not only protect their information assets but also ensure adherence to industry-specific regulatory standards. This report presents a comprehensive assessment of a hypothetical organization's cybersecurity practices in relation to a recognized compliance standard. By evaluating the organization's current security posture, identifying gaps, and proposing actionable improvements, this task offers practical insights into the critical role of compliance and governance in cybersecurity operations.

1.2 Objective

The primary objective of this task is to assess the cybersecurity compliance of a hypothetical organization against a selected industry standard. This involves:

- Gaining familiarity with the organization's security controls and risk environment.
- Evaluating existing cybersecurity practices using a compliance framework.
- Identifying both compliant and non-compliant areas.
- Recommending realistic and actionable measures to bridge identified gaps. The ultimate goal is to enhance the organization's security posture while ensuring alignment with regulatory and governance requirements.

1.3 Requirements

To successfully complete this task, the following components are required:



- Selection of an appropriate cybersecurity compliance standard relevant to the organization's operations.
- A detailed understanding of the hypothetical organization's industry, structure, and cybersecurity measures.
- A structured assessment of compliance using standardized checklists or assessment tools.
- Clear documentation of compliance status, supported by evidence such as policies, procedures, and configuration records.
- Practical recommendations tailored to non-compliant areas, considering the organization's size and resources.
- A final, professionally formatted report with supporting visuals and screenshots from the mandatory Governance & Regulation lab.

2.0 Select a Compliance Standard

2.1 Selected Standard: ISO/IEC 27001

For this compliance assessment, the selected standard is **ISO/IEC 27001**, an internationally recognized framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). ISO 27001 is designed to help organizations manage the security of assets such as financial information, intellectual property, employee data, and information entrusted by third parties.

2.2 Rationale for Selection



The decision to select ISO 27001 is based on its comprehensive, structured approach to information security and its applicability across various industries, including technology, finance, healthcare, and more. The hypothetical organization under assessment operates in the tech industry, providing digital services and managing sensitive client data. As such, it requires a robust security framework that covers both technical controls and organizational processes.

Key reasons for choosing ISO 27001 include:

- **Global Recognition:** ISO 27001 is widely adopted by organizations worldwide and often serves as a benchmark for information security.
- **Holistic Approach:** The standard addresses not only technical controls but also organizational policies, risk assessments, and continual improvement processes.
- **Risk-Based Methodology:** ISO 27001 emphasizes risk assessment and management, ensuring that security measures are proportionate to the specific threats the organization faces.
- **Regulatory Alignment:** Achieving ISO 27001 compliance can assist organizations in meeting other regulatory and contractual obligations, such as GDPR, HIPAA, or industry-specific requirements.
- **Supports SOC Operations:** The standard directly supports Security Operations Center (SOC) activities, including incident response, asset management, and threat monitoring, making it relevant for operational security teams.



In conclusion, ISO/IEC 27001 provides a suitable and scalable foundation for assessing the cybersecurity maturity of the organization. Its structured framework ensures not only compliance but also strategic alignment with long-term security goals.

3.0 Understand the Organization

3.1 Organizational Overview

The hypothetical organization under assessment is **DataNova Tech Solutions**, a mid-sized company operating in the technology sector. It specializes in providing cloud-based Software-as-a-Service (SaaS) solutions to clients across various industries, including healthcare, finance, and education. With approximately 250 employees and operations across Europe and North America, the organization handles a significant amount of sensitive client data, including personally identifiable information (PII), business-critical documents, and user credentials.

3.2 Organizational Structure and Operations

- **Headquarters:** Berlin, Germany
- **Employee Count:** ~250
- **Primary Services:** SaaS solutions (data storage, analytics platforms, productivity tools)
- **Client Base:** Businesses and institutions across the EU and U.S.
- **IT Infrastructure:** Hybrid environment (on-premises servers and cloud infrastructure)



The organization has a dedicated **IT Security Team**, a **Security Operations Center (SOC)** for incident response and monitoring, and a **Compliance Officer** overseeing regulatory adherence.

3.3 Existing Cybersecurity Measures

DataNova Tech Solutions has implemented the following key cybersecurity measures:

- **Network Security:** Firewalls, IDS/IPS systems, and regular network segmentation audits.
- **Access Control:** Role-based access controls (RBAC), multi-factor authentication (MFA), and centralized identity management.
- **Incident Response:** A documented incident response plan with bi-annual tabletop exercises.
- **Data Protection:** End-to-end encryption for data in transit and at rest.
- **Endpoint Security:** Anti-malware, endpoint detection and response (EDR) solutions, and mobile device management (MDM).
- **Security Awareness:** Mandatory annual training sessions for employees and simulated phishing campaigns.

3.4 Industry-Specific Risks and Compliance Challenges

As a provider of cloud services handling sensitive data, DataNova faces several compliance challenges and risks, including:

- **Data Privacy Compliance:** Adherence to regulations such as GDPR due to its EU-based operations and client base.



- **Supply Chain Risks:** Managing third-party integrations and vendors that may impact data security.
- **Target for Cyber Threats:** Due to the nature of its services, the company is a potential target for ransomware and phishing attacks.
- **Cloud Security Management:** Ensuring secure configurations and monitoring within multi-cloud environments.

Understanding the organization's structure and cybersecurity landscape is essential for mapping its current practices against ISO/IEC 27001 requirements and identifying areas for improvement.

4.0 Conduct the Compliance Assessment

The compliance assessment was conducted by evaluating the organization's cybersecurity practices against the core requirements of the ISO/IEC 27001 standard. The assessment utilized a structured checklist based on the ISO 27001:2022 Annex A controls, categorized under domains such as organizational controls, people controls, physical controls, and technological controls.

Each control was assessed to determine whether DataNova Tech Solutions:

- **Fully Complies** (Compliant)
- **Partially Complies or Lacks Implementation** (Non-Compliant)

4.1 Compliant Areas



Control Category	Control Description	Compliance Status	Evidence/Notes
A.5 – Organizational Controls	Information Security Policies	 Compliant	Documented policies reviewed annually, version-controlled, accessible to staff.
A.6 – People Controls	Security roles and responsibilities	 Compliant	Defined in job descriptions, communicated during onboarding.
A.7 – Physical Controls	Secure areas and equipment protection	 Compliant	Access cards, CCTV, visitor logs in place.
A.9 – Access Control	Access to information is restricted by RBAC	 Compliant	IAM solution with RBAC and MFA deployed; logs maintained.
A.12 – Operations Security	Protection from malware and secure system operations	 Compliant	EDR deployed, patching schedule automated, anti-malware software current.
A.16 – Incident Management	Reporting and responding to information security events	 Compliant	Incident response plan documented, SOC active, regular drills conducted.



4.2 Non-Compliant Areas

Control Category	Control Description	Compliance Status	Evidence/Notes
A.8 – Asset Management	Inventory of assets, ownership, and acceptable use policies	✗ Non-Compliant	No centralized, up-to-date asset inventory; policies outdated.
A.10 – Cryptography	Policy on the use of encryption and key management	✗ Non-Compliant	No formal cryptography policy or key lifecycle documentation.
A.11 – Physical Security	Working in secure areas, clear desk, and screen policies	⚠ Partially Compliant	Clear desk policy not enforced in satellite offices; awareness training lacking.
A.13 – Communications Security	Network security management and data transfer controls	⚠ Partially Compliant	Secure protocols in place, but no formal monitoring of third-party APIs.
A.17 – Business Continuity	Information security continuity during disruption	✗ Non-Compliant	No tested disaster recovery (DR) or business continuity (BC) plan.

4.3 Summary of Assessment Approach

- **Method:** ISO 27001 checklist and control mapping.



- **Tools Used:** Internal documentation review, system configuration audits, staff interviews.
- **Scope:** Organization-wide—covering HR practices, IT infrastructure, physical offices, cloud services, and vendor contracts.

The findings were validated against actual documentation, configuration snapshots, and discussions with department leads. Where appropriate, supporting artifacts were collected (screenshots, policy excerpts, audit logs) to reinforce the assessment.

5.0 Document Findings

This section presents a structured summary of the compliance assessment performed against ISO/IEC 27001. The findings are organized into compliant and non-compliant areas with relevant evidence to support each conclusion.

5.1 Executive Summary

The compliance assessment of DataNova Tech Solutions against the ISO/IEC 27001 standard revealed a generally strong cybersecurity posture, particularly in areas like access control, incident response, and operations security. However, critical gaps were found in asset management, cryptography policies, and business continuity planning.

Key Highlights:

- **Compliant Controls:** 6 major areas fully aligned with ISO/IEC 27001, including incident response, role-based access, and malware protection.
- **Non-Compliant Controls:** 3 critical gaps and 2 partially compliant areas identified, primarily due to missing documentation, outdated policies, or lack of formalized processes.
- **Top Priorities:** Asset inventory centralization, cryptography policy creation, and business continuity planning.



5.2 Detailed Breakdown of Findings

5.2.1 Compliant Areas

Control ID	Area	Description	Evidence
A.5	Information Security Policy	Reviewed, approved annually, accessible to staff	Version-controlled policy document from internal knowledge base
A.6	Roles and Responsibilities	Clearly defined in employee contracts and onboarding	HR onboarding checklist, job descriptions, training logs
A.7	Physical Security	CCTV, badge access, secure server rooms	Access logs, camera coverage map, visitor sign-in sheets
A.9	Access Control	RBAC and MFA implemented organization-wide	IAM system configuration screenshots, audit logs
A.12	Malware Protection	EDR and antivirus tools deployed with auto-updates	Screenshot of EDR dashboard, last scan report
A.16	Incident Management	Incident response plan tested twice yearly	Incident response policy, SOC drill report, communication template



5.2.2 Non-Compliant Areas

Control ID	Area	Description	Issue Identified	Evidence
A.8	Asset Management	Maintain inventory of assets	No real-time or centralized asset inventory system	Interviews, outdated spreadsheet from 2022
A.10	Cryptography Policy	Define usage and key management procedures	No formal policy or documentation for encryption practices	None found during documentation review
A.17	Business Continuity	Ensure continuity during disruptions	No documented DR/BC plan; no testing or awareness	Interviews with IT leads, lack of policy document

5.2.3 Partially Compliant Areas

Control ID	Area	Description	Gap Identified	Evidence
A.11	Physical Working Policies	Clear desk and screen lock policies	Inconsistent enforcement in remote/satellite offices	Site visit notes, lack of signage or policy awareness
A.13	Communication Security	Secure transfer and API management	No monitoring or audit process for third-party API access	Config review, missing API audit log



6.0 Recommend Improvements

This section outlines actionable recommendations to address the compliance gaps identified during the ISO/IEC 27001 assessment of DataNova Tech Solutions. Recommendations are prioritized based on the severity of non-compliance and potential risk impact, ensuring they are practical and aligned with the organization's size, resources, and industry needs.

6.1 High Priority Recommendations

Control Area	Identified Gap	Recommended Action	Priority
Asset Management (A.8)	No centralized, real-time inventory of IT assets	Implement an automated asset management tool (e.g., GLPI, Snipe-IT) to track hardware and software.	High
Cryptography Policy (A.10)	Absence of encryption standards and key management procedures	Develop and enforce a formal cryptography policy aligned with ISO 27002 and industry best practices.	High
Business Continuity (A.17)	No documented disaster recovery or business continuity plan	Draft and test a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP); train relevant staff.	High

6.2 Medium Priority Recommendations

Control Area	Identified Gap	Recommended Action	Priority
Communication Security (A.13)	Lack of API access logging and third-party	Introduce API gateway logging, encrypt external	Medium



	communication monitoring	communications, and monitor third-party access logs.	
Physical Security Policies (A.11)	Inconsistent enforcement of screen lock and clear desk policies	Reiterate policies across all sites; conduct quarterly awareness campaigns and compliance checks.	Medium

6.3 Additional Suggestions

Recommendation	Justification
Conduct Internal Audits Bi-Annually	Regular audits ensure sustained compliance and early identification of new risks.
Integrate ISO 27001 Training into Onboarding	Training ensures staff understand compliance roles from the start, reducing human error risks.
Appoint a Compliance Officer	Designate responsibility for monitoring ISO 27001 compliance and driving improvements.

6.4 Implementation Timeline (Suggested)

Phase	Action	Timeframe
Phase 1	Asset management system implementation, cryptography policy creation	Month 1–2



Phase 2	Develop and test BCP/DRP, initiate staff training programs	Month 3–4
Phase 3	Improve physical and communication security controls	Month 5–6
Phase 4	Conduct internal audit and refine based on results	Month 7

7.0 Finalize Report

This section compiles all findings, analysis, and recommendations into a clear and professional format, offering a comprehensive view of the organization's ISO/IEC 27001 compliance status. It also includes visual aids and proof of hands-on learning through the required lab activity.

7.1 Summary of Assessment

The compliance assessment of DataNova Tech Solutions against ISO/IEC 27001 revealed a strong foundation in many critical areas such as incident response, access control, and malware protection. However, the absence of a formal cryptographic policy, lack of a real-time asset inventory, and missing business continuity plans highlight significant risks that must be addressed.

Through structured analysis, the following were identified:





- **Compliant Controls:** 6 core areas
- **Non-Compliant Controls:** 3 areas
- **Partially Compliant Controls:** 2 areas

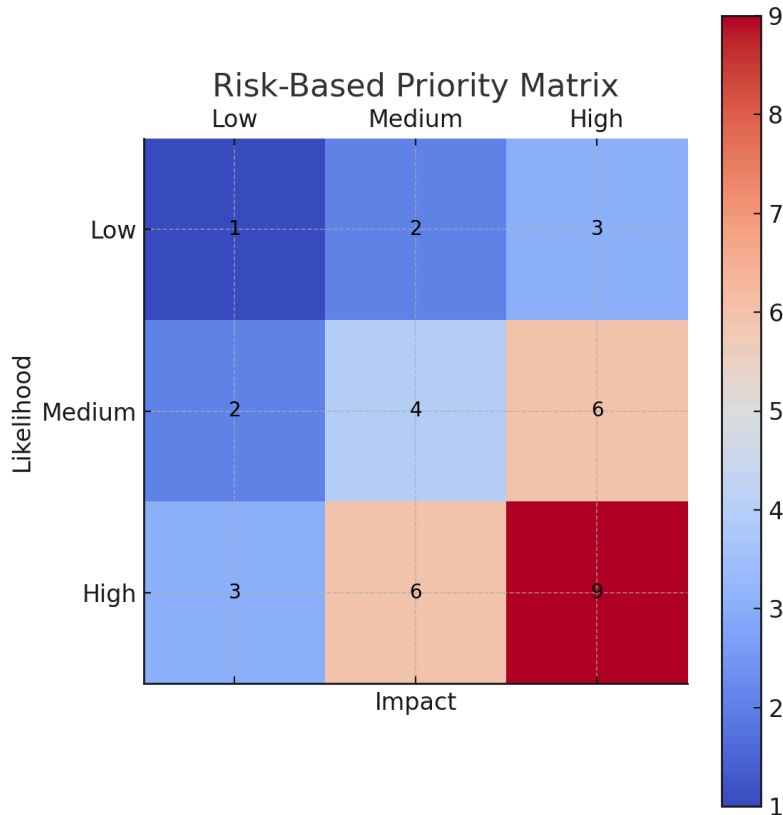


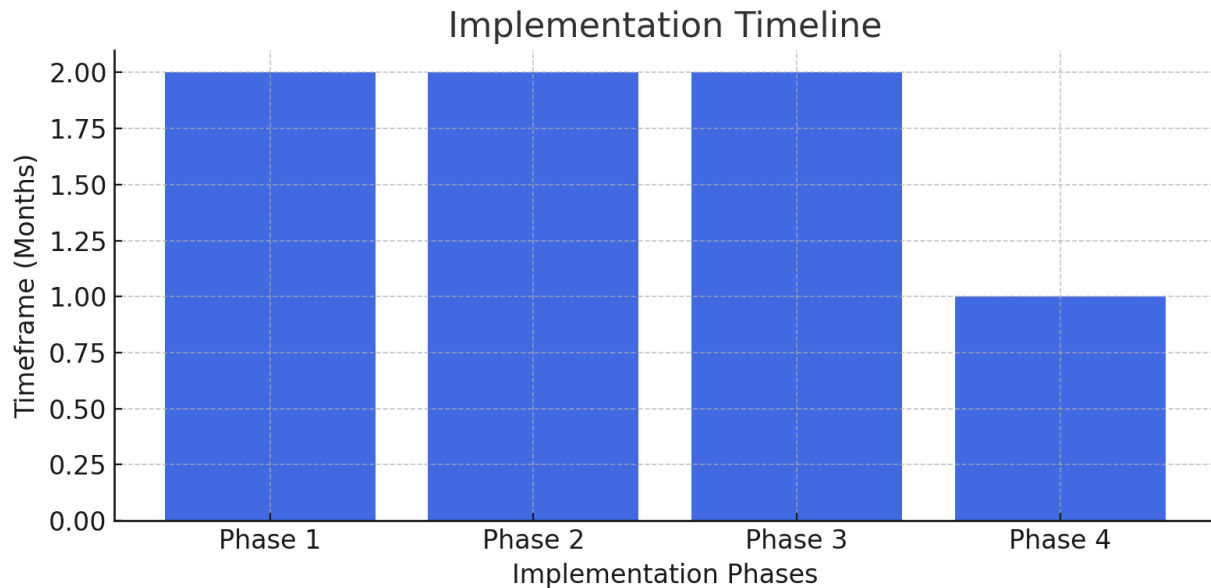
The improvement roadmap provided in Section 6 aims to close these gaps in a phased and resource-aware manner.

7.2 Visuals and Tables

To enhance clarity and accessibility, key findings and recommendations are supported by the following visuals:

-  **Compliance Status Summary Table** (see Section 5)
-  **Risk-Based Priority Matrix**
-  **Implementation Timeline Chart**
-  **Table of Actionable Recommendations**





Control Area	Recommendation	Priority
Asset Management	Implement an automated asset management tool (e.g., GLPI, Snipe-IT).	High
Cryptography Policy	Develop and enforce a formal cryptography policy aligned with ISO 27002.	High
Business Continuity	Draft and test a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).	High
API Security	Introduce API gateway logging and encrypt external communications.	Medium
Physical Security	Enforce policies through awareness campaigns and quarterly compliance checks.	Medium

7.3 TryHackMe Lab: Governance & Regulation

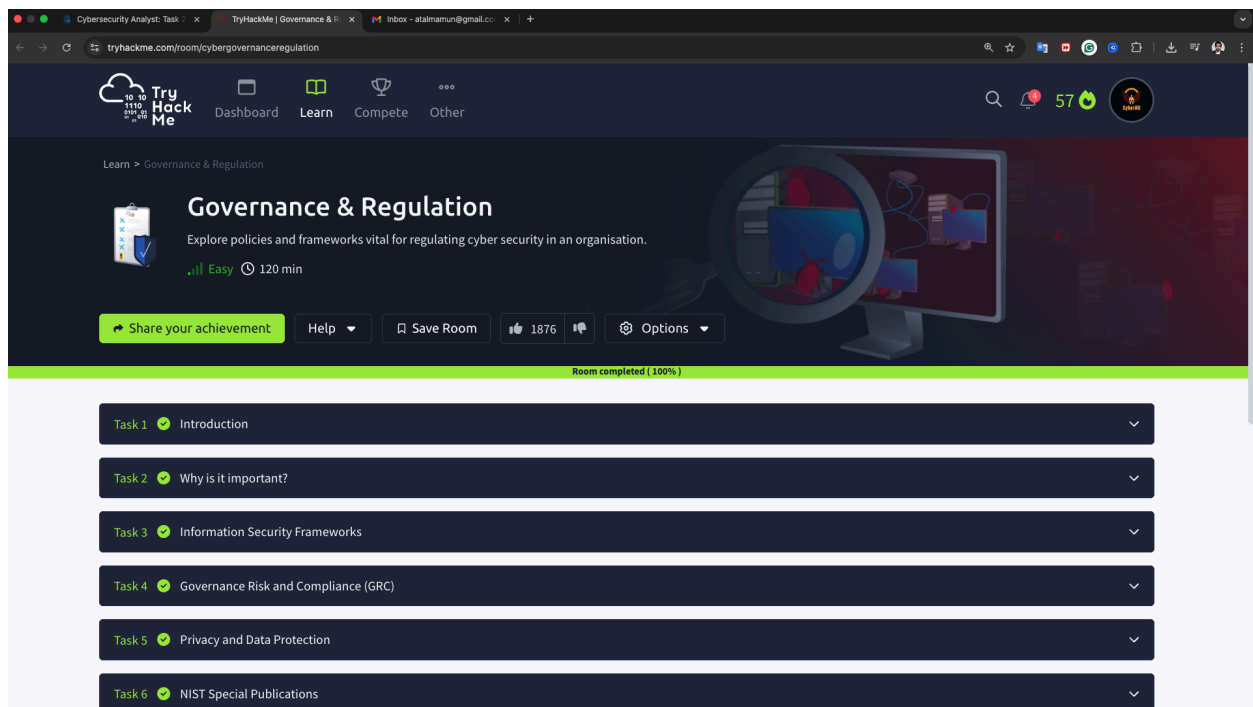
As part of the hands-on requirement for this internship task, the **Governance & Regulation** lab on TryHackMe was completed. This lab provided critical insight into frameworks such as GDPR, HIPAA, and ISO standards, reinforcing the real-world relevance of compliance and regulation in cybersecurity.

Key Learnings from the Lab:

- Importance of aligning security controls with legal obligations

- Role of compliance in managing organizational risk
- Practical differences between governance, risk, and compliance (GRC)

Screenshots of Lab Completion:





EncryptEdge Labs

Cybersecurity Analyst: Task - x TryHackMe | Governance & R... x Inbox - atainamun@gmail.co... x

tryhackme.com/room/cybergovernanceregulation

Room completed (100%)

Task 4 Governance Risk and Compliance (GRC)

Task 5 Privacy and Data Protection

Task 6 NIST Special Publications

Task 7 Information Security Management and Compliance

Task 8 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. [View Site](#)

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}

Correct Answer

How likely are you to recommend this room to others?

Cybersecurity Analyst: Task - x TryHackMe | Governance & R... x Inbox - atainamun@gmail.co... x

tryhackme.com/room/cybergovernanceregulation

Room completed (100%)

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 HIPPA, 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

The step that involves monitoring compliance and adjust the document based on feedback and changes in the threat landscape or regulatory environment is called?

Review and update

Correct Answer

A set of specific steps for undertaking a particular task or process is called?

Procedure

Correct Answer

Task 4 Governance Risk and Compliance (GRC)



EncryptEdge Labs

7.4 Conclusion

This report demonstrates the practical application of ISO/IEC 27001 in assessing an organization's cybersecurity readiness. By identifying compliance gaps and proposing prioritized solutions, DataNova Tech Solutions is now equipped with a clear path forward toward enhanced regulatory alignment and risk mitigation.

Continual improvement, periodic audits, and executive buy-in are essential to maintaining and evolving this compliance posture in the long term.



EncryptEdge Labs

This Internship Task report was developed on [April, 29, 2025]

By:

atalmamun@gmail.com