




Welcome to the CoGrammar

Compliance Frameworks and Roles

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.



Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
(Fundamental British Values: Mutual Respect and Tolerance)
- 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. Moderators are going to be answering questions as the session progresses as well.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: [Questions](#)

Software Engineering Session Housekeeping cont.

- For all **non-academic questions**, please submit a query:
www.hyperiondev.com/support
- Report a **safeguarding** incident:
www.hyperiondev.com/safeguardreporting
- We would love your **feedback** on lectures: [Feedback on Lectures](#)

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:



Ian Wyles
Designated Safeguarding
Lead



Simone Botes



Rafiq Manan



Charlotte Witcher



Nurhaan Snyman



Ronald Munodawafa



Tevin Pitts

Scan to report a
safeguarding concern



or email the Designated
Safeguarding Lead:
Ian Wyles

safeguarding@hyperiondev.com

Learning Objectives & Outcomes

- Describe compliance frameworks
- Explain roles within a cybersecurity team
- Apply regulatory requirements to cybersecurity scenarios
- Discuss the importance of compliance in cybersecurity



**SKILLS
FOR LIFE**
SKILLS BOOTCAMPS


Department
for Education

CoGrammar

CyberSecurity

September 2024

CyberSecurity

- Have you ever heard of companies facing **fines** due to **non-compliance** with **data protection laws**?



Polls

Please have a look at the poll notification and select an option.

Are you familiar with the concept of a compliance framework?

- A. Yes
- B. No
- C. Unsure

Polls

Please have a look at the poll notification and select an option.

Who ensures compliance in cybersecurity teams?

- A. A third-party auditor
- B. CISO (Chief Information Security Officer)
- C. The whole team

What are Compliance Frameworks?

- Compliance frameworks are structured **guidelines** that dictate how organizations **secure sensitive information**.
- **Purpose:**
 - Standardize security across industries.
 - Help manage risks and avoid penalties for non-compliance.

What are Data Protection Laws?

- Data protection laws are legal frameworks designed to safeguard individuals' personal information from misuse, unauthorized access, or exploitation. These laws set rules and standards for how organizations collect, store, process, and share personal data. They ensure that individuals have rights over their data, and organizations must adhere to strict privacy regulations to avoid breaches and penalties.

Examples of Data Protection Laws?

- GDPR (General Data Protection Regulation) - EU
 - Enforces strict guidelines on data collection, storage, and sharing within the European Union.
 - Penalties for non-compliance can be as high as 4% of a company's global revenue.
- CCPA (California Consumer Privacy Act) - U.S.
 - Grants California residents the right to know what data is being collected, the right to opt-out of the sale of their data, and the right to delete personal data.
- HIPAA (Health Insurance Portability and Accountability Act) - U.S.
 - Protects sensitive medical information and ensures that health data is handled securely.
- PIPEDA (Personal Information Protection and Electronic Documents Act) - Canada
 - Regulates the collection, use, and disclosure of personal data in commercial activities.

Real-world Scenarios Related to CyberSecurity Governance and Compliance Frameworks

- In 2020, British Airways was fined **£20 million** under the GDPR for failing to protect personal data. Hackers accessed the data of over 400,000 customers, including login details and payment information.
- In 2019, Facebook (now Meta) was fined \$5 billion by the U.S. Federal Trade Commission (FTC) for privacy violations involving user data being improperly shared with Cambridge Analytica.

CyberSecurity

- Both cases emphasize the severe consequences of non-compliance, which include hefty fines, loss of customer confidence, and long-term damage to a brand's reputation.

Key Compliance Frameworks

- NIST (National Institute of Standards and Technology):
 - Focus on U.S. government systems and vulnerability reduction.
- The General Data Protection Regulation (GDPR):
 - Was brought into effect in 2016 to augment data protection for European Union citizens.
 - This framework influences all organisations or businesses within the EU that collect personal data from EU citizens (this regulation also impacts US businesses).
- ISO 27001:
 - Global standard for Information Security Management Systems (ISMS).
- PCI-DSS:
 - Payment Card Industry Data Security Standard for securing card transactions.

Regulatory Requirements and Impact

Example Case Study: Facebook's GDPR violation and related fines.

- Incident:
 - In July 2019, Facebook was fined €5 billion by the Federal Trade Commission (FTC) for privacy violations under the GDPR.
 - The fine resulted from Facebook's failure to adequately protect user data and notify users of breaches.
- Consequences:
 - Financial Impact: The fine is one of the largest ever imposed under GDPR.
 - Reputational Damage: The violation impacted Facebook's public image and trust with users.
 - Operational Changes: Facebook was required to implement stricter data protection measures and enhance transparency.

The Importance of Compliance in Cybersecurity

- Protects Sensitive Data:
 - Compliance frameworks ensure that sensitive data is handled securely and in line with legal and regulatory requirements.
- Mitigates Risk:
 - Following compliance guidelines reduces the risk of data breaches, security incidents, and financial penalties.
- Builds Trust:
 - Companies that adhere to compliance standards build trust with customers, partners, and regulators.
- Legal Consequences:
 - Non-compliance can lead to hefty fines, legal action, and reputational damage (e.g., GDPR fines).
- Supports Business Continuity:
 - Ensuring compliance helps prevent disruptions in operations and ensures a company can continue to function securely.
- **Question: Why do you think compliance is critical for organizations beyond avoiding fines?**

**Let's take a break
To stretch and relax**



Roles in a Cybersecurity Team

- **Question:**
 - What is the role of a Cybersecurity team?

Roles in a Cybersecurity Team

- Security administrator:
 - is essential because their role spans multiple important functions. For example, it is their responsibility to establish security guidelines, and set up firewalls and malware protection software.
- Security specialist:
 - oversees the company's system security and vets its vulnerabilities.
- Incident responder:
 - detects and responds to threats.
- Vulnerability assessor:
 - similar to an incident responder, these analysts run tests on the security system to find overlooked vulnerabilities in the system.
- Security manager:
 - supervises the rest of the team. They take important decisions and oversee the whole team's work. They also design the security structure, test out the security, and respond to threats.

Roles in a Cybersecurity Team

- Penetration tester:
 - is authorised to hack a system to identify security vulnerabilities. In essence, they simulate the role of a malicious hacker. Their findings are then relayed to their manager. This is a variant of white-hat hacking.
- Help desk:
 - is an entry-level role that requires knowledge of ticketing systems, requires an understanding of security precautions to protect client data, attends to various technical hardware and software issues, and is familiar with IT diagnostics to pinpoint appropriate solutions.
- Security consultant:
 - in a freelance capacity, these consultants assess a company's system(s) and propose improvements.

Roles in a Cybersecurity Team

- Key Roles:
 - **Security Analyst:** Monitors systems for breaches and vulnerabilities.
 - **Security Architect:** Designs and implements secure IT architectures.
 - **CISO (Chief Information Security Officer):** Oversees the company's security strategy and compliance.
- Question:
 - What role do you think is the most challenging in a cybersecurity team, and why?

Role-Specific Responsibilities

- **Security Analyst**

- Responsibilities:
 - Monitor and analyze security alerts and logs to detect potential threats.
 - Conduct vulnerability assessments and penetration tests.
 - Implement and manage security controls and measures.
- Contribution to Regulatory Compliance:
 - PCI-DSS Adherence: Ensures that payment card data is protected by implementing and managing security measures such as encryption and access controls.
 - General Compliance: Regularly reviews and updates security policies and procedures to ensure they meet regulatory standards.

Role-Specific Responsibilities

- **Security Architect**
 - Responsibilities:
 - Design and implement security infrastructure and systems.
 - Develop security protocols and architecture to protect sensitive data.
 - Evaluate and integrate new security technologies.
 - Contribution to Regulatory Compliance:
 - ISO 27001: Ensures that the security architecture aligns with the Information Security Management System (ISMS) requirements.
 - General Compliance: Creates secure system designs that facilitate adherence to various compliance frameworks, such as GDPR and HIPAA.

Role-Specific Responsibilities

- **Chief Information Security Officer (CISO)**
 - Responsibilities:
 - Develop and oversee the organization's security strategy and policies.
 - Manage and coordinate compliance efforts across the organization.
 - Report to executive management and the board on security posture and compliance status.
 - Contribution to Regulatory Compliance:
 - GDPR Compliance: Ensures that data protection and privacy measures are in place, oversees compliance audits, and handles breach notifications.
 - General Compliance: Guides the implementation of security practices and policies to meet various regulatory requirements, and ensures that the organization's security posture aligns with compliance obligations.

Polls

Please have a look at the poll notification and select an option.

Which of the following best describes a compliance framework?

- A. A set of tools to monitor network traffic
- B. A structured set of guidelines that helps organizations meet regulatory and security requirements
- C. A group of individuals responsible for maintaining security policies
- D. A software program that scans for vulnerabilities

Polls

Please have a look at the poll notification and select an option.

Why is compliance important in cybersecurity?

- A. To ensure the use of advanced technology
- B. To protect organizations from legal penalties and maintain trust with stakeholders
- C. To reduce the number of cybersecurity roles required in a team
- D. To make system updates easier and faster

Polls

Please have a look at the poll notification and select an option.

Which role in a cybersecurity team is primarily responsible for designing and implementing security architecture to align with compliance requirements?

- A. Security Analyst
- B. Security Architect
- C. Chief Information Security Officer (CISO)
- D. Penetration Tester

Summary

- Key Takeaways:
 - Compliance frameworks, such as NIST, ISO 27001, and PCI-DSS, set the standards for securing sensitive data and avoiding costly breaches.
 - Regulatory requirements like GDPR and HIPAA hold organizations accountable for protecting personal and sensitive information.
 - Cybersecurity roles (Security Analyst, Architect, CISO) work together to ensure adherence to these frameworks and regulations.
- Final Thought:
 - Maintaining compliance is essential not only for avoiding fines but also for building trust and ensuring the integrity of an organization's security posture.

Questions and Answers



Thank you for attending



Department
for Education

CoGrammar

