

Performing, Using, and Auditing IT Risk Assessments

ISACA – Utah Chapter

The
Cadence
Group





How do organization use IT risk assessments?

Organizations generally perform IT risk assessments for one of more of the following reasons:

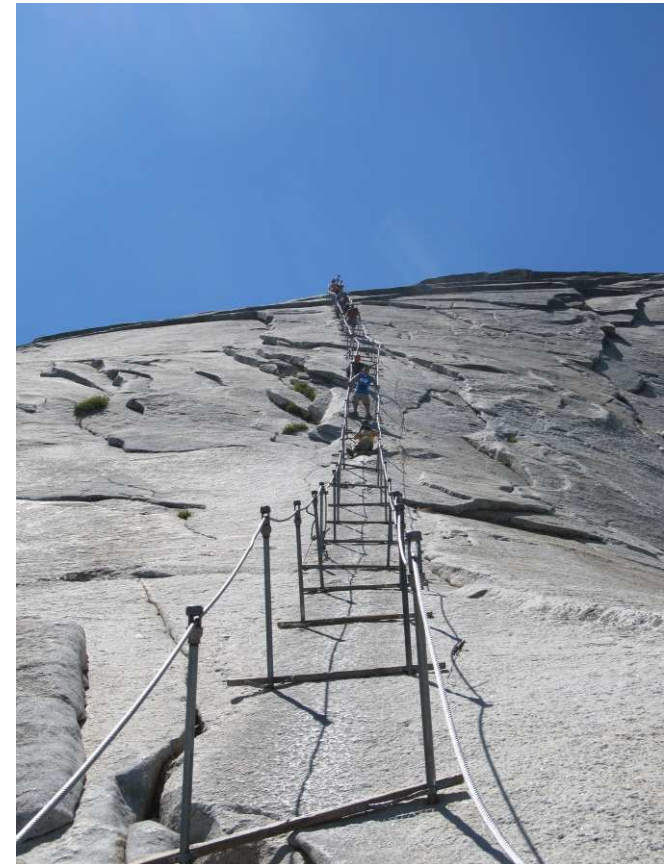
1. Improve the integrity, availability and confidentiality of information systems
2. Assist with strategic and financial risk management decisions
3. Increase effectiveness of policy statements
4. Compliance



How do you perform an IT risk assessment?

NIST SP 800-30 is the predominant standard for IT risk assessments. This standard outlines the following steps:

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation





1. System Characterization

Obtain the following information through automated scans, dataflow diagrams, and inquiry of the business and system owners:

Purpose / Functionality

Version Number

Business Owner

System Owner

Sensitive Data

Confidential Data

Hosted or In-house?

Hosting Environment

In-house Environment:

System Feeds and Interfaces

Database Name(s)

Database Platform

Application Server Name(s)

Application Server Platform

Database Server Name(s)

Database Server Platform



1. System Characterization

In addition, the following questions should be answered and scored to determine the inherent risk of a system environment:

- What type of information is stored in the application?
- What type of transactions does this application support?
- What is the asset or (annual) revenue value this application tracks?
- How many users are impacted by this application?
- What type of system environment is used for this application?
- Who uses this application?



2. Threat Identification



Practical Guidance: Considering skipping this step if time is an issue. While the creation of a threat list will help ensure coverage in step #3, the formal documentation of a threat statement may not provide value.



3. Vulnerability Identification

Practical Guidance: Categorize vulnerabilities into general and system-specific process areas that address identified threats (instead of highlighting specific vulnerabilities). Use past history as a reference.

Refer to the sample areas below:

General Areas:

- IT Policies and Procedures
- IT Strategic Planning / IT Governance
- IT Project Management / System Development
- Security Management and Network Security Architecture
- Physical and Environmental Security
- Third Party Management

System-Specific Areas:

- Change Control / Release Management
- Problem Management / Error Resolution
- Data Management
- Security Configurations, Authentication and Logging
- Access Control
- Backup and Disaster Recovery

Threats identified in step#2 should be mapped to these areas to ensure processes provide a full coverage of the identified threats.



4. Control Analysis

Determine what controls are in place for the general and system-specific processes identified in step #3. Standard control types should be considered. For example:

Change Control / Release Management

- Documented change management procedures
- Scope definition and prioritization
- Version control or code locking mechanisms
- Testing (unit, integration and regression)
- Business approval on the go live
- Segregation of duties (development, testing, migration)
- Post implementation review

Practical Guidance: Understand, but don't 'audit' the controls.



5. Likelihood Determination

Calculate the likelihood of the vulnerability being exploited. This measurement is often subjective, but the more scientific the rating, the more precise the assessment. Regardless of the calculation, it should be based on the following:

- Threats (Step 2)
- Vulnerabilities (Step 3)
- Current Controls (Step 4)

Industry Guidance: Organizations are moving to frequency of occurrence in lieu of likelihood. Instead of guessing on the probability a risk may occur, they are working with historical data. This solution, however, requires strong incident reporting capabilities.



6. Impact Analysis



Impact should include both a quantitative (typically \$) and qualitative analysis (reputational) and should consider integrity, availability and confidentiality.



7. Risk Determination

High	<u>Medium Risk</u>	<u>High Risk</u>
	Share	Avoid
Low	<u>Low Risk</u>	<u>Medium Risk</u>
	Accept	Mitigate
	LIKELIHOOD / FREQUENCY	
	Low	High

Industry Guidance: Some organizations are adding a third dimension to assess the velocity of risks (high: breach/ low: change prioritization).



8. Control Recommendations

Provide control recommendation to improve processes and control. These recommendations should focus on areas with high residual risk.

Practical Guidance: Recommendations should not be a surprise to the business (process) and system owners. In an effort to reduce surprises, recommendations should be:

- Discussed during interviews
- Validated in a closing meeting
- Confirmed in a draft report



9. Results Documentation

Prepare a summary of findings with the following sections:

- Introduction (provides objective)
- Approach (describes the methodology)
- System Characterization (outlines the scope)
- Risk Assessment Results
 - Summary of inherent / residual risk ratings
 - Reference to appendices for detailed assessment
- Control Recommendations (provides high-risk mitigation areas)
- Summary
- Appendices



Auditing IT Risk Assessments

Three basic ways to audit an IT risk assessment

1. Audit the completeness and accuracy of the risk assessment

AND

2. Audit the high-risk systems

- Focus on processes with high residual risk to help improve risk mitigation efforts.
- Focus on systems with high inherent risk to help ensure mitigation techniques are designed and operating effectively.

3. Audit the high-risk processes

OR

- Focus on systems with high residual risk to improve the process in an effort to mitigate risk
- Focus on systems with high inherent risk to help ensure mitigation techniques are designed and operating effectively.



Recap: How do organization use IT risk assessments?

Organizations generally perform IT risk assessments for one of more of the following reasons:

1. Improve the integrity, availability and confidentiality of information systems
2. Assist with strategic and financial risk management decisions
3. Increase effectiveness of policy statements
4. Compliance



Contact Information

Gordy Jacobsen

Office: 801 337 3917

Cell: 801 554 9881

Email: gordy@thecadencegroup.com

Web: www.thecadencegroup.com

QUESTIONS?

The
Cadence
Group



Phone 801 337 3917 ~ Fax 866 326 6612

www.thecadencegroup.com