Unit 4: Security Standards, Frameworks and Disaster Recovery

1. List common security standards and select the appropriate one(s) for a given situation.

Kirvan (2021) asserts that effective IT security frameworks and cybersecurity standards are crucial for safeguarding company data against potential threats. Compliance regulations and standards, such as HIPAA, PCI DSS, Sarbanes-Oxley Act, and GDPR, pose significant challenges to IT security. However, implementing IT security frameworks and standards is indispensable for all infosec and cybersecurity professionals as they provide a foundation for establishing processes, policies, and administrative activities for information security management. Organisations must customise frameworks to address specific information security concerns, such as industry-specific requirements or regulatory compliance objectives, and carefully consider the selection of a particular IT security framework based on various factors, such as the type of industry or compliance requirements.

Here are a few examples of IT security standards and frameworks, as outlined by Kirvan (2021):

- The ISO 27000 series by the International Organization for Standardization provides a flexible information security framework for organisations of all types and sizes. It has 60 standards covering a wide range of information security issues. The primary standards, ISO 27001 and 27002, establish requirements and procedures for creating an information security management system (ISMS) essential for audit and compliance activities. Organisations can achieve compliance through audit and certification processes provided by third-party organisations.

- NIST is the ultimate authority when it comes to IT standards. The SP 800 series, covering almost all aspects of information security, is a must-follow for any organisation that takes security seriously. SP 800-53 is the gold standard for U.S. government agencies and is widely adopted in the private sector. Compliance with NIST SP 800-171 is mandatory for U.S. Department of Defense contractors. NIST CSF is the go-to framework for any organisation that wants to manage cybersecurity risk effectively. The NIST SP 1800 series is a valuable resource for organisations looking to implement cybersecurity technologies in real-world scenarios.

- COBIT is a framework developed by ISACA to reduce IT risks. It includes new tech and business trends to help balance IT and business goals. The current version, COBIT 2019, is used to achieve SOX compliance. ISACA offers professional certifications, such as Certified Information Systems Auditor and Certified Information Security Manager.

- CIS Controls, formerly the SANS Top 20, is a list of technical security and operational controls that can be applied to any environment. Unlike NIST CSF, it focuses solely on reducing risk and enhancing resilience for technical infrastructures. The Controls include Inventory and Control of Enterprise Assets, Data Protection, Audit Log Management, Malware Defences, and Penetration Testing. They help remediate identified risks and are valuable resources for IT departments with limited technical information security expertise.

- The GDPR is a set of security guidelines that organisations worldwide must follow to safeguard the privacy and security of the personal information of European Union citizens. The regulations require measures such as access control, least privilege, role-based access, and multifactor authentication to be implemented to prevent unauthorised access to stored data.

- NERC CIP sets 14 standards for utility companies in the bulk power system. It provides guidelines for securing critical infrastructure systems through monitoring, regulating, managing, and maintaining security. Bulk power system owners, operators, and users must comply with the framework.

2. Describe how to design and create DR solutions.

According to Cloudian (N.D.), disaster recovery is planning for and recovering from disasters that may affect a business. It includes natural events, equipment or infrastructure failure, artificial calamities, and cyber-attacks. A disaster recovery plan enables companies to respond quickly to a disaster and resume operations as soon as possible. It includes emergency procedures, critical IT assets, tools or technologies, a disaster recovery team, and communication procedures. A disaster recovery plan can minimise interruption, limit damages, provide training and preparation, and restore services. Business continuity and disaster recovery are often grouped but differ in scope. Business continuity focuses on minimising risks and ensuring the organisation can continue to deliver products and services, while disaster recovery is focused on IT systems needed for business continuity.

Disaster recovery (DR) planning is critical to business continuity planning. It begins with a Business Impact Analysis that defines two vital metrics: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The smaller these metrics, the more expensive it is to run the application. RTO and RPO values usually combine into another Service Level Objective (SLO) metric. High Availability (HA) is also essential when considering RTO and RPO values (Google Cloud, 2023).

A disaster recovery plan (DRP) is a set of policies and instructions businesses must have to recover quickly from disruptive events. It's not just about preventing downtime but also about resuming operations quickly and avoiding significant losses in revenue or data during emergencies. To ensure a successful DRP, the four stages of the disaster management cycle, prevention, preparation, mitigation, and recovery, must be followed. DRPs have many processes and tools that impact information technology (IT) applications. Therefore, having a robust DRP in place is good practice and a responsibility that can prevent catastrophic consequences (Helixstorm, 2020).

For instance, here are the steps for Designing a Foolproof Disaster Recovery Plan as per Helixstorm (2020) notes:

1. Conduct a Risk Analysis
2. Assess Your Vulnerabilities
3. Identify Critical Business Processes and Applications
4. Set Recovery Objectives
5. Determine the Backup and Data Recovery Methods
6. Establish Activation Protocol
7. Create a Notification Process

8. Form a Response Team and Train Your Employees
9. Test, Revise and Test Again
10. Document Your Disaster Recovery Plan
11. Keep Your DRP Updated

References:

- Kirvan, P. (2021). *Top 7 IT security frameworks and standards explained*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one.
- Cloudian (N.D.). *Disaster Recovery: 5 Key Features and Building Your DR Plan*. [online] Available at: https://cloudian.com/guides/disaster-recovery/disaster-recovery-5-key-features-and-building-your-dr-plan/.
- Google Cloud. (2023). *Disaster recovery planning guide* | *Cloud Architecture Center*. [online] Available at: https://cloud.google.com/architecture/dr-scenarios-planning-guide.
- Helixstorm. (2020). *11 Steps for Designing a Foolproof Disaster Recovery Plan*. [online] Available at: https://www.helixstorm.com/blog/steps-for-designing-a-foolproof-disaster-recovery-plan/.