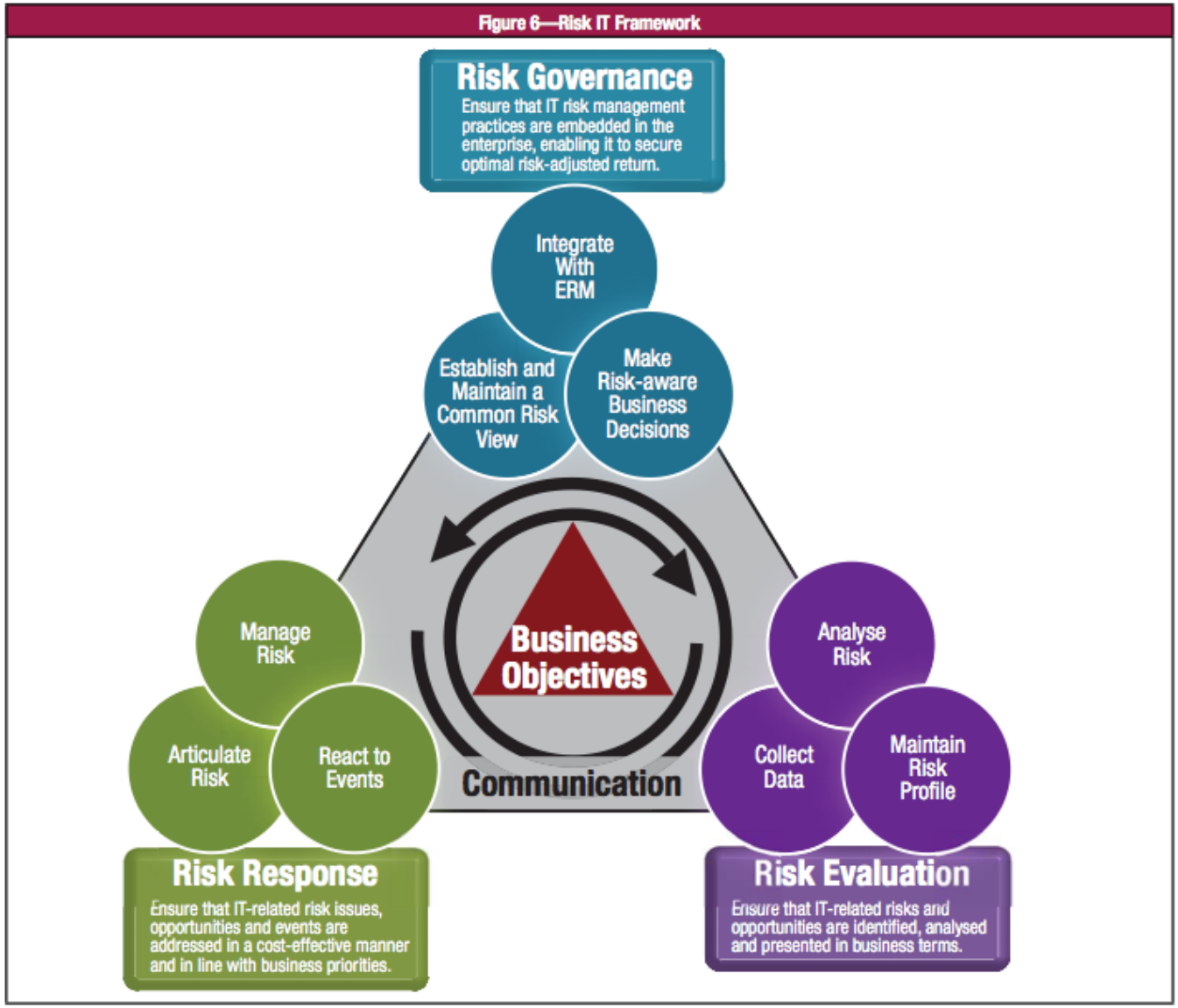
IT Risk
Week 11

ISACA's Risk IT Framework



ISACA's Risk IT Framework

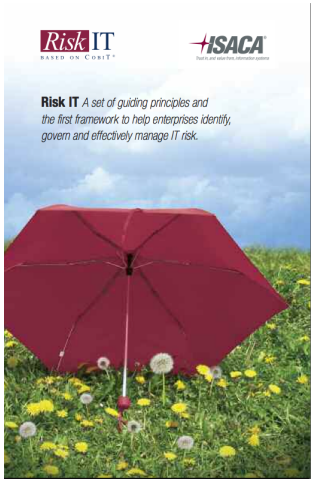
1. What is IT Risk?
2. What are the three types of IT Risk?
3. What are the three risk processes that an enterprise ought to have?
4. What is risk appetite?
5. What is risk tolerance?
6. What are the three parts of a risk culture?

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

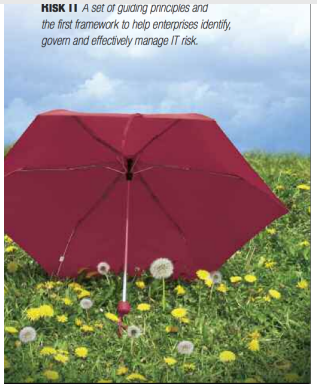
    What risks do you actually face?
  - Risk Response

    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



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?

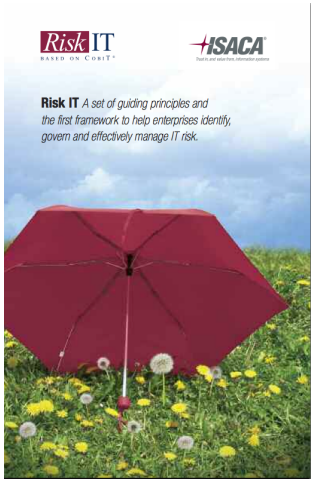
5. Is cyber security the responsibility of a single designated person?

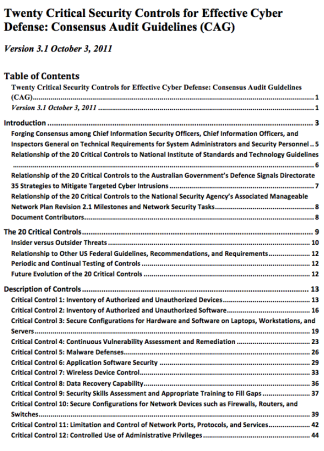
		Response Percent	Response Count
Yes		39.3%	11
No		60.7%	17
	answered question		28
	skipped question		0

- Make it less impactful

Two views of cyber-security controls

ISACA	SANS
Preventive	Getting In
Detective	Staying In
Corrective	Acting





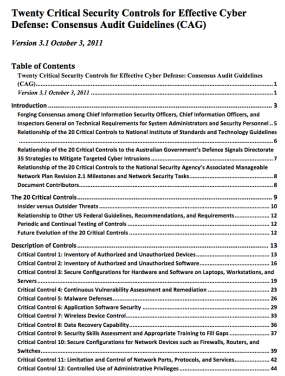
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)

Version 3.1 October 3, 2011

Table of Contents

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 3, 2011

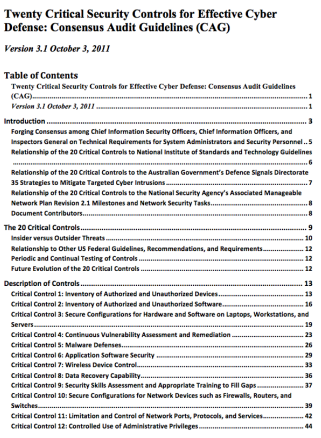
Table of Contents

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

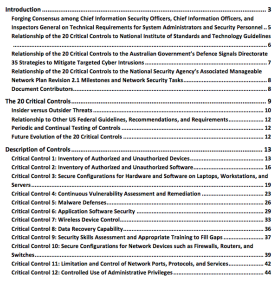
Table of Contents

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

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

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

– SANS quick win: deploy hard drive encryption

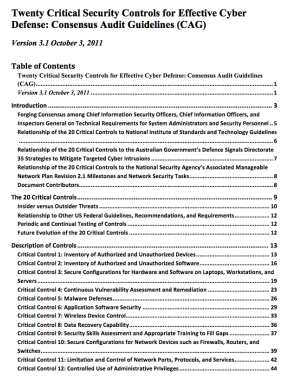


SANS Control # 17:
Data Loss Prevention Data-in-motion

- 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

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.