

Developing and Implementing an Information Security and Control Standards Program

Mike Seifert
Fiserv
May 18, 2011





Fiserv Overview

- Serves more than 16,000 financial institutions worldwide
- 20,000 associates in 230 worldwide locations
- More than 500 products and services
- \$1 trillion in payments transactions annually
- 6+ billion ATM/debit card transactions annually
- 75% of US online bill payment volume
- 300+ million e-bills annually
- Account processing for 1 of every 3 US FI's

fiserv.



Topics

- The Aha! Moment: Knowing it's time to revamp
- Pick Your Poison: Choosing the right external reference standard
- Build Your Army: Identifying SME's and organizing for effective standards development
- Baby and Bathwater: Ensuring continuity with existing content
- Round the Bases: Executive sponsorship, approval and endorsement
- Hearts and Minds: Communicating and training to drive adoption and alignment
- Showing Backbone: Monitoring and enforcing standards compliance
- Continuous Improvement: Creating and learning from feedback loops



Introduction



Fiserv's Definition of Security Standards

- *A set of security features and/or internal controls to be provided by a system or other technologies in order for it to be deemed suitable for use in Fiserv's Corporate or Production technology environments and in accordance with Fiserv's Security and Controls policy*



When Security is not really Secure...

- Enterprise security is typically driven by regulatory and compliance needs
- Information Security and Internal Controls primarily designed around compliance will only partially meet the true security requirements of your organization
- Organizations are meeting compliance requirements but are they really 'doing the right' thing with regards to security?
- **Are your security efforts and resources really making you more secure?**



Risk Process Approach



Risk Process Implementation Components

- Six implementation components were identified as essential for Fiserv

Standards Program Key Components

The Aha! Moment	Pick Your Poison	Build Your Army/ Baby and Bathwater	Round the Bases/ Hearts and Minds	Showing Backbone	Continuous Improvement
Goals	Frameworks	Subject Matter Expertise	Change Management/ Communications	Enforcement	Continuous Improvement
<ul style="list-style-type: none">• Clearly define objectives, rationale and expected benefits	<ul style="list-style-type: none">• Utilize widely-adopted industry standards• Provides a credible basis for design and completeness	<ul style="list-style-type: none">• Credible• Realistic• Ensure continuity• Decision Rights	<ul style="list-style-type: none">• Top-down and bottom-up approach• Distributed responsibilities• Education• Frequent communication	<ul style="list-style-type: none">• Partner with Corporate Audit• Monitoring processes and technology• Relate to everything else!	<ul style="list-style-type: none">• Feedback processes• Incident/Risk identification and anticipation activities• Integration with other risk processes

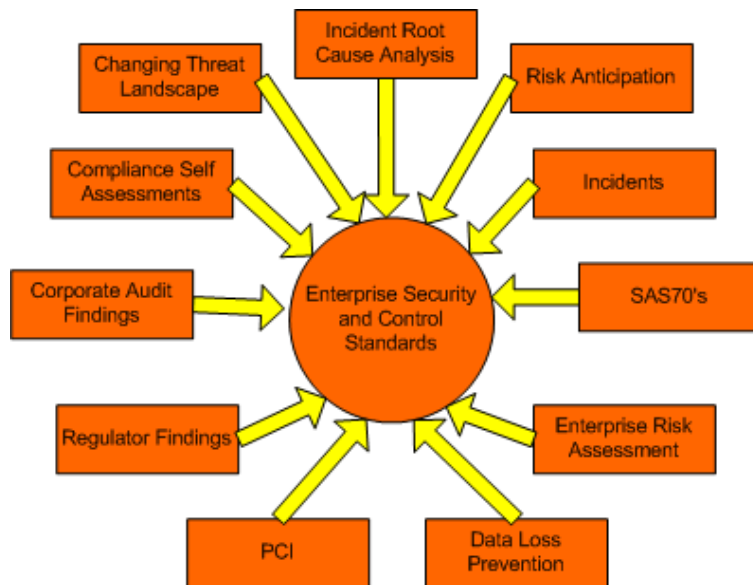
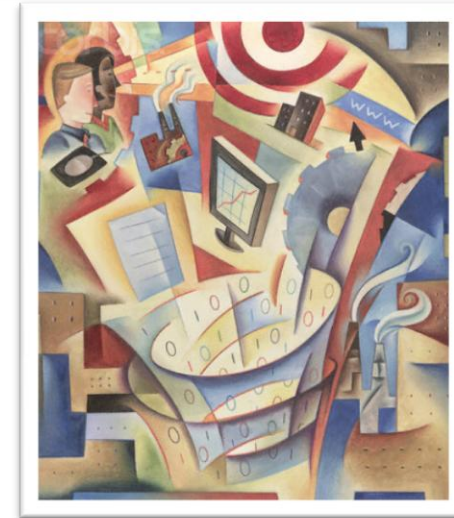


The Aha! Moment



Knowing It's Time to Revamp

- Organizations must realize that attaining and achieving compliance is not sufficient
- Overall security and risk management postures must mature
- Difficult to do in decentralized environments



- Enterprise standards for security and internal control are essential
 - Get everyone on the same page
 - 'Set the bar'
 - Manage continuous change
- The migration of Fiserv from a holding company to operating company structure required common Security and Control Standards



Security AND Control Standards

- The Fiserv standards program addresses both security standards and internal control standards for technology management
- Our 'controls focus' provides guidance on areas of internal control beyond typical security standards
 - Logging/Monitoring
 - Auditing
 - Approvals
 - Other process controls
- All internal communication materials refer to 'Security and Control Standards' or our 'Security and Controls Policy'
 - 'and Controls' is added to all references to ensure consistency and stress the importance



Pick Your Poison



Choosing The Right External Reference Standard

- Many organizations expect frameworks to illustrate the actual controls they should have in place
- Your selection of a control framework is important and should guide the design of your internal controls
- Fiserv's Approach: ISO 27001





Leverage Your Framework as a Guide

- Content for the Fiserv standards was organized according to the ISO 27001 framework
- Base content was derived from existing standards and updated to ensure control objectives and activities in the framework were met
- Content to address gaps was developed by Subject Matter Experts and incorporated into standards
- Standards were reviewed and updated to address critical areas of internal control

ISO Benchmarking Analysis Example

7	A.11 - Access control	A.11.2 User access management	User registration
			Privilege management
			User password management
			Review of user access rights
		A.11.3 User Responsibilities	Password use
			Unattended user equipment
			Clear desk and clear screen policy
		A.11.4 Network access control	Policy on use of network services
			User authentication for external connections
			Equipment identification
			Remote diagnostic and configuration port protection
			Segregation in networks
			Network connection control
			Network routing control
			Secure log-on procedures
A.11.5 Operating system access control	User identification and authentication		
	Password management system		
	Use of system utilities		
	Session time-out		



Clear Alignment With an Industry Standard

- The Fiserv standards are organized by Control Objective and Control Activity per the ISO framework.
- Enables other compliance activities

ISO 27001 Framework

Security Domain	Control Objective Name	Control Activity Name
Communications and operations management	Media Handling	Management of removable media
		Disposal of media
		Information handling procedures
		Security of system documentation
	Exchange of information	Information exchange policies and procedures
		Exchange agreements
		Physical media in transit
		Electronic messaging
		Business information systems

8. Media Handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

8.1. Management of Removable Media

There shall be procedures in place for the management of removable media.

... requires data and media containing data, to be used, stored and disposed of in accordance with the **Fiserv Information Asset Protection and Privacy Standards**. These standards define guidelines for classifying, labeling and handling data and media, and apply to all media types including removable media.

... support for external storage and general access to PC USB ports must be disabled in high-risk environments such as customer care facilities. Users are prohibited from storing sensitive company data on any external storage media (including CD/DVD) without appropriate security controls including encryption.

General Control Objective and Description from Framework

General Control Activity and Description from Framework

Fiserv Specific Standards that Address Framework Requirements



Build Your Army



Identifying SME's and organizing for effective standards development

- Security and Control Standards should be aspirational, not validation of what is already in place
- Standards development requires thought leadership and extensive input from Subject Matter Experts
- A centralized function should have responsibilities for organizing content and coordinating all efforts
- Fiserv's approach...





Baby and Bathwater



Ensuring continuity with existing content

- Adoption of new standards does not happen overnight
- Although standards should reflect a state you aspire to attain, be realistic and reasonable
- Offer opportunities for effective compensating and mitigating controls
 - Focus on framework intentions
- Assess how far you are from full compliance

INSTRUCTIONS:			Data Centers/Facilities							Online Banking				
1. Identify your major facilities including office and data center locations and fill in the fields on row 7 in columns E through K. You may insert additional columns if necessary. 2. Identify your major products/service technology environments and fill in the name fields on row 6 starting in column L. You may insert additional columns for additional environments if necessary. 3. Assess each of the standards from columns B-C in the context of how that standard applies to each of the facility and technology environment columns. For each box in the assessment, fill in the standard status per the below key to indicate whether you are in compliance with the standard or not (values, n, y or p). 4. Some boxes have been pre-filled as 'not applicable'. If you feel that a standard is not applicable to a particular location or environment, enter an 'x' in the box to indicate this. 5. Once the matrix has been completely filled out, run the macro to generate the Gap Details template. Only run the macro after you have completely filled in the matrix since it will overwrite any existing data in the Gap Details tab.														
N NO identified exception Y An exception IS identified P PARTIAL exception identified C Standard covered by CORPORATE X Does not apply in context			Data Center 1	Data Center 2	Office 1	Custom or Care Center	Facility 5	Facility 6	Facility 7	Application Platform/OS	Database	Network		
Standards Document	Control Objective	Control Activity												
1	Information Asset Protection and Privacy	1. Information Classification	1.1 Classification guidelines	y	y	y	y	n	n	n	x	x	x	
			1.2 Information labeling and handling	n	y	n	n	n	n	n	x	x	x	
		2. Responsibility of Assets	2.1 Inventory of assets	n	n	n	n	n	n	n	y	y	y	
		2.2 Ownership of assets	n	n	n	n	n	n	n	n	n	p	p	
		2.3 Acceptable use of assets	n	n	n	n	n	n	n	x	x	x	x	
		3. Data Retention and Disposal	3.1 Data Retention	y	n	n	n	n	n	n	n	n	n	
2	Physical and environmental security	1. Secure areas	3.2 Data Disposal	p	p	n	n	n	n	n	n	n	n	
			1.1 Physical security perimeter	n	n	n	n	n	n	n	n	x	x	x
			1.2 Physical entry controls	n	n	n	n	n	n	n	n	x	x	x
			1.3 Securing offices, rooms, and facilities	n	n	n	n	n	n	n	n	x	x	x
			1.4 Protecting against external and environmental threats	n	p	n	n	n	n	n	n	x	x	x
			1.5 Working in secure areas	n	p	n	p	n	n	n	n	x	x	x
		1.6 Public access, delivery, and loading areas	n	n	n	n	n	n	n	n	x	x	x	
		2. Equipment security	2.1 Equipment siting and protection	n	n	n	n	n	n	n	n	x	x	x
			2.2 Supporting utilities	n	n	n	n	n	n	n	n	x	x	x
			2.3 Cabling security	n	n	n	n	n	n	n	n	x	x	x
			2.4 Equipment maintenance	n	n	n	n	n	n	n	n	x	x	x
			2.5 Security of equipment off-premises	y	y	y	n	n	n	n	n	x	x	x
			2.6 Secure disposal or re-use of equipment	n	n	n	n	n	n	n	n	x	x	x
			2.7 Removal of property	n	n	n	n	n	n	n	n	x	x	x
			1.1 Documented operating procedures	n	n	n	n	n	n	n	n	n	n	



Round the Bases



Executive Sponsorship, Approval and Endorsement

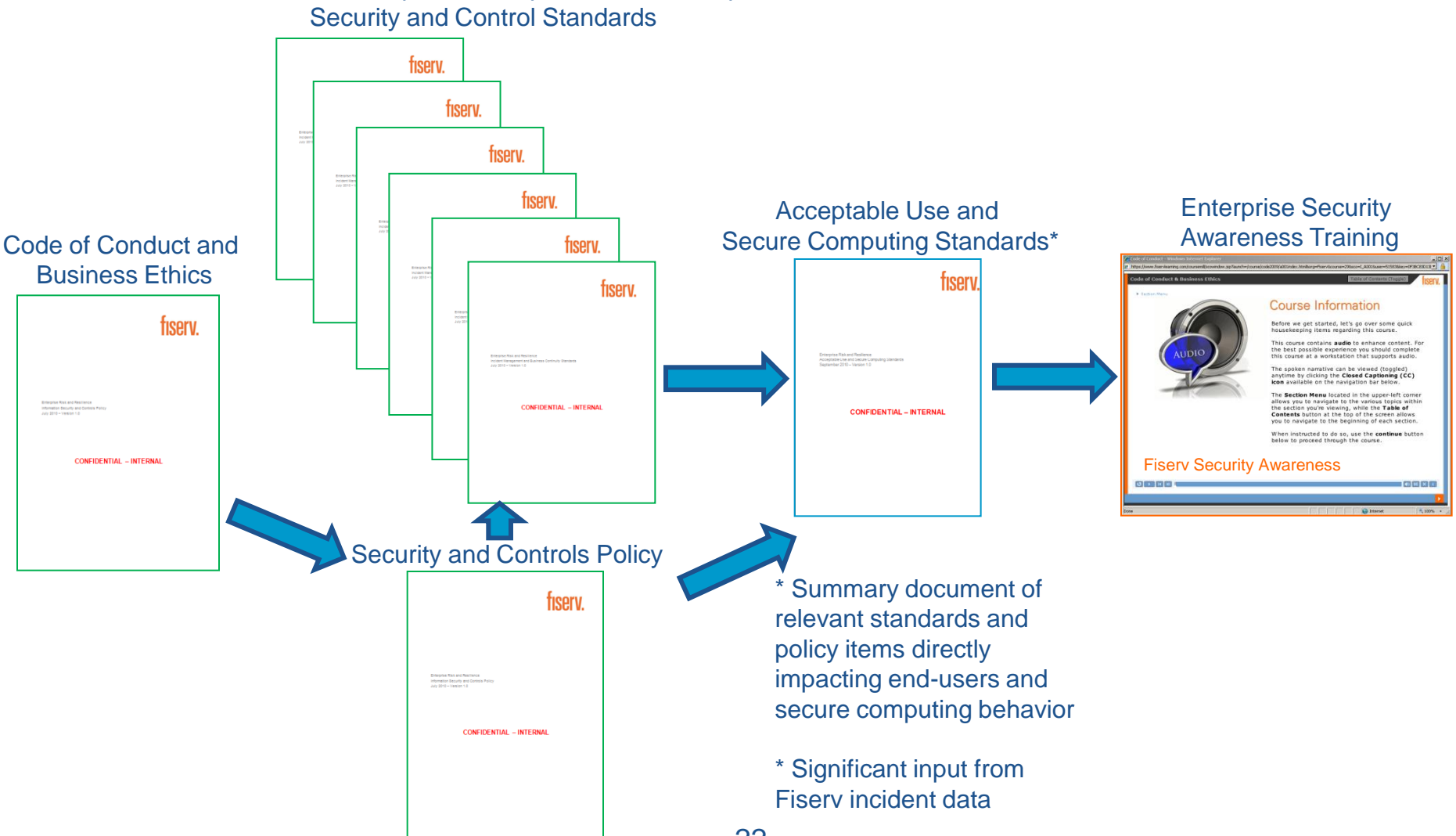
- Effective change management is essential
- Change management requires both top-down and bottom-up approaches
- Important: Your change management efforts should clearly illustrate the logic, intentions and background that went into your standards program





Enterprise Alignment of Standards and Policy Content

- Fiserv's program is designed to ensure alignment with Enterprise strategy, Fiserv values and to communicate the correct 'Tone from the Top' on the importance of this topic.





Hearts and Minds



Communicating and training to drive adoption and alignment

- Partner with communications and marketing groups
- Promote your standards and resources any chance you get
- Integrate with your Security Awareness and other Enterprise Training Programs
- Fiserv's approach...



Showing Backbone



Monitoring and enforcing standards compliance

- Acceptable use standards/practices are monitored and reinforced by the Fiserv Data Loss Prevention, Security Monitoring Center and Incident Management programs

Incident 01005100

Status: **New**

SMTP

Severity: **High**

Key Info | History | Notes | Correlations

Policy Matches

Policy	Matches
Confidential Documents - SMTP [view policy]	3
Confidential-Sensitive or Internal (Keyword Match)	2
Confidential-Sensitive or Internal (Recipient)	1

Incident Details

Server: [BKF - Mail Prevent 04](#)

Date: 4/12/11 2:21 PM

Sender: [Mike.Seifert@fiserv.com](#)

Recipient: [mikejseifert@gmail.com](#)

Subject: [Important Stuff \(test\)](#)

Attachments: [TEST Information Security Policy-V1-FINAL.doc](#)

Message Body

This is the important stuff...

(test)

Michael Seifert

CISSP, CISM, CISA, CGEIT
VP - Risk Process

Enterprise Risk and Resilience
Fiserv
Office: 262.879.5824
Mobile: 262.309.1350
www.fiserv.com <<http://www.fiserv.com>>

P Please consider the environment before printing this e-mail

Matches (matches found in 2 components)

Header (1 Match):

mikejseifert@gmail.com

TEST Information Security and Controls Policy-V1-FINAL.doc (2 Matches):

... **CONFIDENTIAL - SENSITIVE**
<header> Fiserv Enterprise R...
</header> <footer> 2010 Fiserv, Inc. **Confidential - Internal** Information. Do Not...

Attributes

Lookup Edit

Default Attribute Group

First Name: [Mike](#)
Last Name: [Seifert](#)
Title:
Department:
Employee Number: [51583](#)

Predefined

Resolution:
Dismissal Reason:
Assigned To:
Business Unit:
Employee Code:
Sender Email:
Phone:
Manager First Name: [Murray](#)
Manager Last Name: [Walton](#)
Manager Email: [Murray.Walton@fiserv.com](#)

Incident Actions | Report

1-50 of 56 | Show All | Select All

Type	Subject / Sender / Recipient(s)	Sent	ID / Policy	Matches	Severity	Status
<input type="checkbox"/>	Subject: Important Stuff (test) Sender: Mike.Seifert@fiserv.com Recipient: mikejseifert@gmail.com	4/12/11 2:21 PM	01005100 Confidential Documents - SMTP	3	High	New

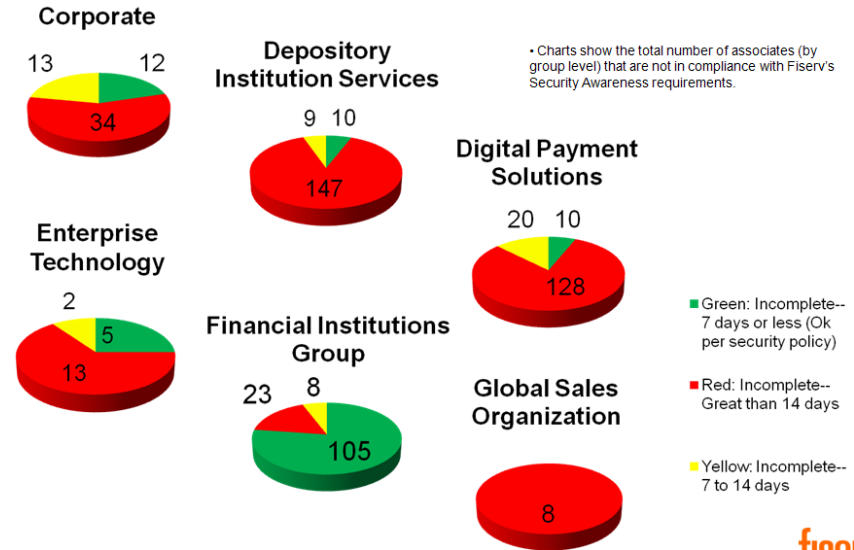


Monitoring and enforcing standards compliance

- A reliable data source and consistent metrics – “single source of truth” – are essential for monitoring and enforcing compliance

Group	Total Associates	# Complete	% Complete
Corporate	3071	3012	98.1%
Depository Institution Services	7302	7136	97.7%
Digital Payment Solutions	5217	5059	97.0%
Enterprise Technology	1030	1010	98.1%
Financial Institutions Group	2141	2005	93.6%
Global Sales Organization	341	333	97.7%
Grand Total	19102	18555	97.1%

Green: >=97%
 Yellow: >=95% and <97%
 Red: <95%





Continuous Improvement



Creating and Learning From Feedback Loops

- Feedback must be solicited
- Risk/threat environments, incidents, audit findings, and other inputs should be monitored to identify improvement opportunities and detect areas for standards refinement
- Incident post mortems are excellent vehicle for reinforcing standards and identifying refinement needs
- No standards are perfect . With eyes wide open, accept constructive feedback and adjust accordingly



Questions?

Mike Seifert
Vice President – Risk Processes
Fiserv – Enterprise Risk & Resilience
262.879.5824
mike.seifert@fiserv.com

