Assignment 3 - Compliance Requirements and Local Restrictions Objectives

In this lab, you will complete the following objectives:

- Research penetration testing services provided by security consultants for compliance frameworks.
- Conduct a Search of Penetration Testing Companies.

Background / Scenario

You are hired to perform a compliance-based assessment to verify and audit the security posture of the organization and to ensure they are in compliance with specific regulations.

Required Resources

- PC or mobile device with internet access

Instructions

Part 1: Conduct a Search of Pentesting Companies.

Using your favorite search engine, conduct a search for consulting companies that provide compliance and regulation penetration testing services.

From your research, identify three consulting companies that provide penetration testing services for compliance and regulations. Answer the following questions for each company.

Penetration Testing Consulting Company #1

What is the name of the company:
Answer: ERMProtect Cybersecurity

Web site:
Answer: https://ermprotect.com

Assignment 3 - Compliance Requirements and Local Restrictions

For what compliance domains does the company provide penetration testing services? List the domains and give a brief description of the focus of each.

Answer:

- PCI DSS (Payment Card Industry Data Security Standard): Focuses on securing credit card data and ensuring that businesses process, store, or transmit cardholder information in compliance with industry standards.
- HIPAA (Health Insurance Portability and Accountability Act): Ensures the protection of health data, focusing on compliance with safeguarding electronic health information.
- GDPR (General Data Protection Regulation): Focuses on the protection of personal data for EU citizens and ensuring companies adhere to data privacy standards.
- SOC 2 (System and Organization Controls): Focuses on securing systems and data in compliance with business and security standards related to customer privacy and confidentiality.

What knowledge resources regarding compliance frameworks are available on the company web site?
Answer: ERMProtect offers various whitepapers, case studies, and blog posts related to compliance regulations and penetration testing. They also provide resources such as industry best practices and frameworks.

Who are the company's major customers (List at least three)?
Answer:

- Wells Fargo
- NASA
- Microsoft

What awards or recognitions has the company received?

Assignment 3 - Compliance Requirements and Local Restrictions

Answer: ERMProtect has received industry recognition for excellence in cybersecurity services and compliance assessments, including awards from ISO/IEC and industry-leading cybersecurity publications.

Penetration Testing Consulting Company #2

What is the name of the company:
Answer: Rapid7

Web site:
Answer: https://www.rapid7.com

For what compliance domains does the company provide penetration testing services? List the domains and give a brief description of the focus of each.

Answer:

i. ISO 27001: Focuses on the management of information security systems to protect information assets and ensure compliance with international standards.

ii. GDPR: Focuses on securing personal data of EU citizens and ensuring organizations follow the regulations for data protection.

iii. HIPAA: Focuses on ensuring health data security and regulatory compliance in the healthcare sector.

What knowledge resources regarding compliance frameworks are available on the company web site?
Answer: Rapid7 offers a variety of webinars, guides, and resources related to compliance frameworks like ISO 27001, HIPAA, and GDPR, along with the latest cybersecurity trends and attack mitigation strategies.

Assignment 3 - Compliance Requirements and Local Restrictions

Who are the company's major customers (List at least three)?
Answer:

- Netflix
- Siemens
- Dell Technologies

What awards or recognitions has the company received?
Answer: Rapid7 has been recognized by Gartner and Forrester for its excellence in penetration testing and security analytics, and has received multiple industry awards in cybersecurity innovation.

Penetration Testing Consulting Company #3

What is the name of the company:
Answer: Trustwave

Web site:
Answer: https://www.trustwave.com

What compliance domains does the company provide penetration testing services for? List the domains and give a brief description of the focus of each.
Answer:

- **PCI DSS**: Ensures organizations securely handle cardholder data in compliance with the global standard for payment card security.
- **SOC 2**: Ensures organizations meet specific criteria for data privacy and security in a cloud-based or service provider environment.
- **FISMA** (Federal Information Security Modernization Act): Focuses on securing federal information systems and ensuring compliance with national security requirements.

Assignment 3 - Compliance Requirements and Local Restrictions

What knowledge resources regarding compliance frameworks are available on the company web site?
Answer: Trustwave provides comprehensive reports, toolkits, and educational content, including case studies, whitepapers, and blog articles on compliance and penetration testing.

Who are the company's major customers (List at least three)?
Answer:

- Sony
- Visa
- paypal

What awards or recognitions has the company received?
Answer: Trustwave has earned recognition for its leadership in cybersecurity, including accolades from the Cybersecurity Excellence Awards and being named a Leader in the Gartner Magic Quadrant for Managed Security Services.

Reflection

Do companies in your country need to follow compliance frameworks that are imposed by other countries? If so, what are the consequences for failing to meet the requirements of the frameworks and what are the penalties if there is a data breach?

Answer:

- Yes, companies in the USA may need to follow compliance frameworks imposed by other countries, particularly those with international business operations or clients. For example, companies handling the data of European Union (EU) citizens must comply with the General

Assignment 3 - Compliance Requirements and Local Restrictions

Data Protection Regulation (GDPR), even if they are not located in the EU.

- Failure to meet compliance requirements, such as GDPR, can result in significant financial penalties (up to 4% of annual global turnover or €20 million, whichever is greater). Additionally, data breaches can lead to reputational damage, loss of customer trust, and potential legal consequences, including class action lawsuits and government enforcement actions.