PaymentsEd FORUM

Master Compliance

Information Security as a driver for Compliance

DRF PAYMENTS EDUCATION

Winston Hoggard
Director Compliance and Information Security
Verifi, Inc

Key Objective

- To understand how Information Security ultimately drives an organization to achieve master level Compliance.

Compliance

What is Compliance?

An adherence to standards, regulations, and other requirements.

Why is Compliance necessary?

- Legal and Regulatory requirements
- Organizational policies
- Fiduciary Responsibility
- Prevents and detects violations
- Reduces potential liability

Benefits of Compliance

Identify intentional criminal and unethical conduct

Identify weaknesses in internal systems and management structures

Allows for investigation of potential problems

Fosters a culture of ethics and adherence that is central to all of an organization's operations and activities

Identify and manage risks that impact an organization's reputation

How is Compliance integrated into an organization?

The Compliance Plan

- Comprehensive strategy
- Specific
- Conduct operations and activities
- Integrity
- Legal and regulatory requirements
- Related to its business activities

Information Security

What is Information Security?

Information Security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Information Security Plan

Highlights:

- Maps every business process
- System/Application/Person
- All information related to how an organization conducts its business
- Suggests procedural efficiencies
- Information accessibility improvements
- How to keep it all safe and relevant

Why is Infosec necessary?

A company's value is its data

Information Security protects these data assets.

Technical Controls Support Compliance

Technical controls are used to provide access to an organization's data in a manner that is consistent with its documented policies.

Preventative

- Firewall
- IPS
- Anti-Malware
- Security Awareness Training
- Jump Hosts
- Authentication
- Data Encryption
- Data Leakage Prevention
- Vulnerability Scanning
- Uninterruptible Power Supply
- Security Guard

Detective

- IDS/IPS
- System Monitoring
- Anti-Malware
- Penetration Testing

Corrective

- Backups
- Patch Management
- Anti-Malware

Compensatory

- Active Failover Site
- Backup Generator

How are Compliance & Information Security related?

Compliance falls out of the back-end of an Information Security Program done well.

What 'should' a system look like all day and monitor/report for change.

Infosec avails segmentation, configuration standards, access controls, logging and monitoring to establish a baseline. Compliance monitors and reports on changes to that baseline.

Examples of Compliance & Infosec in Action

PCI

- Prescriptive; you must do "x"

General Data Protection Regulation (GDPR)

- Principle-based; you must have reasonable controls in place to protect personal data

ISO 27001

- Best Practices

Summary

Compliance and Information Security are both essential

Each needs to be developed with a thought toward the specific activities of an organization

Each needs the support of Senior leadership in order to be effective

Leveraging Information Security as a driver for Compliance **WILL** lead to master Compliance

Questions

Winston Hoggard, Director Compliance & Information Security

P: 323-655-5789

E: winston.hoggard@verifi.com

If you have any questions about the presentation, go to our LinkedIn Group (the Payments Education Forum) and request an invitation (this is a closed group specifically for the payments industry).