Introduction to Principles-Based Security Governance and Compliance Frameworks

HyperionDev

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- What Penetration Testing is
- The Importance of Penetration Testing
- Steps/Methodology
- Types of Pen Tests
- Tools

Objectives

- What Governance + Compliance is
- Principles for Security Governance
- Compliance Frameworks
- Benefits/Considerations

Security Governance & Compliance Frameworks

- Security Governance: Ensures effective management and oversight of security within an organization that are aligned in a way that supports the organization's business goals.

- Compliance Frameworks: Established guidelines and standards for meeting legal, regulatory, and industry requirements.

Principles-Based Security Governance

Flexible approach focusing on guiding principles rather than rigid rules.

Risk-Based decision Making:
- Identifying and assessing risks.
- Prioritizing security measures based on risk levels.

Accountability and Responsibility:
- Assigning clear roles and responsibilities for security.
- Accountability for security actions and outcomes

Transparency & Communication:
- Openly communicating security policies and practices
- Share information and report of security incidents.

Principles-Based Security Governance

Continuous Improvement: - Regular assessing and updating security measures

- Learn from past incidents and implement fixes

Integration and Alignment: - Integrating security into all aspects of the organization.

- Aligning security objectives with business goals and strategies.

Resilience and Adaptability: - Regular assessing and updating security measures

- Learn from past incidents and implement fixes

Questions and Answers

Compliance Frameworks

Ensuring that organizational activities are operated in accordance with the laws and regulations impacting those systems.

- ISO 27001/27002
- NIST Cybersecurity Framework
- PCI DSS
- HIPAA
- GDPR

Hyperiondev

Selecting and Implementing Compliance Frameworks

- 1). Assessing organizational needs and requirements.
- 2). Mapping frameworks to industry standards and regulations.
- 3). Customizing frameworks to align with specific business contexts.

Benefits and Considerations of Principles-Based Security Governance

Benefits:

- Flexibility and adaptability to evolving threats and needs.
- Alignment of security measures with business objectives.
- Enhanced risk management and accountability.

Factors that require consideration:

- Balancing compliance requirements with organizational needs.
- Sustaining security governance and compliance.

Wrapping Up

- Principles-Based Security Governance and Compliance Frameworks provide a solid foundation for effective security practices.

- By incorporating key principles and leveraging compliance frameworks, organizations can establish robust security governance and meet regulatory requirements.

- It is important to continually assess, improve, and adapt security governance practices to ensure ongoing effectiveness.

- Outlined in the results section. It offers practical guidance on how to get the desired outcomes.

Next up

- Incident Responses

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"