Regulatory Drivers & Cyber Security Compliance

Reading

45m

Status | Incomplete

Introduction

With this reading, it is time to circle back to GRC and get more insights about Compliance which is a key component of GRC. In this reading, you will learn how Cyber Security practices in the industry are regulated by regulatory drivers and policies, and how regulatory compliance plays a key role in strengthening the security posture of an organization. In this reading, you will learn about:

- What regulatory drivers are
- Some common regulatory drivers in the industry
- How to comply to Cyber Security laws
- How to implement GRC using the Integrated Controls Management approach

Reading

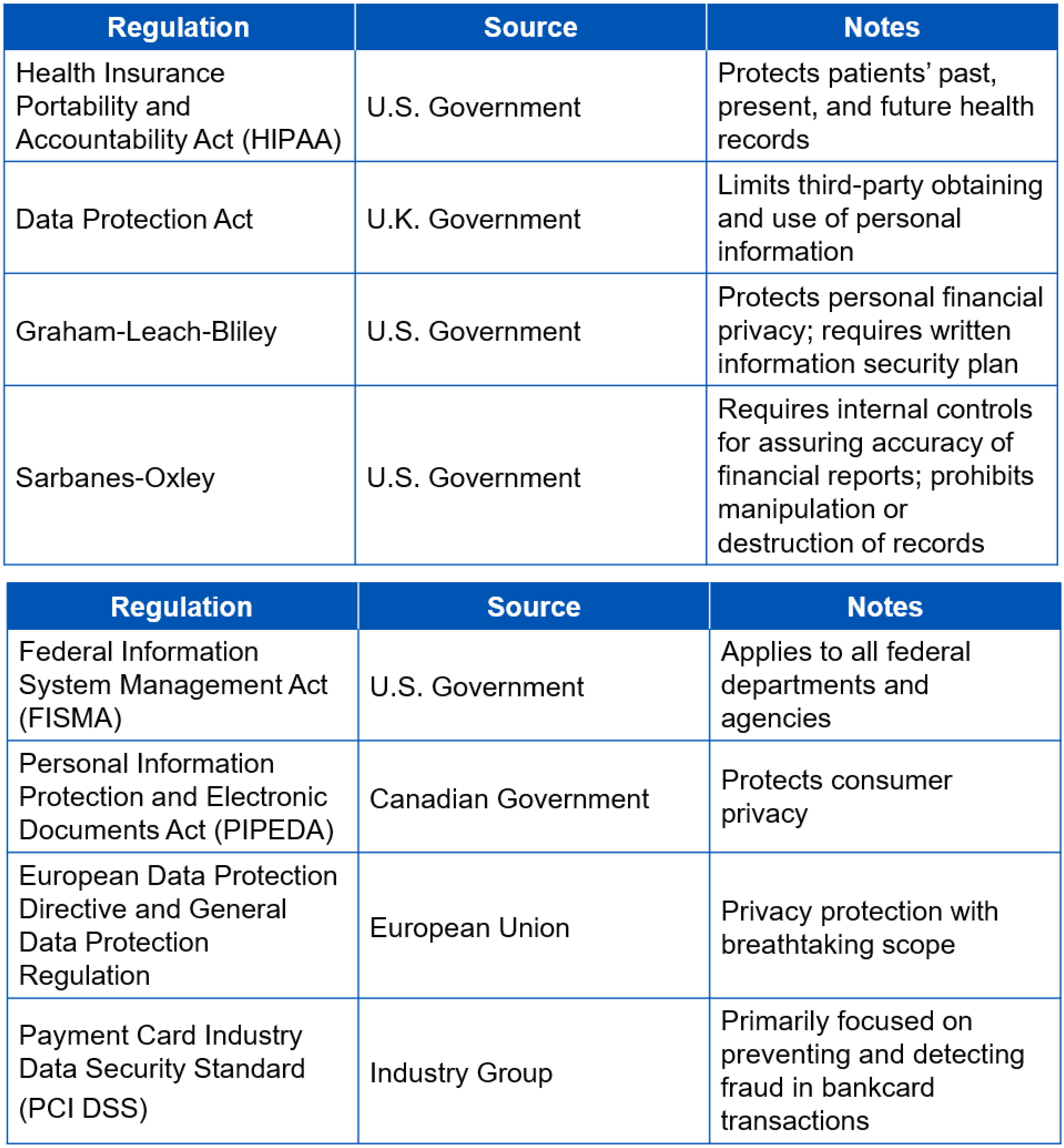
Regulatory Drivers

Cyber Security regulations refer to directives and regulatory guidelines given by governing bodies and authorities to organizations and companies; adherence to these guidelines and regulations helps companies protect their systems and information from cyberattacks.

Regulatory drivers in Cyber Security include privacy, intellectual property, or safety regulations (Vanderburg, 2005). They are derived from different levels of government, industries, and even trade groups. For example, **Payment Card Industry Data Security Standard (PCI DSS)** is a set of regulatory standards that ensures all organizations securely maintain credit card information. Similarly, the **Health Insurance Portability and Accountability Act**, also known as **HIPAA**, is a law that ensures the confidentiality, availability, and integrity of public health information (PHI).

Note, these provisions and regulations may be either mandatory or recommended. Failure to comply with these regulations may result in criminal prosecution, civil liability, or loss of confidence.

Some common regulatory drivers in the industry are shown in the table below:



Regulation	Source	Notes
Health Insurance Portability and Accountability Act (HIPAA)	U.S. Government	Protects patients' past, present, and future health records
Data Protection Act	U.K. Government	Limits third-party obtaining and use of personal information
Graham-Leach-Bliley	U.S. Government	Protects personal financial privacy; requires written information security plan
Sarbanes-Oxley	U.S. Government	Requires internal controls for assuring accuracy of financial reports; prohibits manipulation or destruction of records
Federal Information System Management Act (FISMA)	U.S. Government	Applies to all federal departments and agencies
Personal Information Protection and Electronic Documents Act (PIPEDA)	Canadian Government	Protects consumer privacy
European Data Protection Directive and General Data Protection Regulation	European Union	Privacy protection with breathtaking scope
Payment Card Industry Data Security Standard (PCI DSS)	Industry Group	Primarily focused on preventing and detecting fraud in bankcard transactions

Table 1: Common regulatory drivers used in the industry

Cyber Security Compliance

Cyber Security compliance means adhering to standards and regulatory requirements established by an agency, law, or authority group. Organizations must achieve compliance to protect the confidentiality, integrity, and availability (CIA) of data or information. The information must be protected, whether stored, processed, integrated, or transferred. Depending on the industry and sector, these standards vary, but they often require the use of a variety of organizational processes and technology to safeguard data.

The following types of data and information are subject to Cyber Security compliance:

Personally identifiable information (PII): date of birth, first/last names, address, social security number (SSN), etc.

Financial information: credit card numbers, expiration dates and card verification values (CVV), bank account information, debit or credit card personal identification numbers (PINs), etc.

Protected health information: medical history, insurance records, prescription records, etc.

> ℹ You may refer to the resources given in the Further Reading section to learn more about industry-specific compliance requirements.

How to Comply with Regulations?

Governments and companies alike are taking steps to ensure that they are complying with Cyber Security laws. These regulations include the HIPAA, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act (COPPA), etc.

In order to comply with regulations, it is important that organizations have an adequate understanding of the nature, magnitude, and probability of risks associated with potential threats (Institute of Risk Management, 2022).

Risk Assessment and Management are key to ensuring organizations are able to comply with regulations and manage risks appropriately.

Integrated Controls Management

Read Practical Guidance To Implement Governance, Risk Management & Compliance (GRC) to get an insight into how Governance, Risk and Compliance complement each other when implemented with a practical approach. As you read, focus on the following:

- What is Integrated Controls Management and how it can be used as an approach to implement GRC
- How GRC ensures that the organization is not only secure but also compliant
- How Plan, Do, Check & Act (PDCA) methodlogy is effective while implementing GRC
- How important is to document the process when implementing GRC

Conclusion

In this reading, you learned what regulatory drivers are, what some of the common regulatory drivers in the industry are, and what are some of the practical ways to implement GRC in an organization. Next, you will perform an exercise where you will determine the regulatory drivers of your assigned company.

Further Reading

Read the following article to learn more about industry-specific regulatory drivers and compliance: Celerium. (n.d.) Cybersecurity Compliance: A Comprehensive Guide. Retrieved February 14, 2023.

✓ Mark Completed

← Previous
Risk Management Case Study Presentation

Next
Cyber Security Regulations Presentation →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D2

Tue Jul 23

Outline & Notes (1)

Lectures (1)

Work (10)

10 hrs

- Project: Risk Management Case Study
- Risk Management Case Study Presentation ✓
- Regulatory Drivers & Cyber Security Compliance
- Cyber Security Regulations Presentation
- Course Reflection ✓
- Overview - Vulnerability Assessment
- Vulnerability Concepts
- Common Vulnerabilities and Exploits (CVE) List
- Vulnerability Severity
- Security Vulnerabilities Scenarios with AI

Other (1)

W05D2 Schedule »