Can we fix it? Yes, we can!

6054CEM Security Management Coursework

Ahmed Rashwan

Table of Contents

Assumptions

- **[COMPANY REDACTED]** is looking to comply with ISO 27001 as a global standard
- The following departments are handled by **[COMPANY REDACTED]** Home office
  - Maintenance
  - Sales & Marketing
  - Finance & Accounting
  - Human Resources
  - Cyber Security

Allocated Industry

Allocated Industry	**Accommodation & Food**

Introduction

[REDACTED] is a Spanish hotel chain and the 17th biggest hotel chain in the world. **[REDACTED]** operates 374 hotels in 40 countries on 4 continents. A comprehensive security policy ensures that all parties associated with [REDACTED] comply with standards set to protect sensitive information, reduce risks, and prevent breaches. This report will evaluate the current security policy written by [REDACTED], identify any shortcomings or deficiencies, and recommend improvements to enhance compliance and overall protection.

A Look Into The Establishment

[COMPANY REDACTED] was founded in 1956 and operates over 400 hotels mainly having their headquarters in Palma de Mallorca, Spain founded by **[REDACTED]**. The table below identifies the 3 brand levels defined by **[REDACTED]** and their associated brands. ([REDACTED COMPANY], 2021)

Brand Level	*Brand*
Luxury	6% Gran [redacted] & Resorts
	The [redacted] Collection
	3% [redacted]
	3% [redacted]
Premium	38% [redacted]
	12% [redacted]
Essential	19% [redacted]
	17% Affiliated by [redacted]

([REDACTED COMPANY], 2021)

[REDACTED COMPANY], competes against some of the largest names in the accommodation and food industry both domestically and internationally. Some international competitors include Mariott, Ritz-Carlton, Sheraton, Hilton, Hyatt Hotels and IHG (International Hotel Group). On the more domestic side, **[REDACTED]** competes against NH hotel Group and Barceló Hotel Group. The diagram below represents the company's internal departments and below it, a diagram of the company's governance structure.

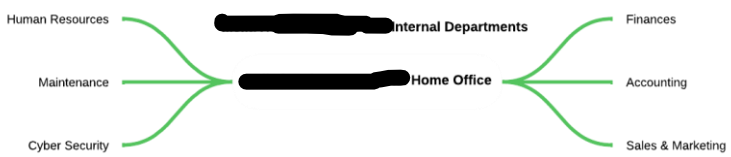

Figure 1: Internal Departments of [REDACTED]

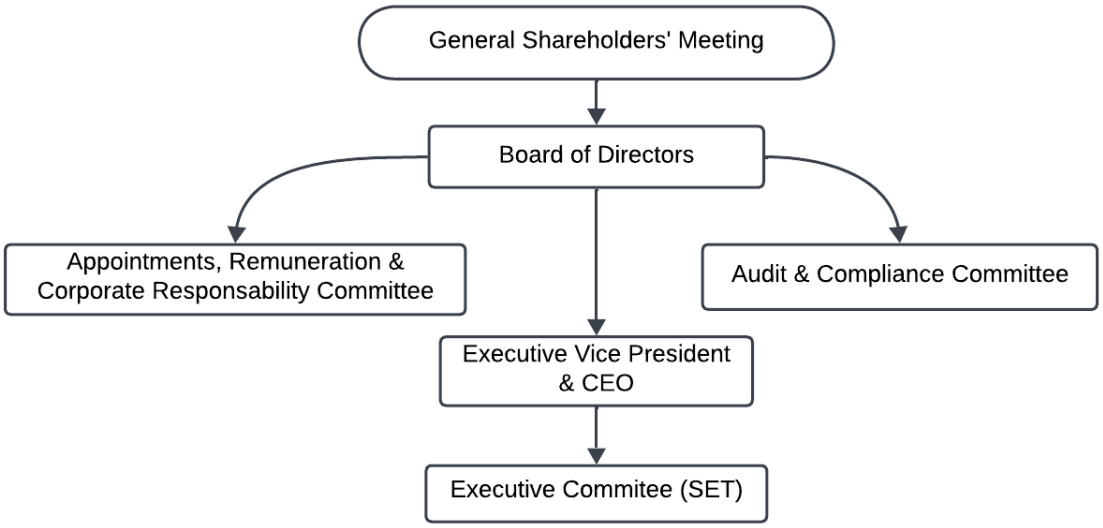

Figure 2: Governance Structure

Below is a table that reflects on the complexities that **[REDACTED]** faces in terms of Information technology infrastructure.

Category	Infrastructure Complexity
Data Security and Privacy	Union compliance across all regions due to varied regulatory frameworks and standards
	No strategy to prevent against insider threats, disgruntled employees.
New system and legacy systems integration	Difficulty integrating newer, potentially cloud based systems with older, more legacy on-premises systems.
	No clear measures in place related to integrating third-party software with current **[REDACTED]** Infrastructure in a safe manner, especially if the third-party software uses outdated or less-secure platforms.
Supply chain security	Lack of detail regarding more large-scale supplier's risks, especially if they don't meet the same standards as **[REDACTED COMPANY]**.

[REDACTED COMPANY] Maturity Model

The following maturity model has been created using the CMMI and tailored specifically towards **[REDACTED]** to represent a benchmark for assessing current the organizations capabilities and use it as a model for continuous improvements. (Wikipedia Contributors, 2019)

Category	Sub-Categories	Level 1 - Initial	Level 2 - Managed	Level 3 - Defined	Level 4- Quantitatevely Defined	Level 5 - Optimized
Governance	Standards and Security Compliance Policy & Documentation Management	• No formal and dedicated security standard defined • Basic regulatory requirements are not fully met with ad-hoc documentation • Minimal information documented on the policy with little employee awareness	• Some policies & Documentation mentioned and in-place but not being strictly enforced, implemented or completed • Compliance of these policies are managed on a high-level • Basic regulatory compliance is met but very minimal additional security controls in place	• An in-depth and comprehensive security policy that is enforced organization-wide, aligns with industry standards like ISO 27001/27002 & PCI-DSS • The policy is clearly documented, annually reviewed, and communicated across all departments	• Policy is checked regularly for compliance with tools in-place to monitor policy adherence is maintained across the departments of the company • Decision driven by data and KPI (key performance indicators) is used to improve documentation practices and overall security compliance • Automated systems in place to monitor and report security breaches or policy infringement automatically	• Continuous analysis/improvement of Policy mentioned clearly in the policies and documentation • Policies are regularly reviewed and optimised by board of directors based on upcoming trends and patterns • Advanced A.I. tools in place to detect and anticipate security threats to maintain compliance
Identity & Access Management	User Access Setup Authentication, Authorization & Accounting Privileged Access Management Solution	• Access to company systems and applications is manual, with no consistency, central oversight or approval of information being accessed • Authentication methods are basic like passwords with no added layer of security like 2FA/MFA with absence of user activities tracking • Privileged accounts are not supervised	• Basic access controls in place but inconsistent in their application and Password policies is enforced but with little application to 2FA/MFA • privileged access is partially managed and Access reviews are occasional but lack detail and are very high level • Corrections take a long time to implement and are inconsistent	• Identity and Access Management are well documented with a clear workflow of requesting and approving access. • A formal Role-Based Access Control (RBAC) is implemented with instead of basic Discretionary Access Control (DAC) • Users activity is logged and tracked regularly with audit trails and tools or solutions to manage privileged accounts activity • Regular access reviews are scheduled any changes are acted upon immediately ensuring constant compliance	• IAM is integrated into a centralized management system with closely monitored access rights and metrics in place to track efficiency and have automated workflow to handle user access setup • 2FA/MFA is enforced organizational-wide with PAM (Privileged Access Management) solution or tool implemented • Real-time and automated alerts setup for any suspicious actions taken by users/privileged accounts • Access Reviews are based on company's analytics and automated with instantaneous corrective actions	• Identity and Access Management is entirely automated and integrated seamlessly into the organizations systems and applications with Access rights is adjusted based on the user's real-time behaviour and a conducted risk assessment • MFA is applied universally • Advanced analytics are used to consistently optimise the authorization process of the company with strict control of privileged access accounts and in-depth monitoring and automated response mechanisms for suspected potential threats • Continuous real-time access reviews occur automatically with advanced A.I. Recommendations to optimise access and ensure compliance
Risk Management	Internal Risk Assessment Risk Mitigation External/Third-party Conducted Risk Assessment	• Inconsistent, informal, unstructured, risk assessment plan with little to no detail on planning • Unstructured risk mitigation with ad-hoc method of response to identified issues • Rarely, if ever, conducted Third-party Risk Assessments	• Periodically conducted risk assessments but missing consistency and detail • Basic risk mitigation process in place but only focused on mitigating the critical issues identified • Occasional third-party risk assessments but only for regulatory compliance's sake	• Regularly conducted and documented internal risk assessment with a set standard and methodology being followed • Structured and well documented risk mitigation that covers different risks and how to prioritise different categories of risks • Third-Party Risk Assessment are conducted to identify additional risks and confirm internal risk assessment findings	• In-Depth and extensive internal risk assessment conducted with proactive approach to risk mitigation • Cost-benefit analysis conducted to make sure the risks mitigated work well with the company's overall budget and financial status • Utilising the MITRE ATT&CK FRAMEWORK to categorise potential threats improving overall risk assessments conducted • Comprehensive third-party risk assessment conducted periodically alongside and after the internal risk assessment.	• Continuous risk assessments conducted with predictive analysis for emerging risks using artificial Intelligence or SAAS solutions. • Fully optimized and adaptable risk mitigation processes that is continuously improved based on response given back • Regular, collaborative partnerships with third-party assessors to ensure holistic and innovative approaches to risk management.
Asset Management	Inventory of Assets Asset Categorization Asset Lifecycle Management Asset Setup & Configuration	• Limited or no formal inventory asset management policy, asset tracking & management is manual, incomplete, or inconsistent. • Assets are not categorized based on sensitivity; categorization is absent. • No structured asset management lifecycle process, assets are managed reactively. • Minimal to no documentation defined, setup and configurations are limited or incomplete.	• Basic inventory is established but may not be detailed or comprehensive, may not be regularly kept up to date. • Some categorization exists, often based on general guidelines. • Lifecycle management exists but is inconsistently applied and only critical assets have a defined process in place. • Basic asset inventory configuration standards are in place but are not always maintained or enforced.	• A formal, well-defined and comprehensive inventory process is in place and updated regularly. • Assets are categorized based on a set of defined criteria (sensitivity, criticality, etc.) with a consistent process. • A structured process for the asset lifecycle management is documented and followed for most assets with employees aware of it. • Configuration standards are defined, documented, and enforced for the most critical assets.	• Near real-time inventory tracking with automation tools • Inventory is regularly audited internally and third-party . • Assets are consistently categorized using automated tools • Categorization aligns with organizational risk assessments and organizations business objectives. • A detailed and comprehensive lifecycle management process includes maintenance, and disposal strategies in place as well as asset replacement. • A defined baseline for configuration is defined, enforced and monitored for compliance with advanced logging in place.	• Asset and inventory management is entirely automated, with continuous tracking and logging. • Categorization is on a dynamic basis, adjusted based on context-driven factors, with periodic re-evaluation for accuracy and improvement. • Lifecycle management is carefully optimized with predictable analytics to anticipate asset needs and automate asset replacement or upgrades. • Automated configuration management system that ensures consistent setup and monitoring for automatic remediation wherever possible.
Security Awareness & Training	Security Awareness Employee Training Simulated Scam/Phishing Campaign	• No structured or well-defined security awareness training , employees receive very little to no guidance on security best practices • No simulated phishing campaigns conducted; employees are unaware of the risks of phishing attacks	• Basic security awareness training is conducted, covering basic and fundamental security concepts, but participation is optional and inconsistent. • Phishing simulations are conducted, but results are not used to improve training.	• Formal security awareness training program is established, with periodic sessions and mandatory attendance for all employees. • Regular simulated phishing campaigns are conducted, with feedback provided to employees who fall victim for phishing attempts.	• Security awareness training includes various content for different roles, employee completion rate is tracked. • Phishing simulation results are analysed, and targeted training is provided to employees who fail simulations, with added metrics to measure improvement.	• Continuous security awareness training based on current threats and trends, with a focus on fostering a security-first culture. • Phishing simulations are customized and aligned with emerging threats, with automated feedback and gamified elements to encourage engagement.
Business Continuity & Disaster Recovery	Disaster Recovery plan Business Continuity plan Backup management BC & DR Resilience Test	• No clearly defined disaster recovery plan • Business continuity planning is minimal or non-existent • Backup management is non-existent. • No resilience testing being conducted for BC and DR	• Basic disaster recovery plan is documented, but missing detail and is rarely, if ever reviewed. • Business continuity plan is under development but lacks clear set of procedures and scope. • Backup management is created btu no validation of data being backed up and no clear backup schedule defined. • BC and DR resilience tests are occasionally conducted but are minor in terms of scope.	• A clear and formal disaster recovery plan is established, with procedures for critical systems regular review of the plan, Cold, Hot, and Warm sites are defined. • Business continuity plan is clearly documented and includes prioritized recovery strategy with activation of cold and hot sites as needed. • Backup management plan is clearly defined and conducted, with regular backups for critical systems and backup is regularly validated. • Regular BC and DR resilience tests are conducted, with clearly documented results.	• Disaster recovery plan is continuously updated based on gathered metrics and previous incident history. • Business continuity plan includes risk assessments being conducted with a clear set of standard predefined responses for different scenarios. • Backup management metrics are monitored, with backups integrity validated and compliance with recovery point objectives (RPO). • Detailed and comprehensive resilience tests are performed, including failover drills and recovery time objective (RTO) validation.	• Disaster recovery plan is fully integrated with business operations, using real-time updates and automation for adaptive response. • Business continuity plan is continuously refined with predictive analytics and scenario planning for enhanced resilience. • Backup management is automated and continuously monitored, with advanced capabilities for rapid recovery and minimal data loss. • BC and DR resilience tests are dynamic, using simulated real-world events, and recovery strategies are optimized based on test outcomes.

[REDACTED COMPANY] IT Governance

The Importance of IT Governance in [REDACTED COMPANY]

IT governance allows an organization or company to maintain and ensure its efficient and safe use of information technology to allow it to contribute to the overall objectives that the company has. [REDACTED] is a global food and accommodation company, so the main criticality lies in maintaining the confidentiality, integrity, and availability of the data that is handled by the company and its associated partners.

Information technology is a crucial aspect for [REDACTED] as stated by their information security policy, they must comply with PCI-DSS to handle, store, and manage digital card security of their customers and ISO 27001.

[REDACTED COMPANY]'s IT governance supports the overall business objectives by having set procedures for Disaster Recovery Plan, Business Continuity Plan, Risk Management Plan, Auditing & Compliance Plan, Third-Party Management Plan, etc.

A company as big as **[REDACTED]** would have a vast scope of triggers for its IT Governance including constant regular compliance of an international law such as GDPR (General Data Protection Regulation) since it has hotels in the EU (European Union) and this includes hotels in Germany, Italy, Portugal, etc. The need to constantly make sure that all countries and all regions cross-comply with the information security policy and the protection against cyber threats to the business. Having to adhere and implement global standards like ISO 27001 and GDPR with the many countries and regions with the challenge that each country must comply with its local regulations. This may lead to the over-consumption of company resources and overall cost implications.

The effect of IT Governance on ISM at [REDACTED COMPANY]

IT governance plays a crucial role in [REDACTED COMPANY] information security management processes and policies as it is used to align the ISM objectives with [REDACTED COMPANY] business goals and ensure that security measures implemented and discussed support the organizations overall strategic business objectives.

Various IT governance frameworks that exist such as ISO/IEC 27001 Information Security Management Systems (ISMS), and NIST (National Institute of Standards and Technology) help promote continuous improvements for [REDACTED] by ensuring structured security practices are followed consistently.

At [REDACTED COMPANY], The IT governance structured in the information security policy clearly aligns with the ISO standard specifically the ISO 27001 information security management. It also reiterates regular compliance and stakeholder /investors engagement through a dedicated cybersecurity committee which ensures consistent compliance with ISO27001 governance framework.

Detailed Critique of [REDACTED COMPANY] Information Security Policy

Based on a detailed and comprehensive review of the information security policy that was last approved by the board of directors on 18th of October 2023, the policy is well written in some respects but is missing and overlooked some key aspects that should be included in a global information security policy. The following section introduces headings and a following description for each missing criteria that has been identified as missing, unclear or have been overall overlooked from being mentioned in the information security policy.

Violation of Information Security Policy

The policy that **[REDACTED COMPANY]** created does not have any claim of any repercussions or consequences that happen to employees or third parties for breaching this policy of not adhering to it.

Absence of mention of gap analysis to assess the security frameworks mentioned (ISO27001, ISO27002, PCI-DSS)

[REDACTED COMPANY] did not mention in their policy that a gap analysis is conducted to assess the following security frameworks that they are compliant with, a gap analysis is necessary to identify the areas of weakness to stay compliant with the appropriate controls of the security frameworks mentioned in the information security policy.

Absence of continuous security audit being conducted

[REDACTED COMPANY] claim that they are PCI-DSS compliant and while this may be the case, since [REDACTED] is classed as a level 1 merchant due to processing more than 6 million card transactions every year they are required to conduct an **annual on-site audit** by a qualified security assessor (**QSA**), **quarterly network scans**, and **continuous monitoring**. The information security policy does not mention that **[REDACTED COMPANY]** Does this to stay compliant with PCI-DSS security framework.

Absence of asset management policy

While the classification of information is in terms of its criticality, impact of their loss, and makes a good overall structure for classifying information it does not mention following a dedicated asset management policy for classifying information.

Absence of Disaster Recovery Plan

In section 'm' in the information security policy, it mentions "...recovery of critical information for **[REDACTED]** in the event of a disaster" but does not explicitly mention a disaster recovery plan in place for the company. There is also no mention of a defined cold, warm, or hot sites to speed up the disaster recovery process in the event of a disaster occurring.

Absence of secure destruction in documentary management section

The documentary management section of the information security policy mention "establishing a methodology for the preparation, labelling, management, and control of all corporate

documentation" but does not mention secure destruction of said corporate documentation or references a document management standard that should be followed.

Absence of backup copies frequency and secure storage

The section in the information security policy with heading back-up copies mentions that the backed-up data must have a minimum the same security measure as the original but does not specify the exact security measures for the type of data backed up, how frequent the backed-up data should be done, or mention secure storage of the said backed-up data. It also does not refer a backup standard.

Absence of access control model being used

Under the access management section of the information security policy, there is no clear mention of which access control model is being used from Rule-Based Access Control (RUBAC) or is it all based on a basic access control model like Discretionary access control (DAC) as different access control models have different pros and cons to them.

Absence of phishing simulations being conducted as part of security awareness

The information security policy mentioned that "all members of the organisation will be promoted" not that it is mandated for all employees to undertake and attend these sessions and there is no mention of a phishing simulation being conducted as part of the security awareness training that the company conducts.

Absence of mechanisms to prohibit unauthorized installations or unattended workstations

The policy mentions that the company will prohibit the installation of IT assets but does not explicitly mention any mechanisms in place to prohibit said IT assets, and the policy only mentions IT assets not software or any other form of asset on the network.

Absence of Incident Response Plan

The information security policy is missing any mention of an incident response plan being made and followed in the event of an incident occurring, an information security team should be assigned to handle incidents and follow through an incident response plan but the information security policy does not mention any of this.

Template for Information Security Policy

1. **Introduction**
   Purpose, scope, objectives, definitions, roles & responsibilities and a mention of violation of policy
2. **Policy Objectives**
   Align with company's business objectives and maintains Confidentiality, Integrity, Availability (CIA Triad)
3. **Information classification**
   Asset management standard to be followed including data classification levels and handling practices
   - Control Example: DLP (Data Loss Prevention) system / solution
4. **Compliance, Audits, standards & Policy**
   GDPR, Data Protection Act (2018), ISO27001/27002, NIST, Internal & External Audits
   - Control Example: Deploy a compliance management tool such as Qualys
5. **Acceptable Use Policy**
   Establishes clear guidelines for using company assets.
   - Control Example: deploy a web proxy server to limit access to certain categories of websites
6. **Business continuity & disaster recovery policy**
   Establishes a policy to outline continued operations during incidents
   - Control Example: Implement a DRaaS (Disaster Recovery as a Service) solution such as AWS Elastic Disaster Recovery
7. **BYOD & MDM policy**
   A policy to specify the rules for mobile device management and bringing your own device to the company.
   - Control Example: implement a solution like Microsoft Intune to be able to remotely wipe and monitor activity
8. **Password policy**
   A policy to define password complexity, expiration date & time, length, and usage
9. **Incident Response Policy**
   Defines a set procedure for detecting, responding and recovering from an incident with dedicated team to handle it
   - Control Example: implement a solution like Splunk SOAR to automate detection, response, and reporting of alerted security incidents
10. **Data retention and disposal policy**
    A high-level policy of a standard that explains how long to retain and how to safely dispose of information of all kinds of sensitivity
11. **Backup & recovery policy**
    This policy covers backup frequency, location, and restoration procedures
    - Control Example: Implement an automated backup and recovery solution like Acronis to perform / schedule automated backups
12. **Security Measures**
    - **12.1. Authorized User Access**
    - **12.2. Physical Security Measures**
    - **12.3. Unattended Workstations**
    - **12.4. Auditing and Compliance**
    - **12.5. Communications Security and Monitoring**

[REDACTED COMPANY] Risk Assessment

Based on the assessed information security policy, a risk assessment has been carried out and the results has been displayed in the risk register table below followed by the specific ISO 27001 and PCI-DSS controls to remediate the associated risks.

Risk Scale	Classification
1-5	Low
6-10	Medium
11-15	High
16-20	Very High
21-25	Severe

Risk	Description	Likelihood (1-5)	Impact (1-5)	Risk Rating (1-25)	ISO27001 Controls (2013)	PCI-DSS Controls (v3.2.1)
Unauthorised access	Any individual that gains access without the relevant permission or access being granted	Medium (3)	Severe (5)	15 (High)	A.9.1.1 Access control policy	7.1.1 Limit access to system components and cardholder data based on job responsibilities
Data Breach	Loss, theft, or exposure of sensitive data	Medium (3)	Severe (5)	15 (High)	A.16.1.1 Responsibilities and procedures	12.8.1 Maintain a policy that addresses information security for employees and contractors
Legal non-compliance	Failure to comply with legal or regulatory compliance	Medium (3)	Severe (5)	15 (High)	A.18.1.1 Identification of applicable legislation and contractual requirements	12.8.1 Maintain a policy that addresses information security for employees and contractors
Phishing attack	A social-engineering attack that tricks victims into sharing sensitive or personal information	High (4)	High (4)	16 (Very High)	A.7.2.2 Information security awareness, education, and training	4.1 Use strong cryptography and security protocols to protect sensitive information during transmission over open, public networks
Wi-Fi security flaws	Exploitation of insecure Wi-Fi configuration like WPA2 misconfiguration or a social-engineering Wi-Fi attack like evil twin attack	Severe (5)	Medium (3)	15 (High)	A.13.1.1 Network controls	4.1 Use strong cryptography and security protocols to protect sensitive information during transmission over open, public networks
Ransomware attack	Malware that encrypts sensitive information and systems and demands payment to be given the key for decryption	Medium (3)	Severe (5)	15 (High)	A.17.1.1 Planning information security continuity	12.10.1 Implement an incident response plan
Insider Threat / Disgruntled Employees	Employees that have been let go or fired and have not lost access to company resources so they use it for malicious intent	Low (2)	Severe (5)	10 (Medium)	A.7.3.1 Termination or change of employment responsibilities	7.1.4 Assign access based on individual personnel's job classification and function
Supply Chain Risks	Security risks posed by third-party vendors or supplies	Medium (3)	Medium (3)	9 (Medium)	A.15.1.1 Information security policy for supplier relationships	12.8.5 Maintain a program to monitor service providers' PCI DSS compliance status
Physical Security Risks	Unauthorized physical access into buildings, rooms, or secure areas	Low (2)	Low (2)	4 (Low)	A.11.1.1 Physical Security Perimeter	9.1.1 Use appropriate facility entry controls to limit and monitor physical access to systems
Cloud Misconfigurations	vulnerabilities arising due to misconfigurations in cloud environment	Medium (3)	Severe (5)	15 (High)	A.13.1.3 Segregation in networks	12.10.5 Include alerts from security monitoring systems in the incident response
Unpatched Vulnerabilities	Known vulnerabilities that have not been patched yet	Severe (5)	Severe (5)	25 (Severe)	A.12.6.1 Management of technical vulnerabilities	6.2.1 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches
Lack of security training	Employees not trained or unaware of security best practices	Medium (3)	Medium (3)	9 (Medium)	A.7.2.2 Information security awareness, education, and training	12.6.1 Implement a formal security awareness program
IT Downtime / Outage	Hardware failure that leads to unexpected availability of systems	Medium (3)	Medium (3)	9 (Medium)	A.17.2.1 Availability of information processing facilities	10.5.1 Implement procedures to back up critical data
Disaster Recovery Gaps	Missing gaps in disaster recovery plan that leads to longer downtime and recovery time	Low (2)	Low (2)	4 (Low)	A.17.2.1 Availability of information processing facilities	10.5.1 Implement procedures to back up critical data
Weak Password Policy	Weak passwords increase the speed and chances of passwords being cracked and compromised	Severe (5)	Severe (5)	25 (Severe)	A.9.4.3 Password management system	8.2.3 Passwords/phrases must meet minimum security requirements
Data Exfiltration	Unauthorized transfer of information without proper approval to outside the organization	Medium (3)	Medium (3)	15 (High)	A.13.2.1 Information transfer policies and procedures	11.4.1 Implement intrusion-detection and/or intrusion-prevention techniques
Advanced Persistent Threats (APTs)	Highly sophisticated cyberattack performed by skilled threat actors	Medium (3)	Severe (5)	15 (High)	A.16.1.5 Response to information security incidents	12.10.1 Implement an incident response plan
Zero-Day vulnerabilities/exploits	Vulnerabilities without publicly released patches being exploited	Low (2)	Severe (5)	10 (Medium)	A.16.1.5 Response to information security incidents	6.2.1 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches

Conclusion

In conclusion, the report provides a deep insight into **[REDACTED COMPANY]** and its establishment, it explains how IT governance is important to the organization and its effects of the information technology infrastructure. Finally, the report presents a template/outline for an information security policy with a short description and example controls alongside a carefully designed maturity model.

References

[REFERENCES HAVE BEEN REMOVED FROM THIS DOCUMENT TO PROTECT THE COMPANY'S SECURITY]

Wikipedia Contributors (2019). Capability Maturity Model Integration. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration.