



SRM – Security Resource Management

A Framework to Support Communications and Boost IT Security

- Ken Leeser, President, Kaliber Data Security

trite



trite: *adjective*

lacking in freshness or effectiveness
because of constant use or excessive
repetition. Hackneyed. Stale.



**2 trite themes we hear all
the time in information
Security**



“We need to take a risk-based approach to IT security”



“We need better communications between IT and Management (Administration)”



Are these themes related?

Let's Explore





Risk-based Approach to Security Management



“The State of Risk-Based Security Management”
Ponemon Institute, 2012

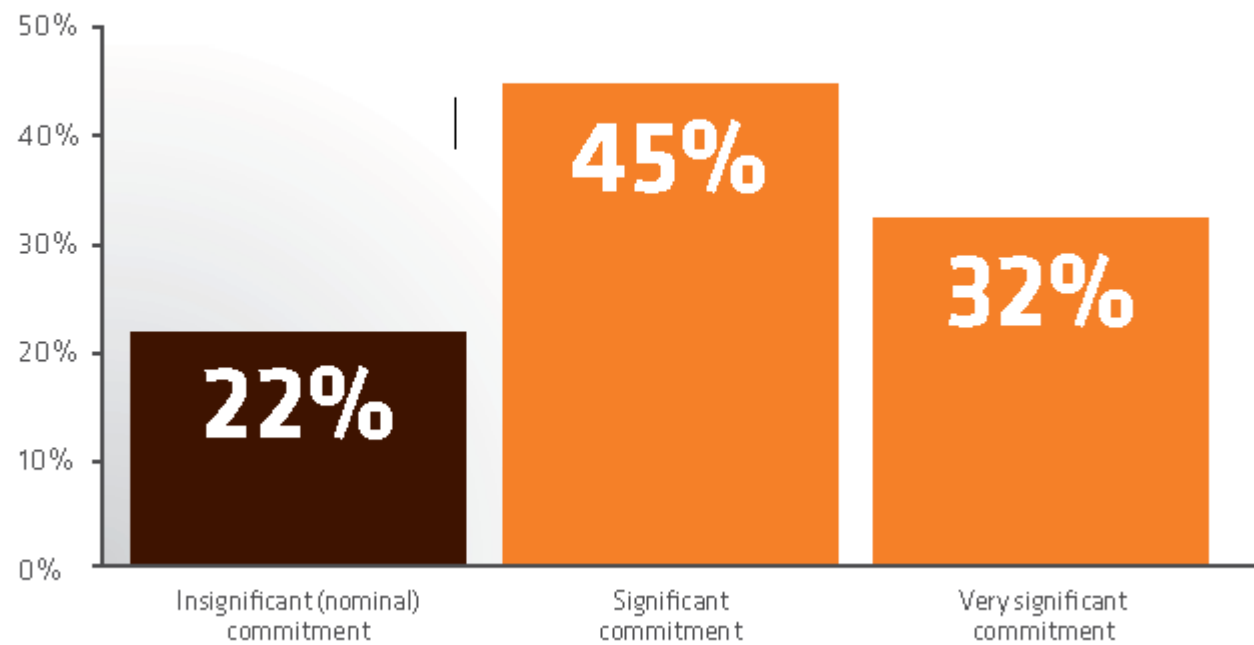


KEY FINDINGS AND ANALYSIS

Commitment to RBSM is high.

“Respondents believe that risk assessments can help assign values to risk, obtain actual costs related to an incident and predict the frequency and impact of future security incidents.”

FIGURE 5. Commitment to RBSM

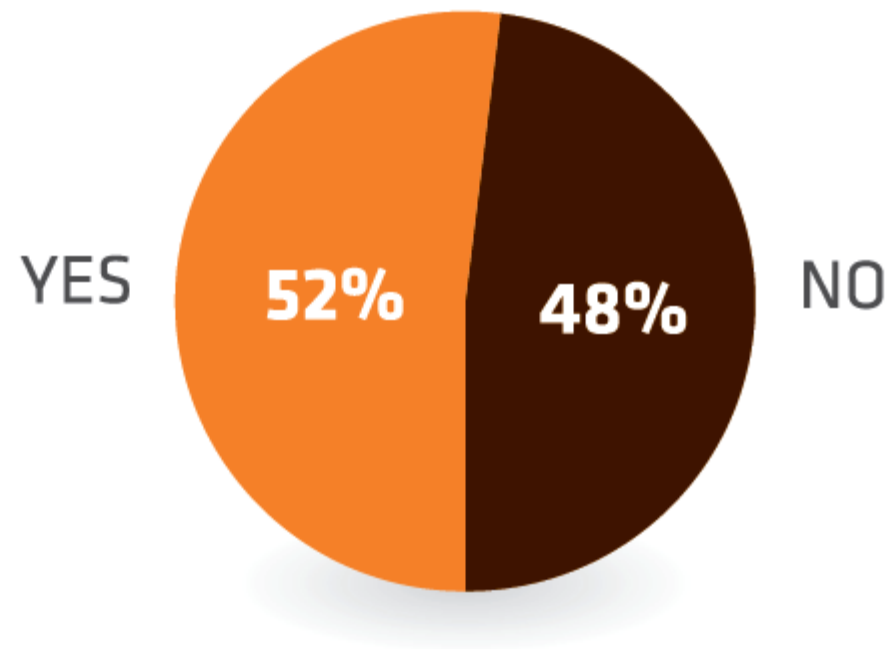


REALITY

Only about half of the organizations in the study have a formal RBSM program.

Most of these are only partially implemented.

FIGURE 6. Existence of a formal RBSM function, program or set of activities



Drill Down on the Details



FIGURE 9. First set of steps to assess, prioritize and manage security risks
Partially completed and Fully completed response combined

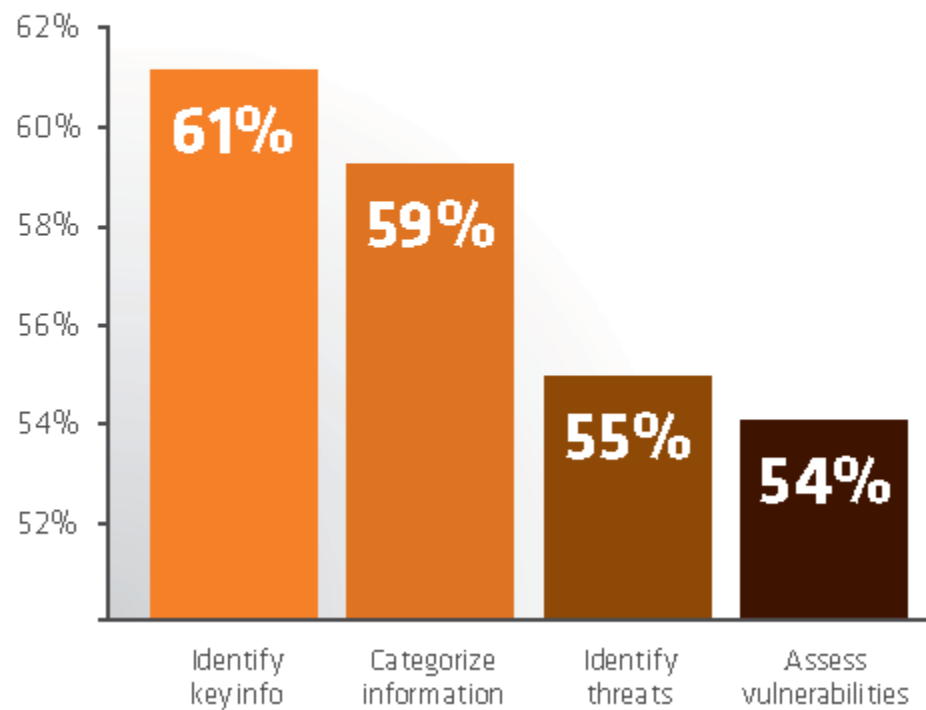
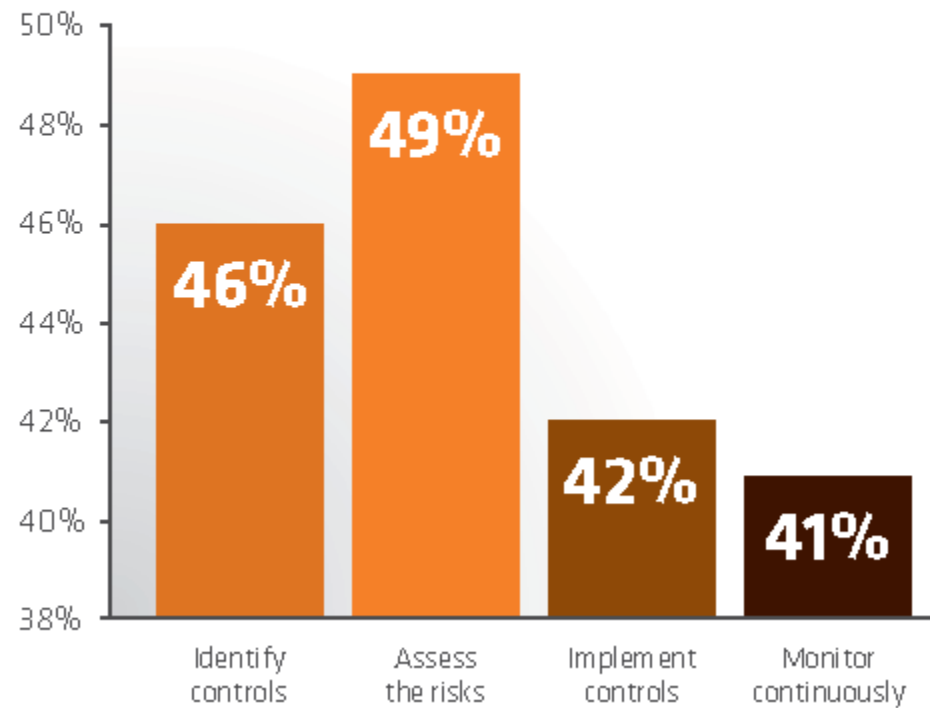


FIGURE 10. Second set of steps
to assess, prioritize and manage security risks
Partially completed and Fully completed response combined





2 Contradictory Statistics



87% of organizations are
'committed' to Risk-Based
Security Management



Only 52% actually have a
Risk-Based Security
Management program

Why?



2 Reasons



No Metrics

“Without a scorecard difficulty getting senior level support, funding and resources.”



No Framework

“An effective RBSM framework aligns organizational effort, metrics, and indicators drives more effective security expenditures.”

Without a Framework Implementing Risk Based Security Management is a Daunting Task



Identify Info

Assets

Threats

Vulnerabilities

Controls

Risk

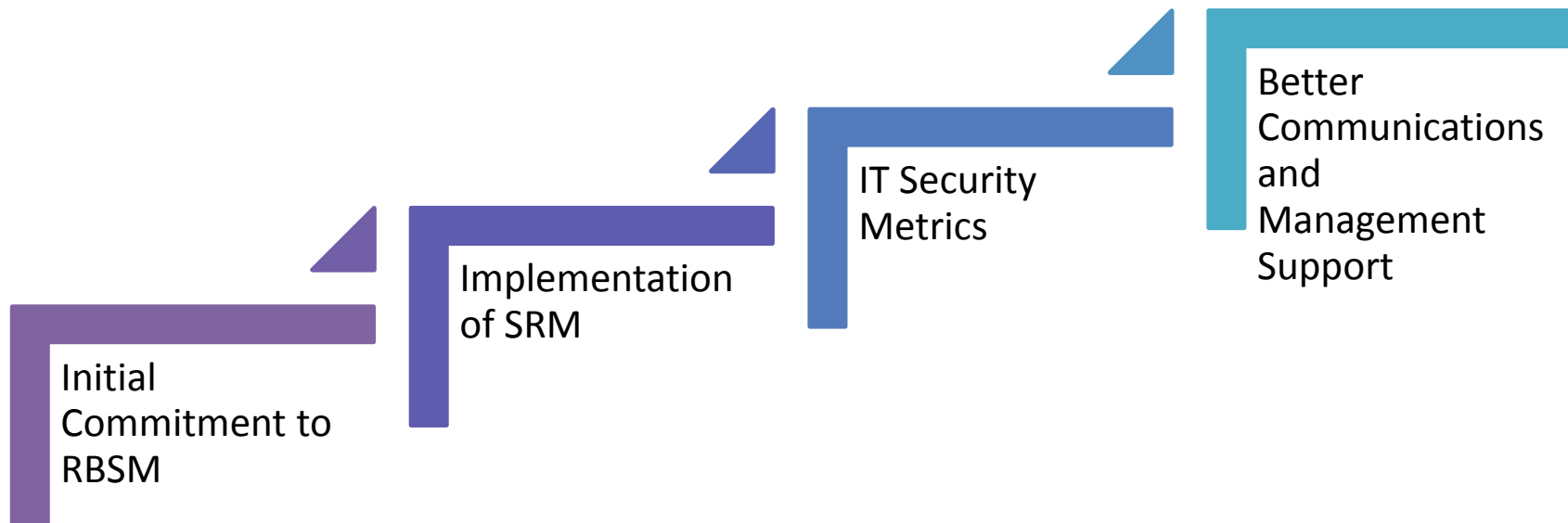
Monitoring

Where do we Begin?



SRM Tools Can HELP: Security Resource Management

23



SRM is CRM for IT Security



SRM FRAMEWORK



Identify Info

Assets

Threats

Vulnerabilities

Controls

Risk



METRICS

Things to look for in an SRM System





#1: Unified Compliance Framework Integration



UCF – Provides Detailed Mapping



Authorities -> Citations -> Controls

 UNIFIED COMPLIANCE FRAMEWORK														
 Harmonized Control Title	Control ID	Banking and Finance Guidance	Energy Guidance	Healthcare and Life Sciences	NASD NYSE Guidance	NIST Guidance	Payment Card Guidance	Records Management Guidance	Sarbanes Oxley Guidance	US Federal Privacy Guidance	US Federal Security Guidance	US Internal Revenue Guidance	US State Laws and Protectorates Guidance	Internal Guidance
		Banking and Finance Guidance	Energy Guidance	Healthcare and Life Sciences	NASD NYSE Guidance	NIST Guidance	Payment Card Guidance	Records Management Guidance	Sarbanes Oxley Guidance	US Federal Privacy Guidance	US Federal Security Guidance	US Internal Revenue Guidance	US State Laws and Protectorates Guidance	Internal Guidance
Acquisition of facilities, technology, and services	01123	4				2		1			1	1		
Allocate sufficient resources, as part of the capital planning process, to protect information systems.	01444					1					1	1		
Define security requirements and/or specifications in information system acquisition contracts.	01124	1				2	2				2	1		
Define operational requirements and required service levels in acquisition contracts.	00825										1			
Define the security controls in acquisition contracts and ensure they are cost-effective.	01125	1				1					2			
Ensure systems documentation is provided when acquiring software.	01445	1				1			1		1	1		
Ensure the information system developer has a configuration management plan for all newly acquired IT assets.	01446					1					1			
Ensure the information system developer creates a security test and evaluation plan, implements the test, and provides the test results for all newly acquired IT assets.	01447					1					1			
Identify and consider alternative courses of action to meet security requirements when acquiring IT assets.	01128													
Conduct an acquisition feasibility study for acquiring off-the-shelf or customized products.	01129	1												
Establish development and test environments to support feasibility and integration testing of applications prior to acquisition.	01130						3					1		
Analyze the proposed information architecture as it pertains to acquisition feasibility.	01132													
Establish and maintain an acquisition strategy for acquiring outsourced or off-the-shelf products and/or services.	01133	2						2						
Ensure third-party outsourcing providers meet organizational standards and employ adequate compliance controls.	01134	2				2			1		1	1		
Conduct a risk analysis of major acquisition project to														

Regular Authority Updates



Vendors

RSA Archer

Bwise

LockPath

TruOps

TraceSecurity

Vendors

- RSA Archer
- Bwise
- LockPath
- TruOps
- TraceSecurity

#2: Ease of Implementation

33



SRM Implementation



Step 1: Identify Authority Documents

<input checked="" type="checkbox"/>	Active Authority Documents
<input checked="" type="checkbox"/>	34 CFR Part 99 ⓘ
<input checked="" type="checkbox"/>	HIPAA ⓘ
<input checked="" type="checkbox"/>	Massachusetts 201 CMR 17.00 Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts ⓘ
<input checked="" type="checkbox"/>	PCI DSS 2.0 ⓘ

Search:

Select Additional Authority Documents

- Asia and Pacific Rim Guidance
- Banking and Finance Guidance
- Energy Guidance
- EU Guidance
- General Guidance
- Healthcare and Life Science Guidance
- ISO Guidance

Step 2: Itemize Assets

CSV XLS XML

Expand/Collapse All

+ Add Asset Showing 1 to 7 of 7 entries

Asset	Description	Confidentiality	Integrity	Availability
Data Center	The organization's primary area housing IT systems	High	High	High
Exchange Servers	Server class information systems	Medium	Medium	High
Mobile Device	Mobile Tablet	High	Medium	Low
Network	Firewalls, routers, switches, LAN, and WAN	Low	Medium	High
Organization	Asset for assigning entity-level threats / controls	High	High	High
Servers	Server class information systems	High	Medium	High
XYZ Application	Database application	High	Medium	Very High

Step 3: Evaluate pre-defined threats

Select your method of adding threats

Add Threat(s) to Single Asset Add Threat(s) to Multiple Assets Remove Multiple Threats

[Expand/Collapse All](#)

Add Threat **Data Center**

- [-] Tier 2: Data Center
 - Unauthorized Access
 - Loss / Destruction of Equipment
 - Natural Disaster
 - Flooding
 - Power Loss
 - Fire

Add Threat **Exchange Servers**

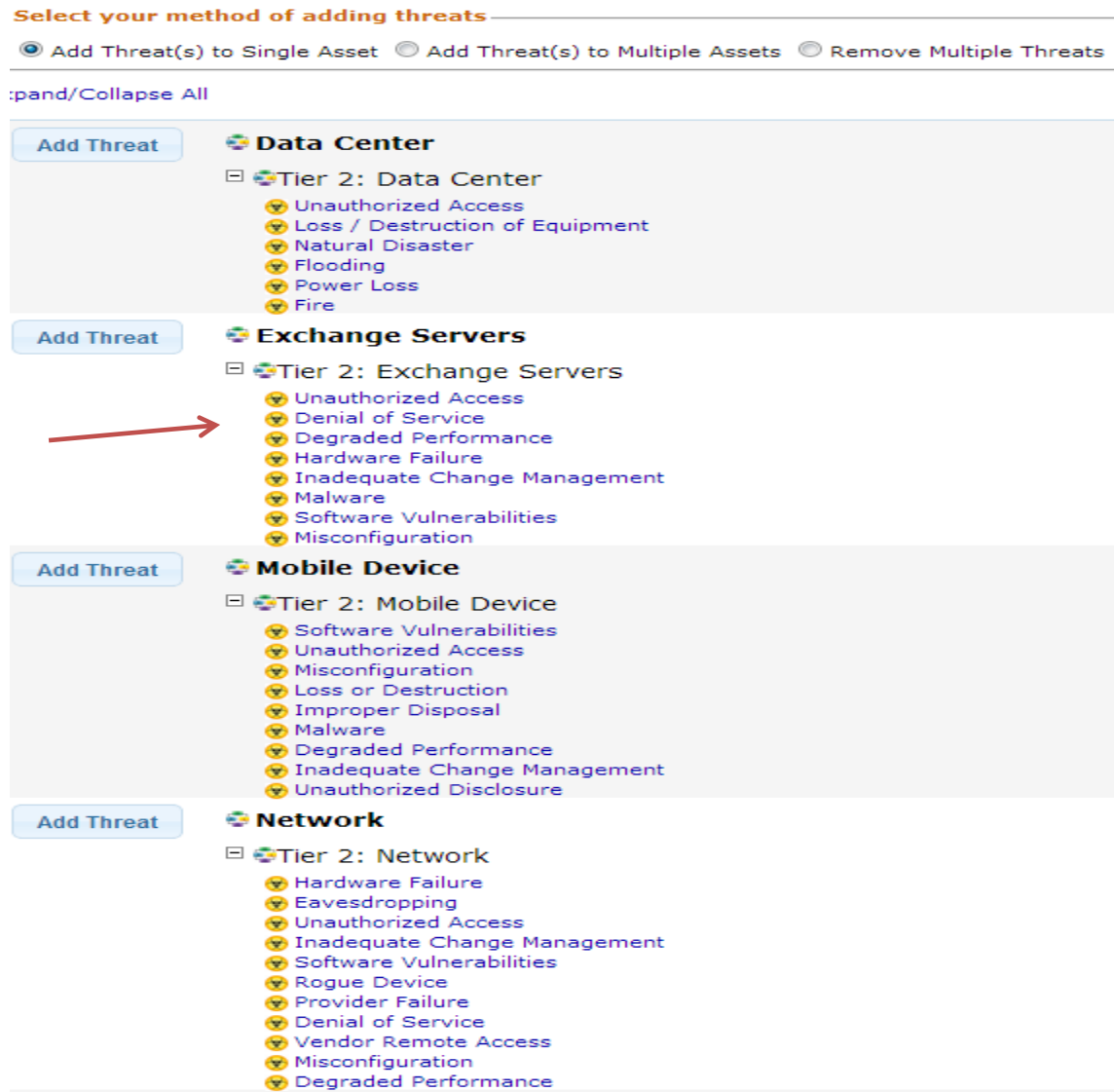
- [-] Tier 2: Exchange Servers
 - Unauthorized Access
 - Denial of Service
 - Degraded Performance
 - Hardware Failure
 - Inadequate Change Management
 - Malware
 - Software Vulnerabilities
 - Misconfiguration

Add Threat **Mobile Device**

- [-] Tier 2: Mobile Device
 - Software Vulnerabilities
 - Unauthorized Access
 - Misconfiguration
 - Loss or Destruction
 - Improper Disposal
 - Malware
 - Degraded Performance
 - Inadequate Change Management
 - Unauthorized Disclosure

Add Threat **Network**

- [-] Tier 2: Network
 - Hardware Failure
 - Eavesdropping
 - Unauthorized Access
 - Inadequate Change Management
 - Software Vulnerabilities
 - Rogue Device
 - Provider Failure
 - Denial of Service
 - Vendor Remote Access
 - Misconfiguration
 - Degraded Performance



Denial of Service Detail

Modify Threat - Denial of Service

Properties

* Name:

* Description:


Risk Properties

	Impact / Probability	Inherent Risk 	Acceptable Threshold
* Confidentiality:	<input type="text" value="Low"/>  	Low	<input type="text" value="Very Low"/> 
* Integrity:	<input type="text" value="Low"/>  	Low	<input type="text" value="Low"/> 
* Availability:	<input type="text" value="Very High"/>  	Medium	<input type="text" value="Very Low"/> 
* Probability:	<input type="text" value="Medium"/>  		
Active:	<input checked="" type="checkbox"/>		

Set thresholds to current calculated values

Step 4: Manage Controls

 **Data Center**

-  Tier 2: Data Center
 -  Fire
 -  Flooding
 -  Loss / Destruction of Equipment
 -  Natural Disaster
 -  Power Loss
 -  Unauthorized Access
 -  Develop a facility physical security plan and physical security procedures.
 -  Employ security guards to provide physical security as necessary.
 -  Establish access rights based on least privilege.
 -  Establish and maintain personnel status change and termination procedures.
 -  Maintain all physical security systems and security alarm systems.
 -  Verify mainframe rooms or data centers meet all physical security standards.



Manage Control Detail

Modify Control - Establish and maintain personnel status change and termination procedures.

Properties

Incidents

* Name: Establish and maintain personnel status change and termination procedures.

Description:

Type: Establish and maintain personnel status change and termination procedures.

* Confidentiality: Strong

* Integrity: Moderate

* Availability: Weak

* Probability: Moderate

Verification Procedure: Interview: Request a description of the organization's procedures for handling personnel status changes and

Control Question(s):

Examples:


Initial Cost: 0

















Yearly Cost: 0

Active:

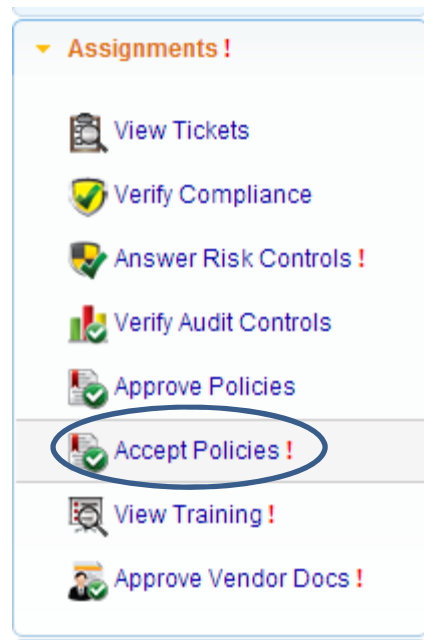
Key Control:

Step 5: Deploy Policies

 Distribute selected policies
Showing 1 to 4 of 4 entries Search:

	Policy Name ▲	Status ◆	Type ◆	Approved ◆	Assigned ◆	Creator ◆	Owner ◆	Delete ◆
<input type="checkbox"/>	Ready to distribute							
<input type="checkbox"/>	 Access controls and logging - Version 1 	Ready	Policy	04/22/2013 	04/24/2013	Kaliber	Kaliber	
<input type="checkbox"/>	 Personally Sensitive Data Definition - Version 1 	Ready	Policy	02/12/2013 		Kaliber	Kaliber	
<input type="checkbox"/>	 Record Handling Management - Version 1 	Ready	Policy	02/14/2013 		Kaliber	Kaliber	
<input type="checkbox"/>	 Personally Sensitive Data Definition Created 2013-04-22 12:48:42 	Ready	Policy	04/22/2013 		Kaliber	Kaliber	



What users see



Select a Policy to View

Showing 1 to 2 of 2 entries Search:

[CSV](#) [XLS](#) [XML](#)

Policy Name	Type	Last Viewed	Assigned	Acceptance Due By
 Network Access Points Configuration	Policy	04/22/2013	04/22/2013	
 Termination Policies and Procedures	Policy	08/19/2013	08/16/2013	

Show entries [First](#) [Previous](#) [1](#) [Next](#) [Last](#)

Select a Policy to View


Modify Accept Policy - Termination Policies and Procedures ✕

Click on each Policy Content title to view that piece of Policy.

By accepting this policy you acknowledge that you have read this entire policy.
By accepting this policy you acknowledge that you understand everything you have read in this policy.
By accepting this policy you accept everything that is written in this policy.

[CSV](#) [XLS](#) [XML](#)


Showing 1 to 1 of 1 entries Search:

View	File	Last Viewed
	Termination Procedures	08/19/2013

[Accept](#)



View Details

	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 3 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

Responsible Party	Required Actions
Information Systems	<ul style="list-style-type: none"> • Immediately upon notification of User termination disable User's access to ALL information assets including: • Email. • Network. • Locally and Perot administered information assets. • Review the terminated/transferred employee report provided by the Human Resources department to ensure that access for all terminated employees has disabled in the prior two week period.

Indicate Acceptance


Modify Accept Policy - Termination Policies and Procedures ✕

Click on each Policy Content title to view that piece of Policy.

By accepting this policy you acknowledge that you have read this entire policy.
By accepting this policy you acknowledge that you understand everything you have read in this policy.
By accepting this policy you accept everything that is written in this policy.

[CSV](#) [XLS](#) [XML](#)

Showing 1 to 1 of 1 entries Search:

View	File	Last Viewed
	Termination Procedures	08/19/2013

[Accept](#)

View/Manage Acceptance



Step 6: Answer Risk Controls

		CSV	XLS	XML			
Asset	Control	!	?	✓	✗	NA	↺
Data Center	Configure the alternate processing site to meet the least needed operational capabilities.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Develop a facility physical security plan and physical security procedures.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Employ security guards to provide physical security as necessary.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish access rights based on least privilege.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish and maintain a fire prevention and fire suppression standard.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish and maintain facility continuity plans.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish and maintain personnel status change and termination procedures.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish and maintain policies and procedures used to authorize removing IT assets from the facility.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish and maintain systems continuity plan strategies and Recovery Time Objectives for all relevant systems.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Establish and maintain systems continuity plans and procedures.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Install a generator sized to support the facility.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Center	Install an Uninterruptible Power Supply sized to support all key systems.		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Step 7: Audit/Verify



Audit Structure

View Assets ⓘ

(7 assets)

[View](#)

View Controls ⓘ

(166 controls)

[View](#)



Perform Audit

Assign responsibility for controls by associating users with standard roles ⓘ

(12 roles unassigned)

[Start](#)

View all controls and assign them to users

(166 unassigned controls)

[Revisit](#)

Configure Alerting, Integration, and Start Date ⓘ

(complete)

[Start](#)

Send notifications to all control auditors ⓘ

(not sent)

[Start](#)

Verify control answers ⓘ

(0% complete)

[Start](#)



Verify

Review the results of this audit ⓘ

[View](#)

Review this audit's Dashboard ⓘ

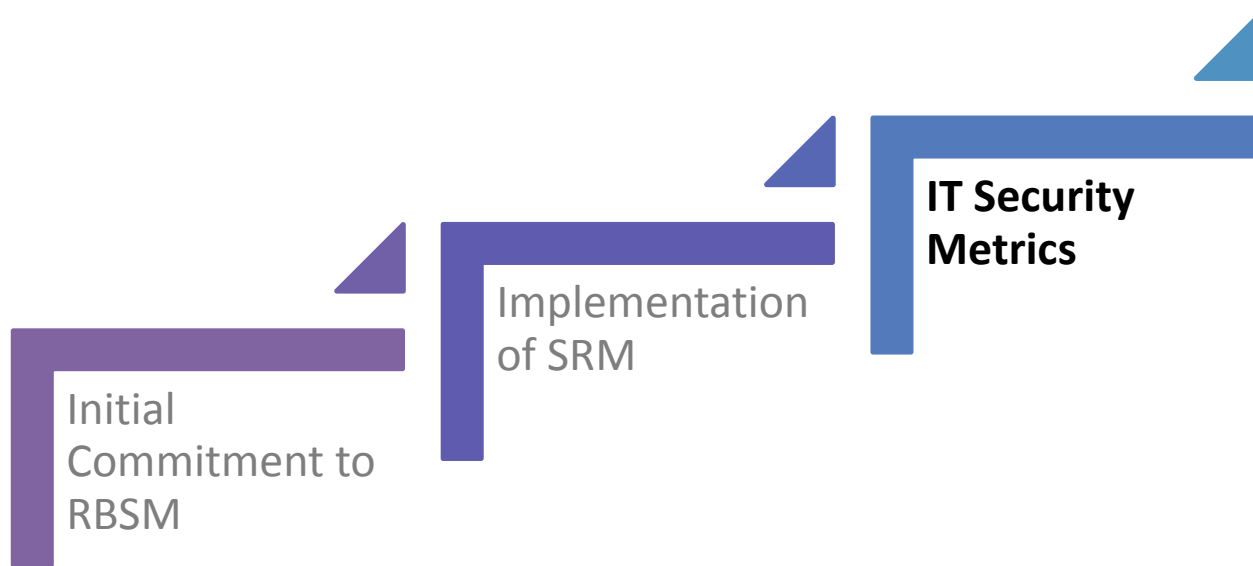
(0% implemented)

[View](#)

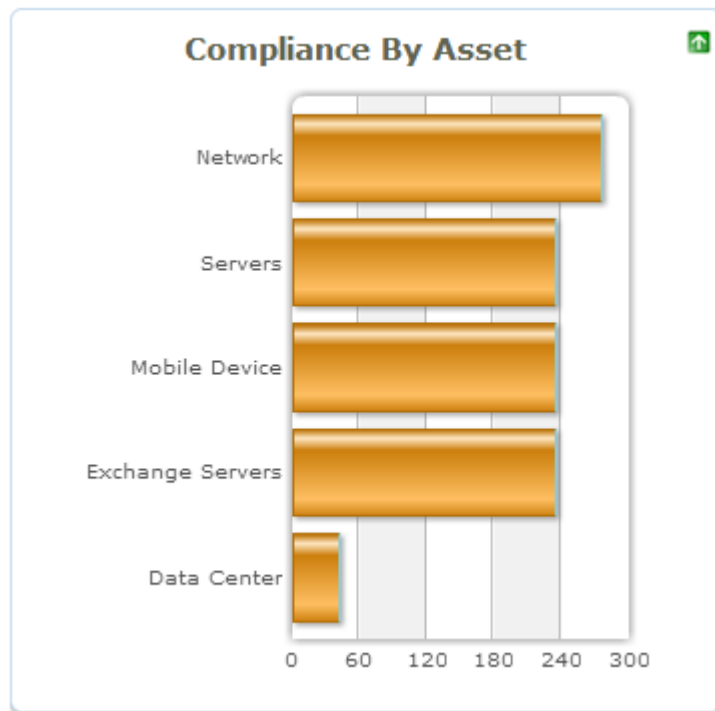
View and Archive Audit Report

[View](#)

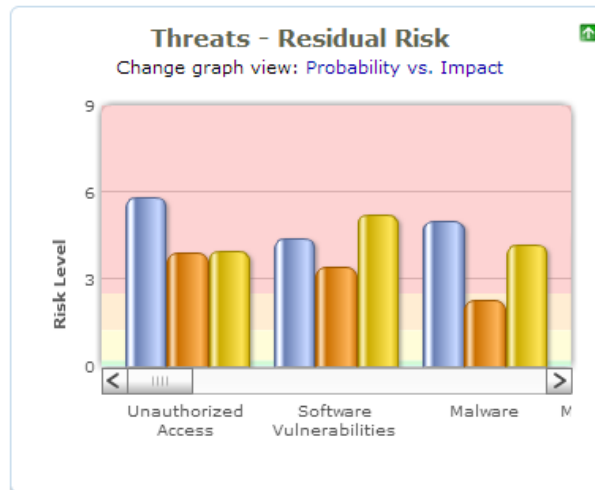
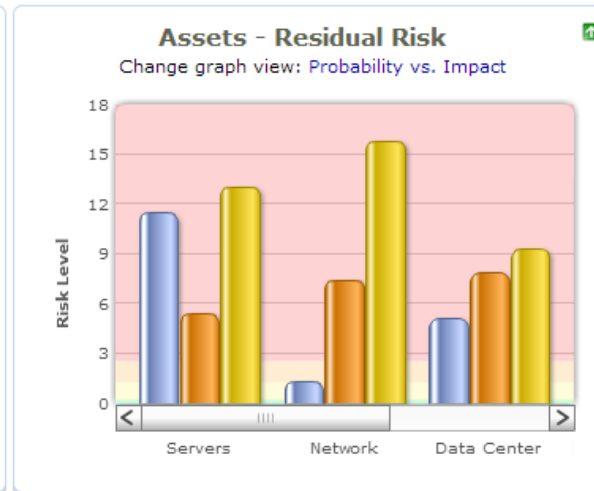
#3: Excellent Risk Metrics



Compliance Dashboards



Risk Dashboards



- CIA:
- Confidentiality
 - Integrity
 - Availability

Summary #1:

The Framework provided by an SRM system is necessary to support good Risk Based Security Management



“We need to take a risk-based approach to IT security”



“We need better communications between IT and Management (Administration)”

Top-Ten IT Issues in Higher Education

- 2007: #2 – “Security”
- 2008: #1 – “Security”
- 2009: #3 – “Security”
- 2010: #3 – “Security”
- 2011: #4 – “Security”

Top-Ten IT Issues in Higher Education

- 2012: SECURITY off the List

Replaced by: “Establishing and Implementing IT Governance throughout the Institution.”

“Establishing an IT governance process is possibly the single most-effective step toward effective IT leadership because it will provide a framework for defining decisions around IT priorities and resource allocation.”

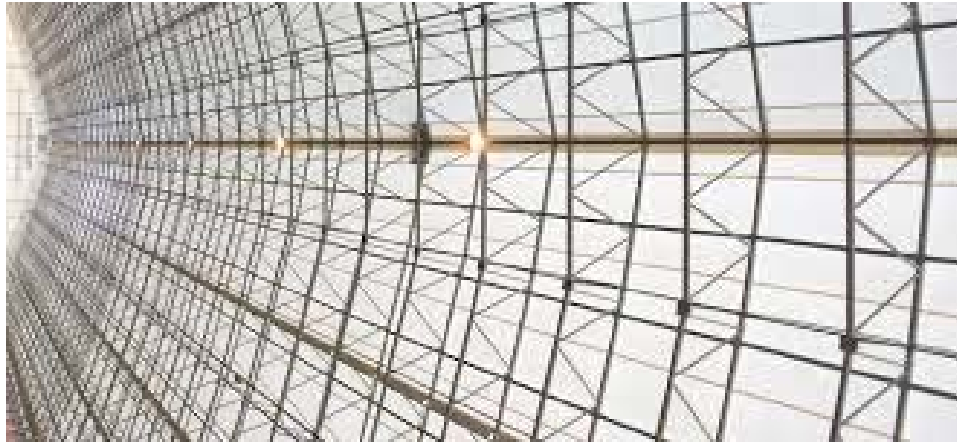
"Once a structure and process—a framework—is established, the institution can focus on the quality of decisions that flow from it. A good framework will result in decisions that are well understood and widely accepted."

—Joseph Vaughan, CIO and Vice President for Computing, Harvey Mudd College

HARVEY MUDD
COLLEGE



What do we need to support
the communications necessary
for good IT governance?



A Framework!

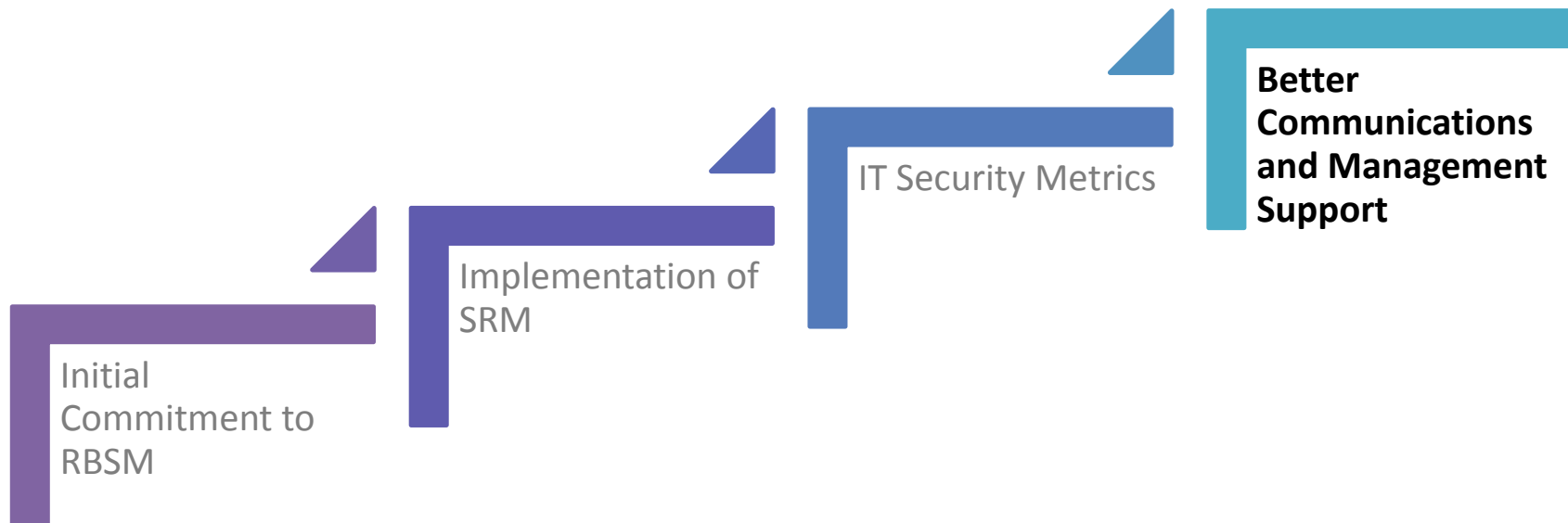
Where can we find such a
Framework?

SRM Systems

SRM Systems

63

Provide a Governance Framework
Facilitate Communications w/Administration



Summary Dashboards



Management Reports

Modify	Name	Report Type	Source	Owner Name	Created Date	Actions
Modify	Audit Report - Regulatory Audit	Executive Detailed	Audit	TraceCSO	08/02/2012	View Report
Modify	Audit Report - Risk-Based Audit	Executive Detailed	Audit	TraceCSO	08/02/2012	View Report
Modify	Compliance Management	Executive Detailed	Compliance	TraceCSO	07/16/2012	View Report
Modify	Incident Report	Executive Detailed	Incident Response Dash Reports	TraceCSO	12/14/2012	View Report
Modify	GCC Report	Detailed	Network Scanning	TraceCSO	08/28/2012	View Report
Modify	Vulnerability Report	Executive	Network Scanning	TraceCSO	07/24/2012	View Report
Modify	Policy Acceptance Report	Executive Detailed	Policies	TraceCSO	07/09/2012	View Report
Modify	Process Report	Executive Detailed	Processes	TraceCSO	07/03/2012	View Report
Modify	Business Continuity Management	Detailed	Risk	TraceCSO	01/11/2013	View Report
Modify	Risk Assessment Report	Executive Detailed	Risk	TraceCSO	07/26/2012	View Report
Modify	Risk Assessment Report-MassPCI	Executive Detailed	Risk	Kaliber	04/10/2013	View Report

Management Reports

Risk-Based Audit

Executive Summary & Details

08/20/2013



Kaliber Demo

Proprietary and Confidential
Copyright © 2013

Table of Contents

Table of Contents	2
Report Parameters	3
Executive Summary	4
Overall Summary	4
Control Status	5
Control Status by Asset	6
Control Status by Control Type	7
Control Status by Authority Document	8
Process & Scope	9
Details	10
Findings & Recommendations - Unverified Controls	10
Findings & Recommendations - Unimplemented Controls	11
Findings & Recommendations - Implemented Controls	12
Control Details	13
Supporting Documentation	70

Summary #2:

The Framework provided by an SRM system is necessary to support good Communications and IT Governance

Review

Let's work our way backwards



Review

- IT Security initiatives require the support and backing of the Administration
- Support and backing are gained through communications and agreed-to IT Governance standards
- IT Governance standards require a Framework
- The Framework collects data necessary to support the Governance Standards

Review

- Framework Data should include:
 - Risk Gaps
 - Compliance Gaps
 - Progress in closing Gaps
 - Identification of new threats and requirements on a regular basis

Review

- Framework Data should be gathered by:
 - Identifying Authority Documents
 - Compliance requirements like FERPA, HIPAA, Mass Data Privacy
 - Best Practices like ISO 27001
 - Identifying Assets Containing Protected Information
 - Evaluating Threats to that Data
 - Identifying Appropriate Controls
 - Assuring that those Controls are implemented

Review

- SRM Systems Provide the Framework
 - Help collect and organize Data
 - Provide pre-mapped conditions for Threat -> Controls -> Compliance Requirements

Conclusion

A Risk-based approach to IT Security management
and
Establishing better communications between IT and the
Administration
ARE Related

THEY REQUIRE A COMMON FRAMEWORK TO EVALUATE RISK
AND COMMUNICATE THAT RISK



2 Final Thoughts



Get started today on truly implementing a Risk-based framework for better IT Governance and better communications



Thank you for your time and attention.



CONTACT INFO

ken.leeser@kaliberdatasecurity.com

617-597-1719 x207

@KALDataSecurity

