

SLT-Mobitel Nebula Institute of Technology
Pearson BTEC Level 5 Higher National Diploma in Digital Technologies (RQF)

Assignment Brief

Programme Title	Pearson BTEC Level 5 Higher National Diploma in Digital Technologies (RQF)
Student Name/ID Number	D Sandeepa Munasingha (DT/MF/2023/B01/06)
Unit Number and Title	Unit 08 Security
Academic Year	2024/2025
Unit Tutor	Priyalukshmy Jeyakumar
Assignment Title	Assignment 1
Issue Date	2024/11/04
Submission Date	2024/11/18
Submission Format	
<p>The submission is in the form of an individual written report and a PowerPoint Presentation. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system.</p> <p>Please also provide an end list of references using the Harvard referencing system.</p>	
Unit Learning Outcomes	
<p>LO1 Assess risks to IT security.</p> <p>LO2 Describe IT security solutions.</p> <p>LO3 Review mechanisms to control organisational IT security.</p> <p>LO4 Manage organisational security.</p>	
Vocational scenario	

EMC Cloud Solutions is reputed as the nation's most reliable Cloud solution provider in Sri Lanka. A number of high-profile businesses in Sri Lanka including Nebula Institute of Technology network, SME Bank Sri Lanka and WEEFM are facilitated by EMC Cloud Solutions. EMC Cloud provides nearly 500 of its customers with SaaS, PaaS & IaaS solutions with high-capacity compute and storage options. Also, EMC is a selected contractor for Sri Lanka, The Ministry of Defence for hosting government and defence systems. EMC's central data centre facility is located at Colombo Sri Lanka along with its corporate head-office in Colombo. It has a six-story building with

- First floor dedicated to sales and customer services equipped with public Wi-Fi facility
- Second-floor hosts HR, Finance and Training & Development departments
- third-floor hosts boardroom and offices for senior executives along with the IT and

Data center department.

- Floor 4,5,6 hosts computer servers which make up the data center.

With the rapid growth of information technology in Kandy area in recent years, EMC seeks opportunity to extend its services to Kandy, Sri Lanka. As of yet, the organization still considers the nature of such extension with what to implement, where is the suitable location and other essential options such as security are actually being discussed. You are hired by the management of EMC Solutions as a Security Expert to evaluate the security-related specifics of its present system and provide recommendations on security and reliability related improvements of its present system as well as to plan the establishment of the extension on a solid security foundation.

Assignment activity and guidance

Assuming the role of Trainee External Security Consultant, you need to compile a comprehensive report and presentation delivery to the Management of EMC Cloud Solutions;

For the report you have to focus on following elements

Activity 01

1.1 Identify types of security risks EMC Cloud is subject to, in its present setup and the impact, such issues would create on the business itself.

1.2 Develop and describe security procedures for EMC Cloud to minimize the impact of issues discussed in section (1.1) by assessing and treating the risks.

1.3 Analyze the benefits of implementing network monitoring systems with supporting reasons collaborated with EMC cloud solutions.

Activity 02

2.1 Discuss how EMC Cloud and its clients will be impacted by improper/ incorrect configurations which are applicable to firewall policies and and VPN solutions.

2.2 Explain with examples how following technologies would benefit EMC Cloud and its Clients by facilitating a 'trusted network'. (Support your answer with suitable illustrations). i) DMZ ii) Static IP iii) NAT

2.3 Propose a method to assess and treat IT security risks that you mentioned above. Further evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of EMC organisation's IT security.

Activity 03

3.1 Formulate a suitable risk assessment procedure for EMC Cloud solutions to safeguard itself and its clients.

3.2 Explain the mandatory data protection laws and procedures which will be applied to data storage solutions provided by EMC Cloud. You may also highlight on ISO 3100 risk management methodology.

Here you have to summarise an appropriate risk management approach or ISO standard and its application in IT security of EMC security solutions, and analyse possible impacts to organisational security resulting from an IT security audit.

3.3 You have to recommend how IT security can be aligned with an EMC organisational policy, detailing the security impact of any misalignment.

Activity 04

Your presentation should focus on design and evaluation of organisational security management policy

4.1 Develop a security policy for EMC Cloud to minimize exploitations and misuses while evaluating the suitability of the tools used in an organizational policy.

4.2 Develop a disaster recovery plan including all the key components, for EMC Cloud to ensure maximum uptime for its customers. Justifications and reasons for decisions and options used. Evaluate the suitability of the tools used in the organisational policy to meet business needs.

4.3 Identify the stakeholders of the organization and discuss the role of them by implementing the security audit.

Recommended Resources

Please note that the resources listed are examples for you to use as a starting point in your research – the list is not definitive.

Textbooks

Alexander, D. et al. (2020) Information Security Management Principles. BSC.

Collins, R. (2017) Network Security Monitoring: Basics for Beginners.

A Practical Guide CreateSpace Independent Publishing Platform. Sanders, C. Smith, J.

(2013) Applied Network Security Monitoring: Collection, Detection, and Analysis. Syngress. Steinberg, R. (2011)

Governance, Risk Management, and Compliance: It Can't Happen to Us – Avoiding Corporate Disaster While Driving Success.

Wiley. Tipton, H. (2010) Information Security Management Handbook. 4th edn. Auerbach Publications.

Web www.bcs.org

www.bsa.org

www.fast.org.uk

www.ico.org.uk

Links BCS, The Chartered Institute for IT (General Reference) Software Alliance (General Reference) Federation

Against Software Theft (General Reference) Information Commissioners Office (General Reference)

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Assess risks to IT security		LO1 and LO2 D1 Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
P1 Discuss types of security risks to organisations. supporting reasons. P2 Assess organizational security procedures.	M1 Analyze the benefits of implementing network monitoring systems with	
LO2 Describe IT security solutions		
P3 Discuss the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs. P4 Discuss, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve network security.	M2 Propose a method to assess and treat IT security risks.	

Pass	Merit	Distinction
LO3 Review mechanisms to control organisational IT security		D2 Recommend how IT security can be aligned with an organisational policy, detailing the security impact of any misalignment.
<p>P5 Review risk assessment procedures risk in an organisation. approach or ISO</p> <p>P6 Explain data IT security. processes as applicable to an organisation.</p> <p>M4 Analyze possible</p>	<p>appropriate management standard and its protection application in and regulations</p> <p>impacts to organisational security resulting from an IT security audit.</p>	
LO4 Manage organisational security		D3 Evaluate the suitability of the tools used in the organisational policy to meet business needs.
<p>P7 Design a suitable security policy for an organisation, including the main components of an organisational disaster recovery plan.</p> <p>P8 Discuss the roles of stakeholders in the organisation in implementing security audits.</p>	<p>M5 Justify the security plan developed giving reasons for the elements selected.</p>	

BTEC HN Assignment Brief Template
Issue Date: Jan 2024 Owner: HN QD
DCL1 Public (Unclassified) Version 2.0

Security

D Sandeepa Munasingha

Introduction

In today's digital age, the rapid expansion of cloud computing and data services has made cybersecurity a critical focus for service providers. EMC Cloud Solutions, one of Sri Lanka's most reliable cloud providers, has become essential for several high-profile clients, including educational institutions, financial organizations, and government agencies. The company offers a full range of cloud-based solutions, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), designed to meet high demands for computational power, storage, and reliability. This suite of services positions EMC Cloud as a significant contributor to digital infrastructure within Sri Lanka.

However, with the rise in cyber threats and an expansion plan to Kandy, EMC Cloud must re-evaluate its current security architecture and protocols to safeguard its reputation, maintain client trust, and prevent potential disruptions. As the appointed Security Expert, this report will identify the critical security risks facing EMC's current setup, evaluate strategies to mitigate these risks, and propose security measures that can provide a robust foundation for the company's planned expansion.

The report is structured into three main activities. The first activity focuses on assessing security risks within EMC's current setup and recommending security procedures to mitigate these risks. The second activity examines the implications of firewall and VPN configurations on the network's reliability and explores specific technologies like DMZ, Static IP, and NAT that can help establish a trusted network. The third activity formulates a risk assessment procedure, discusses data protection laws relevant to EMC's cloud storage solutions, and suggests methods to align IT security with the organization's policy.

Through these analyses and recommendations, this assignment seeks to establish a comprehensive security strategy for EMC Cloud, addressing both current and anticipated risks, and setting a solid security framework for future growth.

Activity 01

1.1 Identify types of security risks EMC Cloud is subject to, in its present setup and the impact, such issues would create on the business itself.

Data Breaches and Unauthorized Access

Risk

- The data center stores important information for major clients, including government and defense systems. Unauthorized access or data leaks can happen due to poor access control, threats from insiders, or cyber-attacks from outside.

Impact

- A data leak could lead to stolen customer information, harm to the company's reputation, loss of government contracts, and possible fines from regulators, especially when dealing with defense and government data. This could reduce customer trust, hurt future business opportunities, and cause expensive legal issues.

Physical Security Risks

Risk

- EMC's Colombo data center has several floors with important IT and server equipment, making it easy for someone to break in, steal things, or cause damage. Weak security, like not checking who comes in, not having cameras, or not following proper safety rules, could let unauthorized people get inside.

Impact

- If someone gets in physically, they could steal data, damage important equipment, or cause the services to stop working. If the systems are physically tampered with, it could interrupt services, result in data loss, and cost a lot to fix, affecting both the business and its customers.

DDoS (Distributed Denial of Service) Attacks

Risk

- As a cloud service provider, EMC is vulnerable to DDoS attacks that try to make its services unavailable. These attacks can be hard to stop and can overload servers, causing downtime for the SaaS, PaaS, and IaaS services it offers to clients.

Impact

- Downtime caused by DDoS attacks could result in lost business, unhappy clients, and financial losses due to not meeting service level agreements (SLAs). Repeated attacks might hurt EMC's reputation for reliability, affecting its ability to keep and attract clients.

Compliance and Regulatory Risks

Risk

- Working with data for government and defense systems means following strict rules. Not following rules like GDPR (for personal data) or local cybersecurity laws can cause legal problems, especially in defense.

Impact

- Not following these rules can lead to fines, legal actions, and harm to EMC's reputation. For a company handling sensitive government data, mistakes could mean losing contracts, affecting income and future government work opportunities.

1.2 Develop and describe security procedures for EMC Cloud to minimize the impact of issues discussed in section (1.1) by assessing and treating the risks.

Data Protection and Access Control

Procedure

- Set up role-based access control (RBAC) so that only people who need to see sensitive information can access it. Access should be given based on their job duties, and permissions should be checked and updated regularly.

Treatment

- Use multi-factor authentication (MFA) on all systems, especially those dealing with very important data (like government or defense info). This stops unauthorized access even if someone gets your login details. Keeping track of and watching access attempts can help quickly spot and deal with any unauthorized access.

Physical Security Enhancement

Procedure

- Improve physical security by setting up surveillance cameras, secure entry systems, and security guards at important entry points to watch who comes in. Protect server rooms with biometric or card-based access systems and use electronic records to keep track of who enters.

Treatment

- Regularly check physical security measures to find and fix any problems. Create emergency plans for physical security issues and train employees so they know what to do. Also, limit access to higher floors (where data centers are) to only authorized people.

DDoS Protection Measures

Procedure

- Utilize DDoS mitigation services, such as cloud-based DDoS protection from providers like Cloudflare or Akamai, which can filter and absorb DDoS traffic before it reaches EMC's network.

Treatment

- Establish a dedicated response team and a DDoS response plan that prioritizes traffic management and scalability options in case of an attack. Regularly stress-test the system to assess DDoS defenses and identify any vulnerabilities in infrastructure.

Compliance and Regulatory Adherence

Procedure

- Create a compliance management program with a specific person in charge of compliance, who will watch over how well we follow rules about handling defense, government, and personal data (like GDPR).

Treatment

- Do regular checks, both inside and outside the company, to make sure all our systems, rules, and ways of handling data meet the required rules. Make a list of things to check for compliance and a training plan for employees to keep them informed about their legal duties and data protection standards.

1.3 Analyze the benefits of implementing network monitoring systems with supporting reasons collaborated with EMC cloud solutions.

Network monitoring systems help detect unusual traffic patterns and potential threats in real-time, such as DDoS attacks or unauthorized access attempts. This allows EMC Cloud to identify and address security issues before they escalate into major problems. For example, if an attack starts overwhelming the network, the system can trigger alerts, enabling the security team to mitigate the threat immediately. This proactive approach helps prevent costly data breaches or service disruptions.

Continuous monitoring allows EMC Cloud to identify network congestion, bottlenecks, or slowdowns in real-time. For instance, if a server is receiving more requests than it can handle, the system can automatically redistribute the load or provide alerts to IT teams to take action. This optimization ensures that clients experience consistent, high-speed performance, which is crucial for a cloud service provider offering reliable services to businesses.

With network monitoring, EMC Cloud can track resource usage, such as bandwidth, storage, and server performance. This data helps in efficiently managing resources, ensuring that they are scaled up or down based on demand. For example, during peak usage times, the system can allocate additional bandwidth to high-demand services, ensuring minimal slowdowns. This improves cost efficiency and ensures resources are not overused or underutilized.

Real-time monitoring enables EMC Cloud to identify and resolve network issues promptly. For example, if a server fails or a network link goes down, the monitoring system immediately alerts IT staff, reducing downtime. This rapid detection and resolution process helps maintain service availability and minimize disruptions, which is vital for businesses that rely on EMC Cloud for critical operations.

Network monitoring can assist in ensuring that EMC Cloud complies with industry regulations and security standards. By tracking traffic and system activities, monitoring

tools can generate reports that help demonstrate compliance during audits, reducing the risk of legal or financial penalties.

Network monitoring systems offer EMC Cloud Solutions the ability to proactively manage security threats, optimize performance, efficiently allocate resources, resolve issues quickly, and ensure compliance. These benefits not only protect the company's infrastructure but also enhance customer satisfaction and trust, helping EMC Cloud maintain its reputation as a reliable service provider.

KEY FEATURES OF A NETWORK PERFORMANCE MONITORING SOLUTION



**Real-Time
Monitoring**



**Performance
Metrics**



**Security
Alerts**



**Data Theft
Prevention**



**Downtime
Detection**



Activity 02

2.1 Discuss how EMC Cloud and its clients will be impacted by improper/ incorrect configurations which are applicable to firewall policies and VPN solutions.

Improper or incorrect configurations in firewall policies and VPN solutions at EMC Cloud could seriously impact both EMC and its clients by exposing systems to various security threats

If firewalls or VPNs are not set up correctly, it could let unauthorized people access important data stored in EMC's data centers. This could put client information at risk for organizations like SME Bank or the Ministry of Defense, causing privacy issues and possible fines from authorities.

Problems with firewall settings, like open ports or too much access, can give attackers a way in, increasing the chance of malware getting in. Once a security problem happens, it could spread across client systems hosted on EMC's network, affecting the reliability of cloud services for clients in banking, education, and defense.

Service Interruptions: Mistakes in allowing or blocking traffic through firewalls can cause important services to stop working. This can disrupt business for clients who depend on EMC's cloud services like IaaS, PaaS, and SaaS, possibly leading to periods when their business can't run and causing financial harm.

Damage to Trust and Reputation: For a well-respected cloud provider, security issues related to configuration mistakes could seriously harm EMC's reputation. Major clients trust EMC for strong security; any problems in this area could cause clients to leave and make it harder to win new contracts.

2.2 Explain with examples how following technologies would benefit EMC Cloud and its Clients by facilitating a ‘trusted network’. (Support your answer with suitable illustrations).

DMZ (Demilitarized Zone)

A Demilitarized Zone, is a part of a network that separates an organization's public-facing services, like web servers and email servers, from its private internal network. It serves as a protective area between the internet and the internal network, helping to lower the risk of cyber threats by keeping external resources separate from sensitive internal systems.

Why It's Needed

- A DMZ stops direct access to an organization's private network, keeping important systems safe.
- Only certain services are allowed in the DMZ, and their access can be watched more carefully.
- Attackers are limited to servers in the DMZ, reducing the harm of any possible attacks.

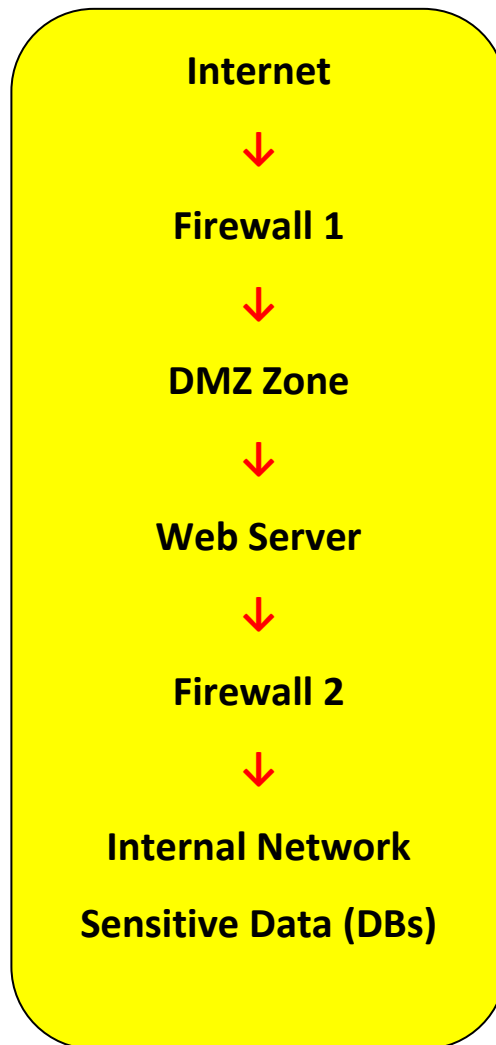
Application for EMC

In EMC Cloud, setting up a DMZ would involve placing publicly accessible applications (like customer portals or websites) in the DMZ area. This separates them from the internal network, ensuring that even if an attacker manages to breach the DMZ, they won't easily gain access to sensitive data or systems within the internal network.

Security Advantage

Enhanced protection by layering defenses, minimizing direct access to critical resources.

DMZ Diagram



How this works

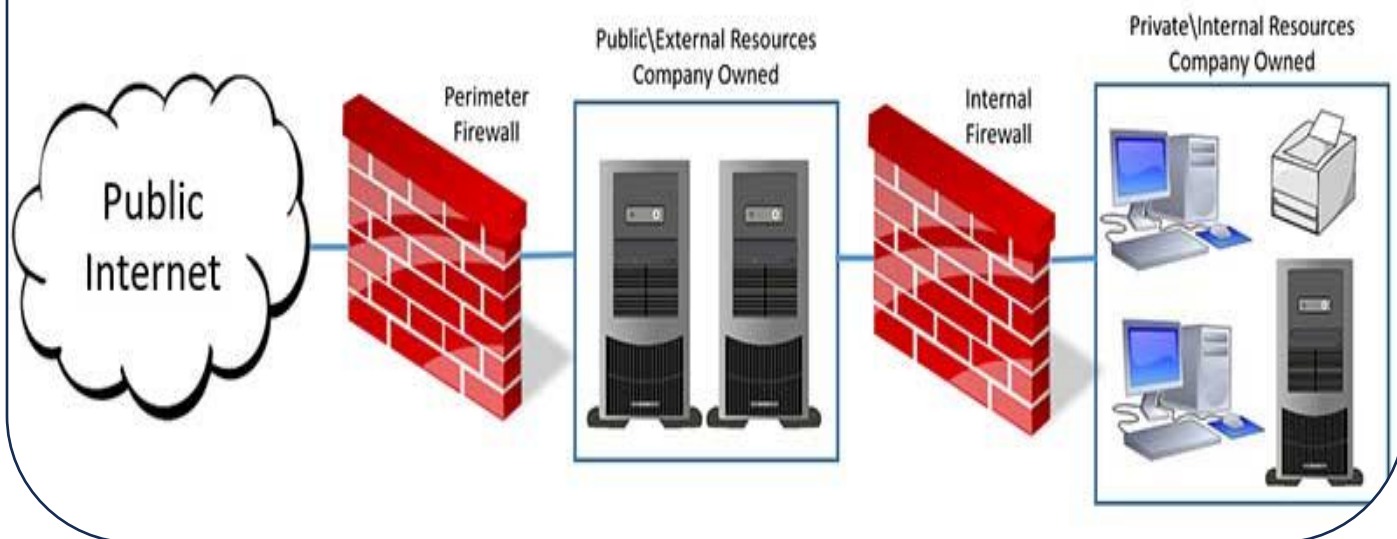
For EMC Cloud Solutions, the DMZ setup is crucial for protecting its network, especially since it works with important clients like the Ministry of Defense and big banks. The DMZ helps EMC keep public services separate from its private network, making sure that important data stays safe and protected from outside risks.

When internet requests arrive, they go through Firewall 1 first. This firewall blocks any unauthorized or potentially harmful traffic, only letting approved requests into the DMZ. Inside

the DMZ, EMC can put servers that are accessible to the public, like web servers. These servers allow clients to use services while keeping the company's important data separate. This setup stops attackers from getting into EMC's sensitive systems if there's a problem with the public servers. Firewall 2 adds another layer of protection, limiting access from the DMZ to the internal network, where very important resources, like databases for HR, finance, and critical government data, are kept.

By setting up a DMZ, EMC can safely offer its SaaS, PaaS, and IaaS services while keeping high security levels. This setup helps protect important data and ensures the privacy of sensitive client information. This multi-layered security method is important as EMC grows into Kandy, where it will need to use similar measures to safeguard both local and Colombo based assets.

DMZ (Demilitarized Zone)



2. Static IP

A Static IP is a permanent IP address assigned to a specific device or server, which remains unchanged over time. This is ideal for systems that require a consistent way to be accessed, such as web servers, VPNs, or email servers.

Why It's Needed

- Static IP addresses make it simpler to add trusted sources to a list, which helps in setting up access rules for clients and partners.
- Since the IP address remains the same, users and systems can always reach the services without any disruptions.
- Using static IPs for crucial services ensures that only specific, approved IP addresses can access them, preventing access from unknown or unauthorized sources.

Application for EMC

EMC Cloud can assign a fixed IP address to important servers, such as those offering SaaS, PaaS, and IaaS services to customers. This ensures stable connections and fewer access problems, since customers always know the exact IP address to use.

Security Advantage

Consistency in connections enhances accessibility and reduces potential disruptions from IP changes, which is critical for high-profile clients.

3. NAT (Network Address Translation)

Definition: NAT (Network Address Translation) is a technique that allows multiple devices on a private network to share a single public IP address for accessing the internet. NAT converts the private IP addresses of devices within the network to a public IP address, thereby hiding the internal network details from external sources.

Why It's Needed:

- NAT masks internal IP addresses, stopping direct access to devices on the network.
- NAT enables multiple devices to share one public IP, which is useful in networks with limited IP addresses.
- Because NAT uses a single public IP, it simplifies managing and tracking network traffic.

Application for EMC

With NAT, EMC Cloud allows several devices on its internal network to access external resources using just one public IP address. This keeps the private IP addresses of devices hidden, making it more difficult for outside sources to attack specific devices within the network.

Security Advantage

Enhances privacy by masking internal IPs, reducing the likelihood of targeted attacks on internal network devices.

2.3 Propose a method to assess and treat IT security risks that you mentioned above. Further evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of EMC organization's IT security.

Why IT Security is so important for EMC

IT security is extremely important for EMC Cloud Solutions because they handle very sensitive information, such as critical government and defense systems, and provide cloud services to important clients in areas like finance and education. Protecting this data is crucial to prevent unauthorized access, which could cause legal issues, harm their reputation, and result in major financial losses. EMC's clients trust the company to keep their information safe, so having a strong IT security system is essential to maintain that trust and keep EMC's reputation as a dependable cloud service provider.

Physical Security Measures

EMC Cloud Solutions can improve its physical security by using access control systems like biometrics and keycards, which only allow authorized people to enter. High-quality CCTV cameras with live monitoring help keep an eye on security, allowing quick action against unauthorized access. Environmental controls, like fire suppression and climate management systems, protect important IT equipment from fire and overheating. UPS systems ensure continuous power supply. Extra security measures, such as perimeter fencing and bollards around the data center, also help keep the area safe, preventing unauthorized access and protecting the physical infrastructure.

Virtual Security Measures

For online protection, EMC can use multiple layers of firewalls and Intrusion Detection Systems (IDS) to watch and secure network traffic. Data encryption for information stored and moving, along with Data Loss Prevention (DLP) tools, keeps sensitive data safe from unauthorized access. Virtual Private Networks (VPNs) allow secure remote access for employees, while network segmentation and DMZ setups separate different network parts, reducing the risk of cyber threats spreading. Strong Identity and Access Management (IAM) practices, including Role-Based Access Control (RBAC) and Privileged Access Management (PAM), limit access to important systems based on user roles. Regular checks, testing for vulnerabilities, and endpoint

security solutions further strengthen EMC's defense against possible cyber threats, ensuring compliance and creating a secure environment for client data and services.

Risk Assessment and Treatment Methods

To properly handle the IT security risks that EMC Cloud Solutions faces, it's important to use a clear method for assessing and managing these risks. This method starts with a detailed risk assessment, where EMC identifies and lists its key assets, like data centers, customer data, and network systems. For each asset, EMC should look at weaknesses, such as old software or poor access controls, and consider possible dangers, including data leaks, insider threats, and physical break-ins. By giving each risk, a score for how likely it is to happen and how bad it could be, EMC can decide which threats need quick action. This helps EMC create a risk chart that sorts these risks by how serious they are.

After identifying and prioritizing risks, specific strategies are used to handle them. Actions like improving access controls and dividing networks into smaller parts help lower the chances or effects of certain threats. EMC can also transfer some risks by using services that protect against DDoS attacks or by getting cyber insurance, which reduces the impact if these risks happen. For very high-risk areas that are expensive or difficult to protect, avoiding the risk—such as limiting access to important physical places—might be the best solution. Lower-priority risks can be watched over time, allowing EMC to save resources while staying alert.

Risk	Description	Treatment	After Treatment Result
Data Breaches	Unauthorized access to sensitive client or internal data, potentially leading to data theft or exposure.	Implement strong access controls, encryption for data at rest and in transit, and multi-factor authentication (MFA).	Reduced likelihood of unauthorized access, with data protected even if intercepted.
Insider Threats	Malicious or negligent actions by employees leading to data leaks or system compromise.	Employ access management (principle of least privilege), conduct background checks, and implement activity monitoring.	Minimized insider risk, with limited access and real-time monitoring of sensitive activities.

Physical Intrusions	Unauthorized physical access to critical areas, risking data or equipment tampering.	Use biometric or card-based access controls, surveillance cameras, and physical barriers (e.g., reinforced doors).	Restricted access to sensitive areas, deterring unauthorized physical access and reducing tampering risks.
Malware and Ransomware Attacks	Infection of systems by malicious software, potentially resulting in data encryption, theft, or system downtime.	Deploy firewalls, antivirus software, IDS/IPS, and conduct regular software updates and vulnerability scanning.	Enhanced system defenses, reducing malware infection rates and enabling quicker threat detection and removal.
Distributed Denial of Service (DDoS)	Overwhelming network traffic disrupting services, impacting client operations and reputation.	Use DDoS protection services to absorb and mitigate attacks.	Reduced service interruptions, with attacks mitigated before affecting client access.



Activity 03

3.1 Formulate a suitable risk assessment procedure for EMC Cloud solutions to safeguard itself and its clients.

Risk Assessment Procedure



To protect itself and its clients, EMC Cloud Solutions should use a complete security plan. This plan should include setting up strong access controls, like multi-factor authentication and role-based permissions, to keep important data safe. Encrypting data while it's being sent and when it's stored ensures that the information stays secure, even if someone tries to access it without permission.

Checking for weaknesses and testing the system regularly are important to find any problems in the infrastructure. This lets EMC fix potential threats before they become a big issue. Using systems that detect and stop intrusions (IDPS) helps monitor the system in real-time, alerting the security team to any unusual activity so they can act quickly.

Physical security measures, such as controlled access to data centers, 24/7 surveillance, and fire suppression systems, help protect hardware from physical threats. Additionally, employee training on security best practices is essential to reduce risks from human error or insider threats.

Risk management strategies involve reducing risks (like using firewalls and limiting access), transferring them (through insurance or outsourcing), avoiding them, and accepting them. Specific teams are responsible for each strategy. Ongoing monitoring, audits, and regular checks ensure that controls work well. Clear documentation and communication keep everyone updated.

Disaster recovery and business continuity planning should be in place, with regular backups and a clear incident response plan to minimize downtime and protect client data in case of an emergency. By combining these measures, EMC can effectively protect its systems and maintain client trust.



3.2 Explain the mandatory data protection laws and procedures which will be applied to data storage solutions provided by EMC Cloud. You may also highlight on ISO 3100 risk management methodology.

Data protection includes steps like classifying data, encrypting it, controlling who can access it, backing it up, minimizing the amount of data collected, anonymizing it, and having a plan for dealing with problems. Rules like the GDPR, CCPA, HIPAA, and PCI DSS tell us how to gather, store, and use personal data. Important rules include giving people access to their data, telling them if there's a problem, and letting them delete their data. Companies need a Data Protection Officer (DPO), regular checks, and training for employees. Not following these rules can lead to big fines and harm to the company's reputation, so it's important to follow the laws and do the right thing when handling data.

To safeguard client information and meet legal requirements, EMC Cloud needs to follow various data protection rules and processes. One important rule is the General Data Protection Regulation (GDPR), especially if EMC Cloud works with clients from the European Union (EU). The GDPR requires strong data protection steps, such as getting consent for data collection, allowing clients to access their data, and having strict plans for handling data breaches, with significant penalties for not following the rules.

Sri Lanka's Personal Data Protection Act is similar to the GDPR and sets clear rules for legal data processing, transparency, and security measures. This makes it crucial for EMC Cloud to include these protections in its operations. If EMC Cloud deals with healthcare data, it must also comply with HIPAA regulations, which demand controls to ensure the confidentiality, integrity, and availability of protected health information (PHI).

To support compliance with these laws, EMC can implement the ISO 31000 risk management methodology. ISO 31000 offers a structured approach for identifying, assessing, and treating risks, providing a flexible framework that EMC can adapt to its specific IT security needs. This standard guides EMC in establishing clear processes to analyze security risks related to data storage solutions, with an emphasis on continuous improvement and adaptability. Through this methodology, EMC can systematically address security risks in areas such as data access, encryption, and physical safeguards in its data centers.

Using ISO 31000 in EMC's data protection methods improves resilience and compliance by promoting regular risk evaluations and updates to address new threats. This systematic approach ensures that EMC Cloud not only complies with legal data protection rules but also matches industry security standards, enhancing overall data integrity and customer trust.

ISO standard and its application in IT security of EMC security solutions

Adopting the ISO standard, particularly ISO/IEC 27001, in IT security at EMC Cloud Solutions will aid in creating a strong Information Security Management System (ISMS). ISO/IEC 27001 offers a structured method for handling confidential information, guaranteeing its protection, and covers both physical and digital assets. Below is a detailed plan for integrating ISO 27001 at EMC and how it can enhance its IT security.

Establishing an Information Security Management System Framework

EMC can begin by creating an ISMS framework that matches the structure and requirements of ISO 27001. This includes establishing clear information security goals, determining which important business areas (like SaaS, PaaS, and IaaS services) the ISMS will cover, and assigning roles and responsibilities throughout the company. This framework serves as the base for security measures and policies, tailored to meet the needs of EMC's cloud and data center operations.

Risk Assessment and Treatment

ISO 27001 focuses on ongoing risk evaluation and management. At EMC, this means finding, studying, and judging risks linked to data leaks, unauthorized entry, system weaknesses, and meeting rules. After looking at these risks, EMC can handle them by using ISO-approved methods. For example:

Data Protection and Access Limits: Use encryption to keep data safe when it's stored and when it's moving. Only let certain people access important systems and data, and make sure they need more than one way to prove who they are.

Regular Checks for Weak Spots and Testing: These helps find and fix possible problems in EMC's cloud services, apps, and network.

Implementing ISO Controls and Policies

ISO 27001 outlines controls in various areas such as access control, physical security, data integrity, and incident management. EMC can apply these controls according to the standard's Annex A, which covers

Access Control Policy: Determine who has permission to access certain data and under which conditions. This is especially important for data center areas, where limited access ensures that only authorized individuals can enter.

Data Classification and Handling: Set up clear rules for classifying and managing data to make sure sensitive customer and government information is properly secured.

Incident Management Procedures: Develop a written plan for responding to security incidents quickly, including steps for containing the issue, resolving it, and reporting it.

Employee Training and Awareness

ISO 27001 highlights the significance of employee awareness and training in keeping security strong. EMC can organize regular training sessions on security protocols, recognizing phishing attempts, proper data handling, and reporting incidents. This helps all employees understand their part in keeping security tight and enables them to handle potential threats effectively.

Application of ISO 27001 in EMC's IT Security

Using ISO 27001 helps EMC Cloud Solutions create a planned and organized method for handling information security risks. The standard's rules improve EMC's security in these ways:


Better Data Safety: Following ISO-standard encryption, access control, and data integrity rules keeps client and government data safe from unauthorized access and cyber threats.



Meeting Rules: Following ISO 27001 helps EMC follow data protection rules like GDPR and local Sri Lankan laws, avoiding possible legal problems and increasing trust from clients.

Risk Reduction: By assessing risks regularly and applying corrective actions, EMC minimizes vulnerabilities across its data center and cloud services, ensuring reliable and secure services.

Incident Preparedness: Documented response plans based on ISO guidance allow EMC to manage and mitigate incidents efficiently, reducing downtime and reputational damage.

Continuous Improvement: ISO 27001's emphasis on audits and management reviews encourages EMC to continuously refine its security practices, adapting to new threats and ensuring its ISMS remains effective.

 ISO 27001




ISO/IEC 27001:2013

**Information technology – Security techniques –
Information security management systems -
Requirements**

Standards that provides methodology for the implementation of
Information Security Management System in an organization.

Can be implemented in any kind of organization, profit or non-
profit, private or state-owned, small or large.



www.belajarmikrotik.com

05

Analyze possible impacts to organizational security resulting from an IT security audit.

What is an IT Security Audit and why it Important

An IT security audit is a thorough examination of an organization's IT systems, rules, and practices to check how well they protect against security risks and find any weak spots. This review ensures that the organization follows important security rules like ISO 27001 or GDPR, making sure that data protection methods and rules work well against cyber threats. By finding potential problems, an audit helps organizations improve their defenses before any issues happen, lowering the chance of security breaches. Regular IT security audits are very important for staying in line with rules and avoiding legal and financial problems. They also help build trust with clients by showing that the organization is serious about data security, which is especially important for businesses that handle sensitive client information. Overall, an IT security audit is a crucial tool for protecting both the organization's assets and customer data in today's changing threat environment.

Enhanced Security Posture

An IT security audit finds weaknesses, mistakes, and missing parts in current security rules, helping a company like EMC Cloud Solutions fix these issues. By fixing these problems, the company makes its security better, protecting important things, customer information, and business operations. This makes EMC more able to handle possible cyber threats, greatly lowering risks.

Improved Compliance and Risk Management

A security audit helps EMC's operations follow important rules for protecting data, like GDPR, ISO 27001, and local laws. Following these rules not only lowers the chance of getting in trouble with the law but also makes clients feel more secure, especially those in industries like government or finance that have strict rules. Plus, by using the audit's suggestions, EMC can create a plan to handle risks before they become big problems, making sure new risks are always watched and managed well.

Increased Employee Awareness and Responsibility

Security audits frequently point out the importance of employee awareness and training. During the audit, issues might be found that result from human mistakes or inadequate security practices among employees. After the audit, EMC can set up specific training programs to teach employees about security rules, stressing how crucial security is in their daily work. This increased awareness can create a more careful and security-minded team, lowering the chances of insider threats or accidental security issues.

Operational Disruptions

Although a security audit is helpful in the long term, it can briefly interrupt EMC's work. Some parts of the network or systems might need to be turned off for checking, evaluating, or fixing issues. This usually lasts only a short time but needs good planning to avoid affecting important services. For a cloud provider like EMC, where keeping clients online is very important, it's crucial to handle these interruptions well. Companies must manage these disruptions to keep things running smoothly and ensure clients stay satisfied with the service.

Increased Financial Investment

Fixing weaknesses and making security better after an audit might need more money. EMC could have to spend on new tools, technology updates, or hiring more people to follow the audit's advice. Even though this spending makes security stronger, it can change short-term budgets and need moving money around.

Improved Reputation and Customer Confidence

Effectively completing and addressing an IT security audit can boost EMC's image as a safe and dependable service provider. Showing dedication to top security practices helps build customer trust, which can be a key advantage, especially for important clients such as government agencies. By clearly explaining the actions taken after the audit, EMC can assure clients of its focus on data security, possibly drawing in more customers who value secure cloud services.

3.3 You have to recommend how IT security can be aligned with an EMC organizational policy, detailing the security impact of any misalignment.

why IT security should match an organization's policy

IT security should be in line with an organization's policies to make sure all security steps help achieve business goals, follow rules, and manage risks. When IT security fits with the organization's policies, important data and systems are kept safe, lowering the chance of problems, legal issues, and business interruptions. This matching also helps by making security practices the same across different parts of the organization, improving how problems are handled and how employees follow rules. In the end, it helps build trust with clients, protecting the organization's reputation and financial health.

What If Happen Misalignments

- ❖ When security rules are not clear, it can lead to poor security practices, like weak access controls, making sensitive data easy to steal or access without permission.
- ❖ If security doesn't follow the rules set by law, the organization could face big fines and legal problems, hurting its money and reputation.
- ❖ Security measures that don't work well together can cause problems, increasing the chance of issues that stop business and lead to lost time or productivity.
- ❖ Security practices that don't match well can cause data leaks, which can hurt trust from customers, especially in businesses that handle important information.

how IT security can be aligned with an EMC organizational policy

To ensure IT security matches EMC's overall strategy, it's important to include security goals in the company's main objectives and daily activities. This starts by creating clear and complete security rules that fit EMC's purpose, legal needs, and industry rules. Regular training helps all staff know and follow these rules, lowering the chance of accidental security issues. Also, EMC should use standard systems like ISO 27001, which offer helpful guidelines for managing information security.

Misalignment between IT security and organizational policy can lead to serious security risks. For example, weak or inconsistent access controls can expose sensitive data to unauthorized users, increasing the likelihood of data breaches and legal consequences. Additionally, misaligned policies may create operational inefficiencies, such as slow incident response times, which can exacerbate the impact of security incidents. Non-compliance with regulatory standards due to policy misalignment can result in fines, reputational damage, and loss of client trust. By ensuring alignment, EMC can protect its data and maintain a strong, cohesive security posture that supports business continuity and client confidence.

Encouraging cooperation between the IT security team and other departments, like HR, finance, and operations, helps make sure that security measures work well across the whole organization. Using systems like ISO 27001 can give a consistent way to handle information security, making sure that security practices are both regular and complete. By using these standards, EMC can deal with risks in a planned way, make sure rules are followed, and stay in line with both internal and external rules.

Mismatches between IT security and company rules can cause serious security problems. If IT security steps don't help the business goals, important data and systems might stay open to attacks, causing data loss, money penalties, and harm to the company's reputation. For example, weak access rules or not enough data protection can let people get into private client info, hurting trust and maybe causing business loss. Also, not following rules because of mismatched security plans can lead to legal issues and big fines, hurting the company's money and place in the market. Working less well can also happen, as mixed or not clear security ways can leave gaps, making it easier for cyber threats to find and use weak spots.

Not having things in sync can make it hard for the organization to handle security problems well. If there's no clear security plan that works together with business activities, dealing with incidents might be slow or not very good, making the problems worse and costing more to fix. Confusion among employees or not following unclear rules can also raise the risk of insider threats and accidental data leaks.

Recommendations to Align IT Security with EMC Organizational Policy

1.) Make rules that match EMC's goals and legal requirements. Make sure these rules cover everything in IT security, like who can access what, keeping data safe, and what to do if something goes wrong.

- **Impact of Misalignment:** If rules are confusing or don't match, it can cause security problems, making it easier for bad things like data theft or unwanted access to happen.

2.) Keep teaching employees about security rules, especially how to handle and protect data.

- **Impact of Misalignment:** If employees don't get regular training, they might accidentally do things that risk data getting out or breaking rules.

3.) Plan periodic security reviews to ensure that rules are being followed and that EMC meets legal and industry requirements.

- **Impact of Misalignment:** Skipping these reviews could lead to overlooked weaknesses, legal fees, and penalties for not following rules.

4.) A well-known security standard to organize and direct EMC's security rules and procedures.

- **Impact of Misalignment:** Without a clear plan, security efforts might vary between departments, raising the chances of problems and data leaks.

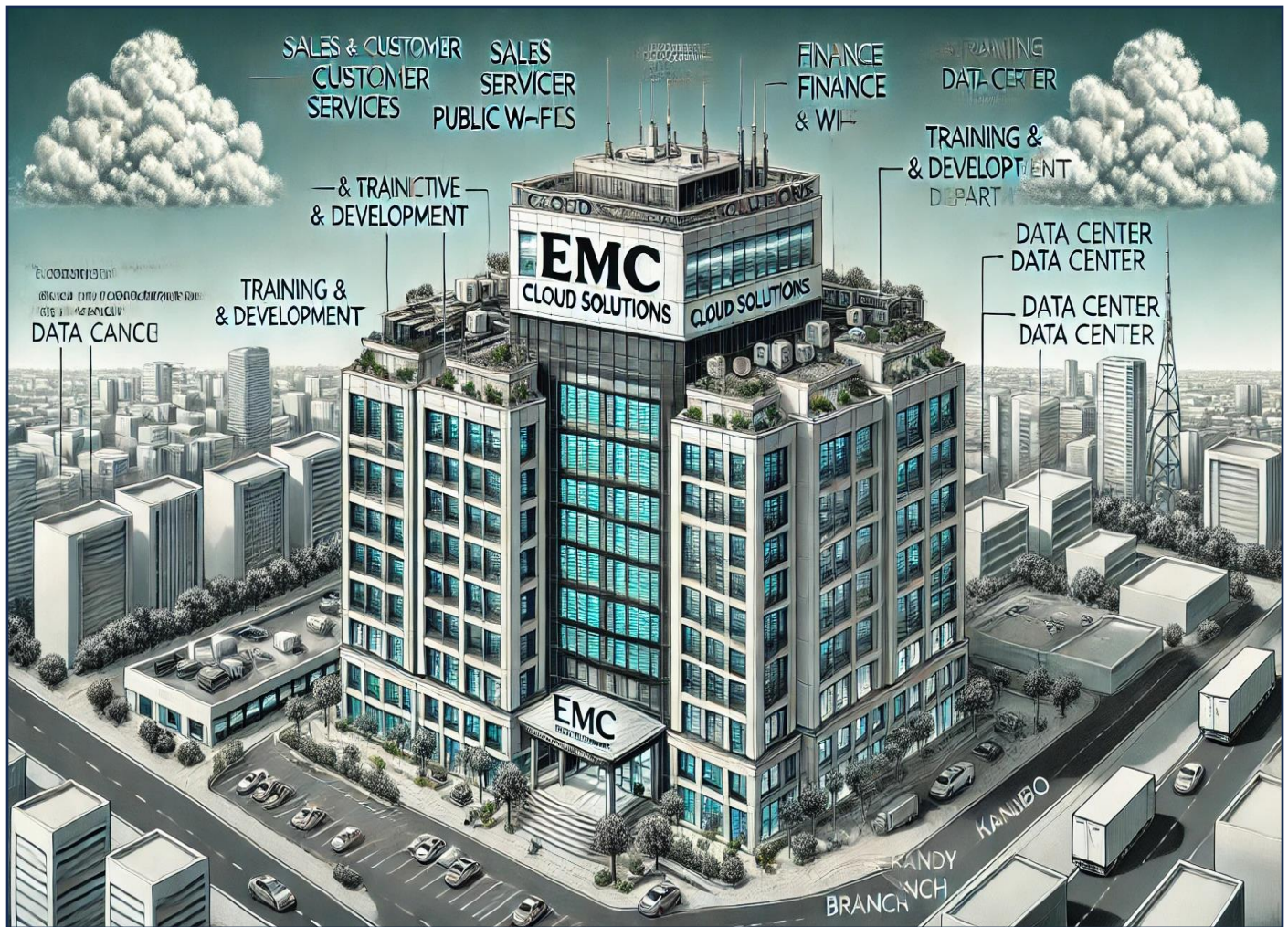
5.) Ensure security practices are embedded in daily operations and across all departments, from HR to IT, so they align with EMC's overarching goals.

- **Impact of Misalignment:** Isolated or inconsistent security practices across departments can lead to miscommunication, fragmented security measures, and exposure to cyber threats.

Making sure IT security fits with the organization's overall plan is very important for keeping strong security that helps meet business goals and follow rules. Good alignment not only protects important data and systems but also makes things run smoother and builds trust with clients. On the other hand, if things aren't aligned, it can cause big security problems, money losses, legal issues, and harm the organization's reputation.

Conclusion

Securing EMC Cloud Solutions' infrastructure is pivotal to maintaining its reputation as a reliable cloud service provider. Addressing risks such as data breaches, system misconfigurations, and external threats requires implementing robust security procedures, including firewalls, VPNs, DMZs, and network monitoring systems. Adopting ISO 31000 standards and adhering to data protection laws will fortify EMC's IT security framework and enhance client trust. Extending services to Kandy necessitates comprehensive risk assessments, integration of physical and virtual security measures, and alignment with organizational policies to ensure seamless, secure operations. This holistic approach safeguards EMC Cloud's assets and promotes sustainable growth.



References

1. Ibm (2024) 'IT security,' martin foxx, 11 September. <https://www.ibm.com/topics/it-security> (Accessed: November 13, 2024).
2. *Security and privacy controls for information systems and organizations* (2020). <https://doi.org/10.6028/nist.sp.800-53r5>.
3. CSA Security Guidance for Cloud Computing | CSA (no date). <https://cloudsecurityalliance.org/research/guidance>.
4. CIS controls (Accessed: November 13, 2024). <https://www.cisecurity.org/controls?form=MG0AV3>.
5. Msmbaldwin (Accessed: November 14, 2024) Azure security documentation. <https://learn.microsoft.com/en-us/azure/security/?form=MG0AV3>.
6. Mather, D. (2022) 11 Benefits of network monitoring. <https://securitygladiators.com/network/monitoring/benefits/>.
7. Tripathy, S. (2024) What is network monitoring? Definition, benefits, and types. <https://www.enterprisenetworkingplanet.com/management/network-monitoring/>.
8. Datadog (2021) What is Network Monitoring? How it Works & Use Cases | Datadog. <https://www.datadoghq.com/knowledge-center/network-monitoring/>.
9. Hein, D. (2019) 8 Benefits of network performance monitoring solutions. <https://solutionsreview.com/network-monitoring/8-benefits-of-network-performance-monitoring-solutions/>.

10. Shackleford, D. (2024) Top 10 identity and access management risks.
https://www.techtarget.com/searchsecurity/answer/What-are-some-of-the-top-identity-and-access-management-risks?utm_source=bing&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lP11132024GOOGOTHR_GsidsSecurity_CyberArk_KTO_IO324014_2861982&utm_campaign=CyberArk_KTO_sSEC_ANZSG%3Dsy_lP11132024GOOGOTHR_GsidsSecurity_CyberArk_KTO_IO324014_2861982&msclkid=d5d48d7dae981e895edaea44d6e36cb7.
11. GeeksforGeeks (2022) Relationship between VPN and firewall.
<https://www.geeksforgeeks.org/relationship-between-vpn-and-firewall/>.
12. Okeke, F. (2023) Firewall Policy: design, configuration, and examples.
<https://www.enterprisenetworkingplanet.com/security/firewall-policy/>.
13. Chkadmin (2023) 8 Firewall best practices for securing the network.
<https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/8-firewall-best-practices-for-securing-the-network/>.
14. Shackleford, D. (2024b) Top 10 identity and access management risks.
https://www.techtarget.com/searchsecurity/answer/What-are-some-of-the-top-identity-and-access-management-risks?utm_source=bing&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lP11132024GOOGOTHR_GsidsSecurity_CyberArk_KTO_IO324014_2861982&utm_campaign=CyberArk_KTO_sSEC_ANZSG%3Dsy_lP11132024GOOGOTHR_GsidsSecurity_CyberArk_KTO_IO324014_2861982&msclkid=412c7140e82e1548c369167991448725.
15. Nolle, T. (2019) Virtual network security measures to thwart access threats.
<https://www.techtarget.com/searchsecurity/tip/Virtual-network-security-measures-to-thwart-access-threats>.

16. Cyber Security Risk Assessment: Step-by-Step Process (2024).
<https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-risk-assessment/>.
17.
IT Risk Assessment Fundamentals and Best Practices | AuditBoard (no date).
<https://www.auditboard.com/blog/it-risk-assessment-fundamentals/>.
18. Tajuddin, A. (2023) 'Complete guide to conducting risk assessment: importance, benefits, and 5 simple steps,' Safety Notes, 17 April. <https://www.safetynotes.net/risk-assessment/>.
19. British Safety Council (no date) Risk Assessment and Management: A Complete guide.
<https://www.britsafe.org/training-and-learning/informational-resources/risk-assessments-what-they-are-why-they-re-important-and-how-to-complete-them>.
20. Sri Lanka (2022) Personal Data Protection Act, Personal Data Protection Act.
<https://www.icta.lk/icta-assets/uploads/2022/08/Article-Personal-Data-Protection-Act-Updates-April-2022-1.pdf>.
21. Lahiru (Accessed: November 15, 2024) Data Protection Authority.
<https://www.dpa.gov.lk/DPA.php>.
22. ISO - ISO 31000 — Risk management (2021). <https://www.iso.org/iso-31000-risk-management.html/>.
23. Risk management — Guidelines (2018).
<https://cdn.standards.iteh.ai/samples/65694/60673072317a4b96bd36efb910b68926/ISO-31000-2018.pdf>.
24. Kosutic, D. (no date) What is ISO 27001? An easy-to-understand explanation.
<https://advisera.com/27001academy/what-is-iso-27001/>.

25. Admin (2024) The Ultimate Guide to ISO 27002. <https://www.isms.online/iso-27002/>.

26. Barker, S. (2024) ISO 27001 Checklist. <https://hightable.io/iso27001-checklist/>.