Practical SQL Server Security, Compliance, and Auditing

UNDERSTANDING REGULATORY COMPLIANCE

Russ Thomas
DATABASE MANAGER

@sqljudo www.sqljudo.com

Course

Security

- User Security
- Data Security

Compliance

- Policy
- Agreements
- Professional Standards
- Statutes and Laws

Auditing

- Establishing Proof

Abacos Widgets

Compliance Applies to Nearly All of Us

Government & Non Profit

Publicly Traded Companies

Private Organizations

Major Concerns of Data Compliance and Accreditation Processes

Securing Sensitive and/or Personal Data

Organizational Transparency and Accuracy

Auditing

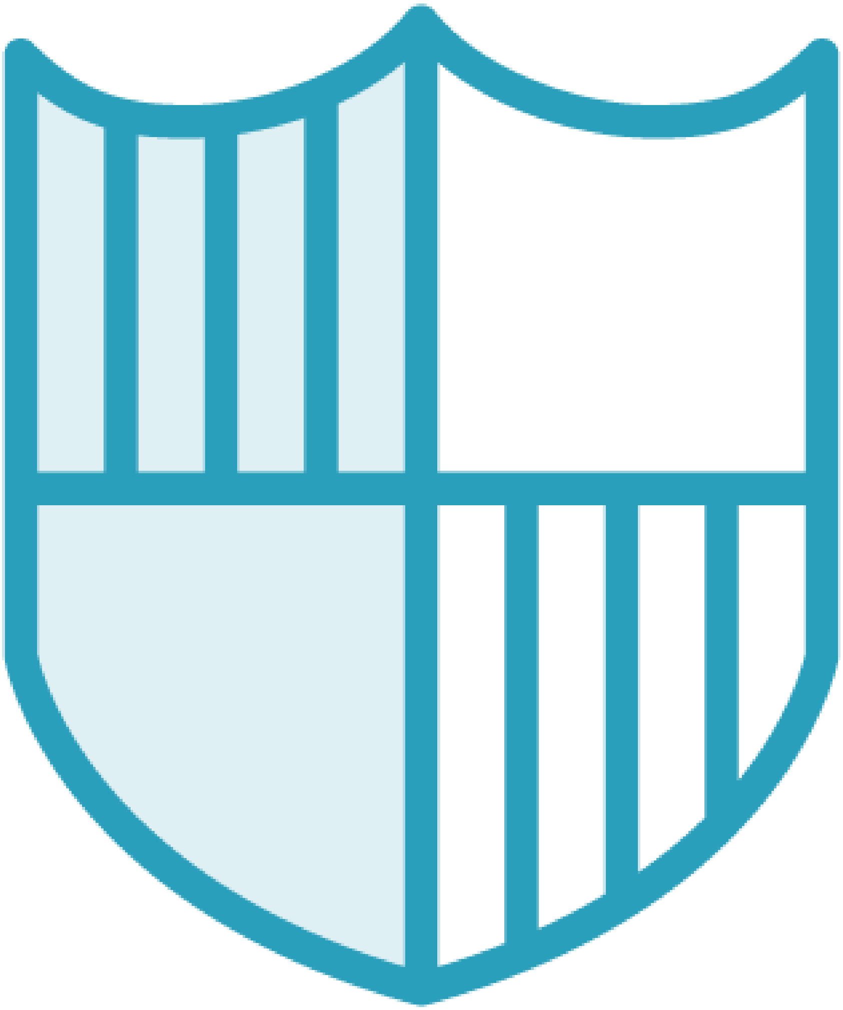
Typical Regulatory Acts and Standards

PCI

HIPAA

SOX

Misc.



No matter the compliance category or process, it always comes down to “proving it” during and audit

Modules

1. Understanding Regulatory Compliance
2. Implementing Security with Users, Groups, and Roles
3. Modeling Schemas to Support Security Best Practices
4. Protecting Sensitive Data with Encryption
5. Protecting Sensitive Data In-Transit
6. Setting up Compliance Enforcement, Monitoring, and Logging
7. Watching the Watcher with SQL Audit
8. Passing Audits with Compliance Reports and Documentation
9. Miscellaneous Tips and Tricks

Typical Regulatory Acts and Standards

PCI

HIPAA

SOX

Misc.

Health Insurance Portability & Accountability Act

1. Amend Internal Revenue code 1986
2. Improve portability and continuity
3. Combat waste, fraud and abuse
4. Promote medical savings accounts
5. Improve access to long term coverage
6. Simplify administration of insurance
7. Other purposes

Health Insurance Portability & Accountability Act

Title 1

- Health Care Access, Portability, and Renewability

Title 2

- Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform

Title 2

2.1 Privacy Rule

2.2 Transactions and Code Sets Rule

2.3 Security Rule

2.4 Unique Identifiers Rule

2.5 Enforcement Rule

Violations Can Bring

1. Fines and Penalties

2. Criminal Charges

3. Civil Lawsuits

4. Affects Many Organizations

Sarbanes-Oxley Act of 2002

1. Protect shareholders and the general public from errors and fraud

2. Improve accuracy of corporate disclosures

3. SEC administers the act

Sarbanes-Oxley Act of 2002

Result of unethical practices and accounting practices which lost many employee retirement accounts and investments when revealed

Sarbanes-Oxley Act of 2002

Primary tenants of act that concern those who work with databases is ensuring that data is protected by

Transparency and Accuracy

Controls

Security

Documentation

PCI-DSS

Payment Card Industry Data Security Standard

Violations are typically not criminal, but can lead to significant liability or inability to conduct business within the payment industry

NEWS
Lorem ipsum dolor sit amet, pede et congue viverra velit placerat, amet nec mauris nullam justo ac praesent. Urna maecenas in neque, ridiculus aliquam sodales nec turpis volutpat
Et neque laoreet arcu egestas at. Vel hendrerit nisl, curabitur fermentum. Lectus ligula magna. Rhoncus mollis habitasse etiam in, bibendum imperdiet placerat lorem justo quam, cras fames purus elementum velit eget, dictumst arcu, maecenas

Loss of card holder data is often most harshly felt in the court of public opinion and the loss of customer confidence

Security is the primary concern of PCI

- Proving compliance to standards of data security and encryption
- Establishing that environments where card holder data is stored adhere to standards
- Maintaining logs and historical evidence

Internal Policy Compliance and Audits

- Change control management
- Source control management
- Sensitive data
- Backup regularity
- Failover / DR tests

Up Next:

Our First Hands-On Module

Implementing Security with Users, Groups, and Roles