

IT Risk

Week 11

ISACA's Risk IT Framework



ISACA's Risk IT Framework

1. What is IT Risk?
2. What are the three types of IT Risk?
3. What are the three risk processes that an enterprise ought to have?
4. What is risk appetite?
5. What is risk tolerance?
6. What are the three parts of a risk culture?

Risk Evaluation

- What are some ways you might express IT risk in business terms?
 - COBIT
 - COSO ERM
- What is a risk scenario?
- What is a risk factor?
- What are the four types of risk response and when would you use them?

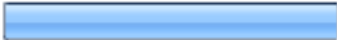
ISACA's Risk IT Framework

- Part of Enterprise Risk Management
 - Look at the breadth of IT risk, not just cyber-security
 - Should align to business strategy
-
- Risk IT Framework
 - Risk Governance
 - How much risk can you stand?
 - Risk Evaluation
 - What risks do you actually face?
 - Risk Response
 - How can you make these risks acceptable?



How much risk can you stand?

12. Has your board of directors considered IT risks?

		Response Percent	Response Count
Yes		39.3%	11
No		60.7%	17

RISK II A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk.



What risks do you actually face?

9. Have you had a cyber-security risk assessment performed?

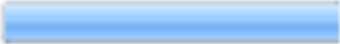
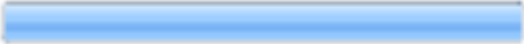
		Response Percent	Response Count
Yes		28.6%	8
No		71.4%	20
		answered question	28
		skipped question	0

—
Risk



How can you make these risks acceptable?

5. Is cyber security the responsibility of a single designated person?

		Response Percent	Response Count
Yes		39.3%	11
No		60.7%	17
		answered question	28
		skipped question	0

— make it less impactful



Two views of cyber-security controls

ISACA	SANS
Preventive	Getting In
Detective	Staying In
Corrective	Acting



Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG) Version 3.1 October 3, 2011

Table of Contents

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)..... 1

Version 3.1 October 3, 2011 1

Introduction..... 3

Forging Consensus among Chief Information Security Officers, Chief Information Officers, and Inspectors General on Technical Requirements for System Administrators and Security Personnel 5

Relationship of the 20 Critical Controls to National Institute of Standards and Technology Guidelines 6

Relationship of the 20 Critical Controls to the Australian Government's Defence Signals Directorate IS Strategy to Mitigate Targeted Cyber Intrusions 7

Relationship of the 20 Critical Controls to the National Security Agency's Associated Manageable Network Plan Revision 2.1 Milestones and Network Security Tasks 8

Document Contributors 8

The 20 Critical Controls..... 9

Insider versus Outsider Threats 10

Relationship to Other US Federal Guidelines, Recommendations, and Requirements 12

Periodic and Continual Testing of Controls 12

Future Evolution of the 20 Critical Controls 12

Description of Controls..... 13

Critical Control 1: Inventory of Authorized and Unauthorized Devices 13

Critical Control 2: Inventory of Authorized and Unauthorized Software 16

Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers 19

Critical Control 4: Continuous Vulnerability Assessment and Remediation 23

Critical Control 5: Malware Defenses 26

Critical Control 6: Application Software Security 29

Critical Control 7: Wireless Device Control 33

Critical Control 8: Data Recovery Capability 36

Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps 37

Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches 39

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services 42

Critical Control 12: Controlled Use of Administrative Privileges 44

SANS Control # 3: Secure Configurations of HW & SW

- Utah Department of Health – 701,000 records
 - Policy to delete information not followed
 - Old configuration gave hacker access

- St. Joseph’s Health System - 32,000 records
 - “...security settings incorrect.”

- SANs quick wins: Standard, hardened builds, preferably put on by vendors, no variations unless specifically approved

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)
Version 3.1 October 5, 2011

Table of Contents	
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG).....	1
Version 3.1 October 5, 2011	1
Introduction	3
Fading Consensus among Chief Information Security Officers, Chief Information Officers, and Inspectors General on Technical Requirements for System Administrators and Security Personnel	5
Relationship of the 20 Critical Controls to National Institute of Standards and Technology Guidelines	6
Relationship of the 20 Critical Controls to the Australian Government's Defense Signals Directorate IS Strategy to Mitigate Targeted Cyber Intrusions	7
Relationship of the 20 Critical Controls to the National Security Agency's Associated Manageable Network File Revision 2.1: Mitigation and Network Security Tool.....	8
Document Contributions.....	8
The 20 Critical Controls	9
Inside versus Outside Threat.....	10
Relationship to Other US Federal Guidelines, Recommendations, and Requirements	12
Periodic and Continuous Testing of Controls.....	12
Future Evolution of the 20 Critical Controls	12
Description of Controls	13
Critical Control 1: Inventory of Authorized and Unauthorized Devices.....	13
Critical Control 2: Inventory of Authorized and Unauthorized Software.....	16
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.....	19
Critical Control 4: Continuous Vulnerability Assessment and Remediation.....	23
Critical Control 5: Malware Defenses.....	26
Critical Control 6: Application Software Security.....	29
Critical Control 7: Wireless Device Control.....	33
Critical Control 8: Data Recovery Capability.....	36
Critical Control 9: Security Risk Assessment and Appropriate Training to FBI Employees.....	37
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.....	39
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services.....	42
Critical Control 12: Controlled Use of Administrative Privileges.....	44

SANS Control # 3: Controlled Access Based on Need to Know

- Memorial Healthcare System – 10,000 records
 - Two employees “...improper access”
 - Intended to file fraudulent tax returns
- South Carolina Department of Health – 228,000 records
 - Employee moved 17 spreadsheets by email
- SANS quick wins: multi-level data classification with access allowed to minimally acceptable authorized users

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)

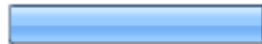
Version 3.1 October 3, 2011

Table of Contents	
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG).....	1
Version 3.1 October 3, 2011	1
Introduction	3
Forging Consensus among Chief Information Security Officers, Chief Information Officers, and Inspectors General on Technical Requirements for System Administrators and Security Personnel	3
Relationship of the 20 Critical Controls to National Institute of Standards and Technology Guidelines	6
Relationship of the 20 Critical Controls to the Australian Government's Defence Signals Directorate 35 Strategies to Mitigate Targeted Cyber Intrusions	7
Relationship of the 20 Critical Controls to the National Security Agency's Associated Manageable Network Plan Revision 2.1 Milestones and Network Security Tasks	8
Document Contributors.....	8
The 20 Critical Controls.....	9
Insider versus Outsider Threats	10
Relationship to Other US Federal Guidelines, Recommendations, and Requirements	12
Periodic and Continual Testing of Controls	12
Future Evolution of the 20 Critical Controls	12
Description of Controls.....	13
Critical Control 1: Inventory of Authorized and Unauthorized Devices	13
Critical Control 2: Inventory of Authorized and Unauthorized Software	16
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	19
Critical Control 4: Continuous Vulnerability Assessment and Remediation	23
Critical Control 5: Malware Defenses	26
Critical Control 6: Application Software Security	29
Critical Control 7: Wireless Device Control	33
Critical Control 8: Data Recovery Capability	36
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	37
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.....	39
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services.....	42
Critical Control 12: Controlled Use of Administrative Privileges	44

SANS Control # 17: Data Loss Prevention Data-at-rest

11. Do all desktops and laptops use data encryption by default?

Yes



28.6%

8

No



71.4%

20

answered question

28

skipped question

0

– SANS quick win: deploy hard drive encryption

Introduction 3
 Fading Concerns among Chief Information Security Officers, Chief Information Officers, and
 Inspectors General on Technical Requirements for System Administrators and Security Personnel... 5
 Relationship of the 20 Critical Controls to National Institute of Standards and Technology Guidelines 6
 Relationship of the 20 Critical Controls to the Australian Government's Defense Signals Directorate
 IS Strategy to Mitigate Targeted Cyber Intrusions 7
 Relationship of the 20 Critical Controls to the National Security Agency's Associated Manageable
 Network File Section 3.1: Message and Network Security Tool 8
 Document Contributions 8
 The 20 Critical Controls 9
 Insider versus Outsider Threats 10
 Relationship to Other US Federal Guidelines, Recommendations, and Requirements 12
 Periodic and Continual Testing of Controls 12
 Future Evolution of the 20 Critical Controls 12
 Description of Controls 13
 Critical Control 1: Inventory of Authorized and Unauthorized Devices 13
 Critical Control 2: Inventory of Authorized and Unauthorized Software 16
 Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and
 Servers 19
 Critical Control 4: Continuous Vulnerability Assessment and Remediation 23
 Critical Control 5: Malware Defense 26
 Critical Control 6: Application Software Security 29
 Critical Control 7: Wireless Device Control 33
 Critical Control 8: Data Recovery Capability 36
 Critical Control 9: Security Risk Assessment and Appropriate Training to FBI Employees 37
 Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and
 Switches 39
 Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services 42
 Critical Control 12: Controlled Use of Administrative Privileges 44

SANS Control # 17: Data Loss Prevention Data-in-motion

- South Carolina Department of Health – 228,000 records
 - Employee moved 17 spreadsheets by email
- CA In-home support Services – 701,000 records
 - Unencrypted microfiche lost on way to insurance company
- SANS: Monitor outbound transactions for anomalies, move data using secure, authenticated, encrypted mechanisms

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)
Version 3.1 October 3, 2011

Table of Contents	
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG).....	1
Version 3.1 October 3, 2011	1
Introduction..... 3	
Forging Consensus among Chief Information Security Officers, Chief Information Officers, and Inspectors General on Technical Requirements for System Administration and Security Personnel.....	5
Relationship of the 20 Critical Controls to National Institute of Standards and Technology Guidelines.....	6
Relationship of the 20 Critical Controls to the Australian Government's Defense Signals Directorate IS Strategies to Mitigate Targeted Cyber Intrusions.....	7
Relationship of the 20 Critical Controls to the National Security Agency's Associated Manageable Network File Resilience 2.1: Mitigation and Network Security Tools.....	8
Document Contributions.....	8
The 20 Critical Controls..... 9	
Insider versus Outsider Threats.....	10
Relationship to Other US Federal Guidelines, Recommendations, and Requirements.....	12
Periodic and Continual Testing of Controls.....	12
Future Evolution of the 20 Critical Controls.....	12
Description of Controls..... 13	
Critical Control 1: Inventory of Authorized and Unauthorized Devices.....	13
Critical Control 2: Inventory of Authorized and Unauthorized Software.....	16
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.....	19
Critical Control 4: Continuous Vulnerability Assessment and Remediation.....	23
Critical Control 5: Malware Defenses.....	26
Critical Control 6: Application Software Security.....	29
Critical Control 7: Wireless Device Control.....	33
Critical Control 8: Data Recovery Capability.....	36
Critical Control 9: Security Risk Assessment and Appropriate Training to FBI Employees.....	37
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.....	39
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services.....	42
Critical Control 12: Controlled Use of Administrative Privileges.....	44

The All World Airlines Case

- Take 45 minutes
- Your team has been requested to compile a list of risks for each of five areas identified by the CFO for the risk assessment.
 - Group your thoughts by section, using the details that Don has provided, your understanding of the COBIT risk management issues and your understanding of IT issues.
 - How would you perform a risk assessment of the risks identified in question 1 to provide an objective and subjective assessment for management's consideration?
 - Identify what role the retained organization should have in its interactions with the vendor for the outsourced IT function.