



**O-ISC '07**  
Ohio Information Security Conference

# IT Risk Assessment Considerations

**Jerry Echternacht**  
**NCR**



Transforming Transactions into Relationships

# Speaker Biography



## ■ Jerry L. Echternacht, *CISSP, CISA, CPA*

is a manager of Global Information Security at NCR Corporation. Jerry has been employed at NCR for over 13 years, where he is currently involved with Sarbanes-Oxley testing, risk assessment and analysis, awareness programs, and information security policies and standards. Before this, he provided information technology consulting to a wide variety of companies and industries.

[Jerry.Echternacht@ncr.com](mailto:Jerry.Echternacht@ncr.com)



- Purpose of IT Risk Assessment
- Approaches to IT Risk Assessment
- IT Risk Criteria & Impact of Threats and Vulnerabilities
- Results of IT Risk Assessment

# Purpose of IT Risk Assessment

## ■ What is risk?

Risk = potential damage to value

## ■ Purpose of IT Risk Assessment

- Information is susceptible to an ever-widening spectrum of threats
  - Information Owners need to know their “information resources” are in good order
- Business success is increasingly dependent on IT
  - More and more systems and data are online and networked
  - Electronic commerce is raising dependence to a new level

## ■ Purpose of IT Risk Assessment

- Governance requirement
  - Top Management needs to know “information risk” is under control
- Regulatory compliance
- Business continuity and disaster recovery
- Operational impact
- Internal auditor understanding and scoping
- External auditor understanding and scoping

# Approaches to IT Risk Assessment

- Approaches to IT Risk Assessment
  - Quantitative
  - Qualitative

## ■ Quantitative Approaches

$$(AV \times EF = SLE) \times ARO = ALE$$

- AV = Asset Value
- EF = Exposure Factor = impact or loss of asset value when threat occurs, 0% - 100%
- SLE = Single Loss Exposure = when threat occurs, loss in monetary terms
- ARO = Annualized Rate of Occurrence = how often a threat is expected to happen in a year
- ALE = Annualized Loss Exposure = loss expectancy for a given threat

## ■ Quantitative Approaches

$$(AV \times EF = SLE) \times ARO = ALE$$

- The risk is a fire
  - Asset Value = \$2 million
  - Exposure Factor = 50%
  - Single Loss Exposure = \$2M x 50% = \$1M
  - Annualized Rate of Occurrence – 1/10, or once in 10 years
  - Annualized Loss Exposure = \$1M x 1/10 = \$100k
- The organization would be justified in spending up to \$100k per year to prevent the occurrence or reduce the impact of a fire

## ■ Quantitative Approaches

### ● Pros

- Assessments based on independent objective metrics
- Cost/Benefit analysis assists in budget decision making
- Results expressed in quantitative business language (monetary value, percentages, probabilities)

### ● Cons

- Huge amount of work to gather quantitative information, data, expected probabilities, etc. (or expensive to purchase automated tool or methodology)
- Many items are hard to quantify, especially in information security area
- People forced to express their qualitative, anecdotal info in quantitative terms

## ■ Qualitative Approaches

- Uses softer criteria to evaluate IT risk
- Uses relative classifications of risk and impacts (high, medium, low)
- Relies on judgment
- Considers threats and vulnerabilities in context of current organizational environment

## ■ Qualitative Approaches

### ● Pros

- Usually quicker completion
- Not necessary to quantify values, probabilities, threat frequencies
- Easier to involve multiple organizations (business units, management, IT)

### ● Cons

- Perception of value and loss of value may not reflect the actual value at risk
- Less basis for cost/benefit analysis – harder to determine what to spend to mitigate risk
- Difficult to track risk management performance objectively when all measures are subjective

- Qualitative approaches are the predominant method used
  - Some form of quantitative data may be incorporated to provide additional rationale
  - Even this data may be classified in relative terms



# IT Risk Criteria

# IT Risk Assessment Considerations



Aspect of Information Security (C / I / A)	Information Resource	Threat (What are you afraid of? What are you trying to avoid?)	Probability of experiencing loss	Impact	Mitigations/ Controls	Do we implement this Mitigation/ Control?

## ■ Aspect of Information Security

- Confidentiality
- Integrity
- Availability

## ■ Information Resource

- Define types
  - Information (database)
  - Application (system)
  - Computer installation (data center / server)
  - Network
  - Development activity (project)
- Determine scope of assessment

## ■ Threats and Vulnerabilities

- Ultimately, loss of confidentiality, integrity, and/or availability
- Brainstorm possible ways that information resources can be compromised or exploited
- Various criteria to consider:
  - Malfunction of software
  - Malfunction of hardware
  - Loss of service
  - Human error
  - Unforeseen effects of change
  - Virus or Malware
  - Internal actions
  - External actions

## ■ Probability

- Probability of threat occurring – may be impacted by:
  - Other controls in place
  - Considerations within your own organization
- Use relative measures – high, medium, low

- Impact – that incidents would have on organization in terms of:
  - Financial loss (loss of sales, assets)
  - Cost increases (to fix incident, insurance rates)
  - Degraded performance (service level, productivity, disruption to operations)
  - Loss of management control (compliance and governance)
  - Damaged reputation (negative publicity, regulatory issues)
  - Impaired growth (delayed new business lines or ventures)
    - Many of these could lead to customer loss and/or impact viability of organization

## ■ Impact - compliance and governance

- Lapse in organizational compliance to governing body laws, statutes, regulations, and requirements?
- Lapse in compliance to corporate policies?
- Lapse in issue resolution process?
  - Impact timely response to issues
  - Impact timely and proper escalation to corporate office
  - Impact timely disciplinary actions and corrective actions
- Increase exposure to upcoming legislation, issues, or pressures?
- Consider exposure geography, line of business, etc.

## ■ Impact – items to really consider

- What % of sales, transactions, customer calls, etc., does this information resource handle? What is the materiality to the organization?
- What if information is corrupted?
- What if information is disclosed or made available to the wrong people?
- What if the information resource is rendered unavailable for:
  - 1 hour?
  - Half day?
  - 1 day?
  - 1 week?
  - 1 month?
- Is this information resource customer facing?

## ■ Mitigation/Control Environment

- Both current status and future actions should be considered
- Areas include:
  - Policies and standards
  - Organizational ownership
  - Risk identification
  - Risk awareness
  - Service agreements
  - User capabilities
  - IT capabilities
  - Communication and Awareness
  - System configurations
  - Backup arrangements
  - Contingency arrangements
  - Physical security
  - Access to information
  - Change management
  - Problem incident management
  - Audits and reviews



# Case Study



# Results of IT Risk Assessment

## ■ Results of IT risk assessment

### ● Categorize sites by tiers

- When looking at networks, determine which sites / locations are more important, i.e., from a materiality standpoint, or from a business processing standpoint
- Assign the information resources to categories - Tier 1, Tier 2, and Tier 3.
- Those in more critical tiers are networked with higher bandwidth and more redundancy features than those in lower tiers.

## ■ Results of IT risk assessment

### ● Service Level Agreements

- Highest criticality is assigned to anything directly used by customers or used to directly support customer interfacing activities
- Determine if support should be available or provided 24\*7, 24\*5, during work hours only, or some other variation
- Some service levels may have to be “best effort” – meaning they will be supported when time and resources allow
- Determine notification process

## ■ Results of IT Risk Assessment

- Vary levels of response for information resource
  - Vary service levels during the month or quarter
    - For instance, financial systems may be covered by your most responsive service level agreement during month end close, but then drop to a lower service level during the rest of the month
  - Vary response times for initial contact compared to problem resolution
  - Vary response times for fixing problems vs. recovering from a disaster
    - Decide criteria to declare a disaster – then use it – don't second guess in the heat of the crisis

## ■ Results of IT risk assessment

### ● Network segregation

- Use of DMZ, firewalls, etc.
- In order to meet regulatory requirements, use dedicated, segregated networks to isolate specific regulated activity



**O-ISC '07**  
Ohio Information Security Conference

---

# Questions & Answers



Renewing Business Intelligence