WEEK 3 ASSIGNMENT- GROUP D

By Oyinkansola, [redacted]

Q. Research and submit a report on ISO 27017 & ISO 27032 considering the following:

- Scope and objectives of standards
- Identify the key principles, concepts, and core components of the standards
- Discuss the benefits of implementing the standards
- Discuss the relationship between the standards and relevant standards like ISO 27001.
- Provide examples of cloud security challenges addressed by ISO 27017.
- Provide examples of cyber incidents where adherence to ISO 27032 principles could have mitigated risks.

	ISO 27017	**ISO 27032**
Scope and objectives	The scope of ISO 27017 is to provide guidelines and controls specifically focused on information security in cloud computing environments. It addresses the unique challenges and risks associated with the adoption and use of cloud services. The standard applies to both cloud service providers (CSPs) and cloud customers, outlining their respective roles and responsibilities in ensuring cloud security. **Objectives** a) Provide a consistent and structured approach to cloud security: ISO 27017 aims to establish a common framework for organizations to assess, implement, and manage cloud security controls. It ensures that organizations have a systematic approach to address cloud-specific risks and protect their information assets in the cloud. b) Enhance the security of cloud services: The standard aims to enhance the security posture of cloud	The scope of ISO 27032 includes: a. an explanation of the relationship between Internet security, web security, network security, and cybersecurity; b. an overview of Internet security; c. identification of interested parties and a description of their roles in Internet security; d. high-level guidance for addressing common Internet security issues **Objectives** The primary goal of ISO/IEC 27032 is to promote safer and more secure transactions and interactions in cyberspace by preventing data breaches and lowering potential risks.

	services by providing a set of controls and practices tailored for cloud environments. It helps organizations identify and implement appropriate security measures to protect their data and systems from potential threats and vulnerabilities. c) Define roles and responsibilities: ISO 27017 clarifies the roles and responsibilities of Cloud Service Providers and cloud customers, ensuring that both parties understand their obligations in maintaining a secure cloud environment. d) Support compliance with regulatory requirements: ISO 27017 assists organizations in aligning their cloud security practices with relevant regulatory frameworks and industry-specific standards.	
Key principles, concepts, core components	**Key Principles and Concepts**: ● ISO/IEC 27017 builds upon ISO/IEC 27002 by offering additional implementation guidance for relevant controls. ● It introduces controls with implementation guidance that specifically relate to cloud services. ● The standard provides controls and implementation guidance for both **cloud service providers** and **cloud service customers**.	**Key Principles and Concepts**: ● ISO/IEC 27032 aims to enhance the state of cybersecurity globally. ● It addresses the challenges posed by cyber threats and vulnerabilities. ● The standard helps organizations enhance their resilience against cyber incidents. ● ISO/IEC 27032 encourages collaboration and information sharing among stakeholders.

	o **Core Components**: ● Detailed advice on how to implement relevant controls from ISO/IEC 27002 in cloud environments. ● Specific controls tailored for cloud services, addressing aspects like data privacy, access management, and incident response.	o **Core Components**: ● This includes code review, testing, protection of source code, and secure configurations. ● Regular security testing, vulnerability management, patch management, and separate QA/test environments
Benefits of implementing the standards	Implementing ISO 27017 standards offers several benefits for organizations that include: 1. Tailored Cloud Security. 2. Risk Management 3. Improved Governance. 4. Compliance and Assurance. 5. Cost Reduction. 6. International Recognition. 7. Continuous Improvement.	Implementing ISO 27032 standards offers several benefits for organizations that include 1. Improved cyber resilience 2. Enhanced cybersecurity posture 3. Effective management of cyber risks 4. Increased protection of critical information assets 5. Strengthened incident response capabilities 6. Enhanced trust and confidence among stakeholders 7. Alignment with international best practices 8. Compliance with regulatory requirements
Relationship between the standards and relevant standards like ISO 27001	ISO 27001, ISO 27017, and ISO 27032 are all related standards within the ISO 27000 family, which addresses information security management systems (ISMS) and cybersecurity. ISO 27001 is the core standard for information security management, while ISO 27017 provides additional guidance specific to cloud computing environments, and ISO 27032 focuses on cybersecurity in general, covering broader aspects of information security beyond cloud computing.	

Examples of cloud security challenges addressed by ISO 27017	Some examples of cloud security challenges addressed by ISO 27017 include ● Enhanced Security Framework: Which provides organizations with an internationally recognized framework tailored specifically for cloud services, enhancing trust and security. ● Compliance: Assists both providers and users of cloud services in meeting regulatory and compliance requirements. ● Risk Management: Improved management of information security risks particular to cloud computing environments. ● .Supplier relationships: ISO 27017 helps organizations manage the security risks associated with third-party cloud service providers and subcontractors, ensuring that they meet security requirements. ● Incident response: The standard provides guidance on developing and implementing an incident response plan for addressing security breaches and other incidents in the cloud. ● Data sovereignty: ISO 27017 addresses concerns related to data sovereignty by providing guidance on where data can be stored and processed, ensuring compliance with legal and regulatory requirements. ● Data loss: The standard helps to mitigate the risk of data loss by providing guidance on	NA

	backup and recovery strategies, ensuring data availability.	
Examples of cyber incidents where adherence to ISO 27032 principles could have mitigated risks.	NA	● **Sony PlayStation Network Outage:** The 2011 incident where personal data from millions of accounts was stolen could have been mitigated by adhering to ISO/IEC 27032's guidelines, which emphasize the importance of robust cybersecurity measures and effective incident management strategies. ● **Target Corporation Breach (2013):** The breach was facilitated by stolen credentials from a third-party vendor. ISO 27032's emphasis on comprehensive stakeholder coordination and robust cybersecurity measures could have helped mitigate such risks through better security practices for third-party vendors. ● **Sony Pictures Hack (2014):** This breach, involving data leakage and system damage, emphasized the need for better cybersecurity measures across the board. ISO 27032's emphasis on governance and stakeholder collaboration could have facilitated more effective threat intelligence sharing and incident response and enhanced resilience against the sophisticated phishing attacks that initiated the breach. ● **WannaCry Ransomware Attack (2017):** This global ransomware campaign

		exploited vulnerabilities on a massive scale. Adherence to ISO 27032 would have promoted better preparedness and faster response to the spread of ransomware through effective patch management and incident response that would have mitigated the impact of the attack.