In this executive brief we examine regulatory compliance requirements and their impact on technology and security initiatives within organizations. We specifically review the following legislations:

- Sarbanes-Oxley (SOX)
- Payment Card Industry (PCI)
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Food and Drug Administration’s Title 21 CFR
- Basel II and several other international regulations including PIPEDA

We also review privacy legislations enacted by several state governments in the United States. We then examine the COSO and COBIT frameworks as well as the ISO 27001 and 17799:2005 Standards. Next, we review the importance of contingency planning, its requirement in legislations and international standards. Finally, we establish best practice recommendations for enabling an enterprise that meets compliance requirements and whose information infrastructure security is resilient, robust and roving.
This Executive Brief is based on content that was developed by ecfirst.com Academy for the Certified Security Compliance Specialist™ (CSCS™) program. This is an in-depth 2-day program that is presented once a month in select cities across the United States by Ali Pabrai, chief executive, ecfirst.com, an Inc. 500 Business and a firm endorsed by the American Hospital Association (AHA).

The schedule and detailed information about the Certified Security Compliance Specialist™ (CSCS™) program is available at [www.ecfirst.com](http://www.ecfirst.com).

### Table of Contents

I. The Compliance Challenge
   - Penalties for Non-compliance
   - North American Electric Reliability Council (NERC)
   - U.S. State Regulations
   - International Regulations
   - Basel Background

II. Financial Industry and Information Security
   - Gramm-Leach-Bliley (GLB)
   - Sarbanes-Oxley (SOX)
   - Payment Card Industry (PCI)
   - Federal Financial Institutions Examination Council (FFIEC)
   - Getting Started with COSO and COBIT

III. Health care Industry and Information Security
   - Health Insurance Portability and Accountability Act (HIPAA)
   - Food and Drug Administration’s Title 21 CFR

V. U.S. Government Security Certification & Accreditation
   Federal Information Security Management Act (FISMA)
   Federal Information Processing Standards (FIPS)

VI. Contingency Planning and Security
   Business Impact Analysis (BIA)
   Getting Started
   Summary

VII. Best Practices
   Business Nervous System
   Under Siege: Rising Threat
   Core Security Objectives
   The Seven Steps to Enterprise Security
   Business Security Goals
   Best Practice Recommendations

Case Study I: Compliance and Single Sign-On (SSO)
   Getting Started with SSO
   Questions for Your Potential SSO Vendors
   Scenario: Identity Management Best Practice

Case Study II: Compliance and Encryption
   Create an Encryption Policy

Case Study III: Audit and Monitoring
   Create an Information Audit Policy
   Product Review: Microsoft’s MBSA
   Product Review: Nessus
   Product Review: eEye’s Retina Network Security Scanner

Appendix A: CSCS™ Program
Appendix B: About ecfirst.com
Appendix C: Managed Compliance Services Program for HIPAA
Appendix D: Endorsements
   About the AHA
   About the U.S. Department of Veterans Affairs
Appendix E: About the Author