Enterprise Security and Risk Management Office
Risk Management Services

Risk Management Guide

March 22, 2011
Revision 1.9

Enterprise Security and Risk Management Office

Risk Management Services

Risk Management Guide

Initial Release Date:	March 31, 2004	Version:	1.0
Date of Last Review:	March 22, 2011	Version:	1.9
Date Retired:			
Architecture Interdependencies:			
Reviewer Notes: October 27, 2005 – Updated website links and confirmed reference links. March 09, 2007 – Updated website links and Office information. December 11, 2009 – Scheduled review, minor update. March 22, 2011 – Scheduled review, minor updates.			

Office of the State Chief Information Officer
Information Technology Services
PO Box 17209
Raleigh, North Carolina 27619-7209
Telephone (919) 754-6231

Enterprise Security and Risk Management Office

Risk Management Services

Risk Management Guide

Risk Management Guide

Risk Management Guide

Introduction

The purpose of this Risk Management Guide is to present an approach to help state agencies in assessing risk that could impair their ability to deliver critical services to the citizens of North Carolina. There are many types of risk inherent in the state's business activities. Agency management needs to understand adverse events that impede agency operations are likely to happen.   They need to take reasonable and prudent steps to avoid and/or minimize business disruptions.

In general, "**risk**" is the potential exposure of an activity to damage. Some types of risk are:

- Business Risk – The cost and/or lost revenue associated with an interruption to normal business operations.
- Organizational Risk – The direct or indirect loss resulting from one or more of the following:
  - Inadequate or failed internal processes
  - People
  - Systems
  - External events
- Information Technology Risk- The loss of an automated system, network or other critical information technology resource that would adversely affect business processes.

Due to the increasing organizational dependence on data and information technology (IT) infrastructure, most organizations need an approach for incorporating IT risk into their business risk management strategy. IT risk continually changes with the usage of new and evolving technologies to support business services.

Scope

State law *G.S. § 147-33.89 Business Continuity Planning* and the statewide security policy, *Information Technology Risk Management Policy with Guidelines*, define the scope of this risk management guide. The State of North Carolina recognizes that each agency, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to the state's citizens.

This Guide explains how to assess the risk that is associated with a particular line of business that relies on information technology (IT) systems. It presents a starting point to view the activities that must be done to bring an agency into compliance with the statewide security policy, *Information Technology Risk Management Policy with Guidelines*. It demonstrates that IT risk must be considered as a part of business risk and such risk management activities must be conducted by both the business and technology managers. Agencies that require a more thorough risk analysis are encouraged to pursue further risk management activities including consultation with professional risk managers.

Assumptions

This risk assessment approach begins with the following assumptions:

- The line of business has been identified.
- The line of business relies on identified automated system(s).
- The automated system has been identified as critical to support the line of business.
- The business owner(s) have been identified.
- Staff has been identified to facilitate the risk assessment process.
- The line of business is exposed to risks other than IT.
- Legal parameters that control delivery of program services are understood.

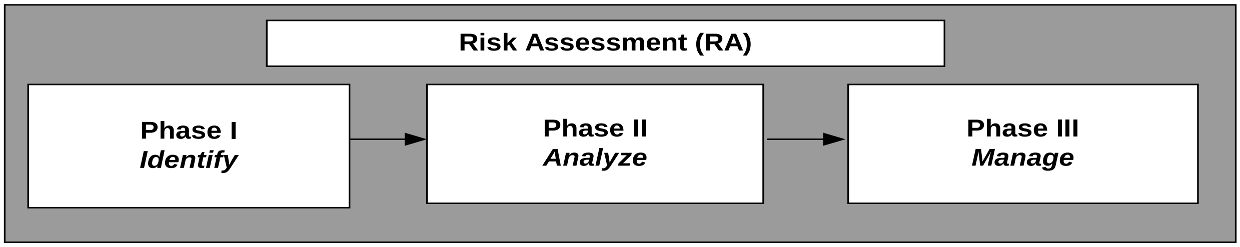
See Appendix B for a template to assist in identifying the base criteria in pre-risk assumptions.

Phased Approach

Although there are many approaches to managing business risks, this Guide provides a risk assessment process that recognizes three distinct phases. Phase I starts with identification of risks. Phase II concentrates on risk analysis activities. Phase III focuses on risk mitigation and management. This is a step down approach where the next activity phase is only conducted if sufficient risk is determined in the prior phase. This tiered approach considers agency business needs, including industry best practices for business continuity and information security. It has been designed for state government. This is a beginning, not an end, as risk management including a thorough Business Impact Analysis is a process that should be conducted on a regular basis. Risk management is an ongoing process that should be incorporated into the overall business strategies of your organization.

The utilization of a structured approach to assessing risks improves decision-making, minimizes liability, protects information assets, secures operations, and supports the legal compliance requirements of an organization. The goal is not to eliminate risk, rather to manage the risks inevitably involved in many statewide activities, and to maximize the opportunity to avoid negative outcomes. This requires state agencies to be forward thinking, have a proactive approach to assessing risk and at the same time achieve a balance between the costs of managing risks and the anticipated benefits.

Line of Business Risk Assessment Process



Risk assessment is a major part of business continuity and security planning where risk events and the frequency and probability of occurrence must be identified and properly managed. Risk assessment evaluates business dependencies and single points of failure being affected by a risk occurrence.

This three-phase approach, identified above recognizes steps within the assessment process that evolve based on the level of risk identified. This approach includes:

Phase I (Identify): Begins with business leaders identifying risks utilizing a questionnaire by evaluating threats, liabilities, and vulnerabilities, both known and potential, which may adversely impact a particular line of business. Generally speaking, risks rated as low in phase I would require a lower level of security and/or business continuity planning. Risks assessed as moderate or high proceed to Phase II.

Phase II (Analyze): Begins with mid-level managers and staff further analyzing the risks identified in Phase I by completing a more detailed questionnaire. Risk assessments rated as low in Phase II will be managed in a similar fashion as those rated low in Phase I. Risk Assessments rated as moderate or high proceed to Phase III.

Phase III (Manage): Begins with a collective group of business leaders, mid-level managers and staff to further analyze and identify the differences, effects, and methods required for reducing risk between required capabilities and those that actually exist (gap analysis). A documented action plan follows to detail, mitigate, or remove the risk. Phase III risks necessitate a much higher level of security and/or business continuity planning. (Refer to Line of Business Risk Assessment Process diagram.)

Risk Prioritization: Risk assessments enable management to determine prioritization of actual risk mitigation. This decision is based on the pre-risk assessment business impact analysis (BIA) that resulted in defined mission critical activities (MCA) and the cost/benefit analysis that was performed in phase III. This method allows for sound business continuity management (BCM) solutions that are based on industry best practices.

Risk Questionnaire

A questionnaire is utilized to document the results of the risk assessment process identified on the previous page. The questionnaire is designed to consider risk impact categories that are relative to state government where risk levels are assigned based on the National Institute of Standards and Technology (NIST) rating scale.

NIST rating scale:

Low – If an event could be expected to have a limited adverse effect on agency operations (including mission, functions, image or reputation, agency assets, or individuals; and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

***Moderate* –** If an event could be expected to have a serious adverse effect on agency operations, agency assets or individuals, and cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.

High – If an event could be expected to have a severe or catastrophic adverse effect on agency operations, agency assets, or individuals; and cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

Risk Impact Categories:

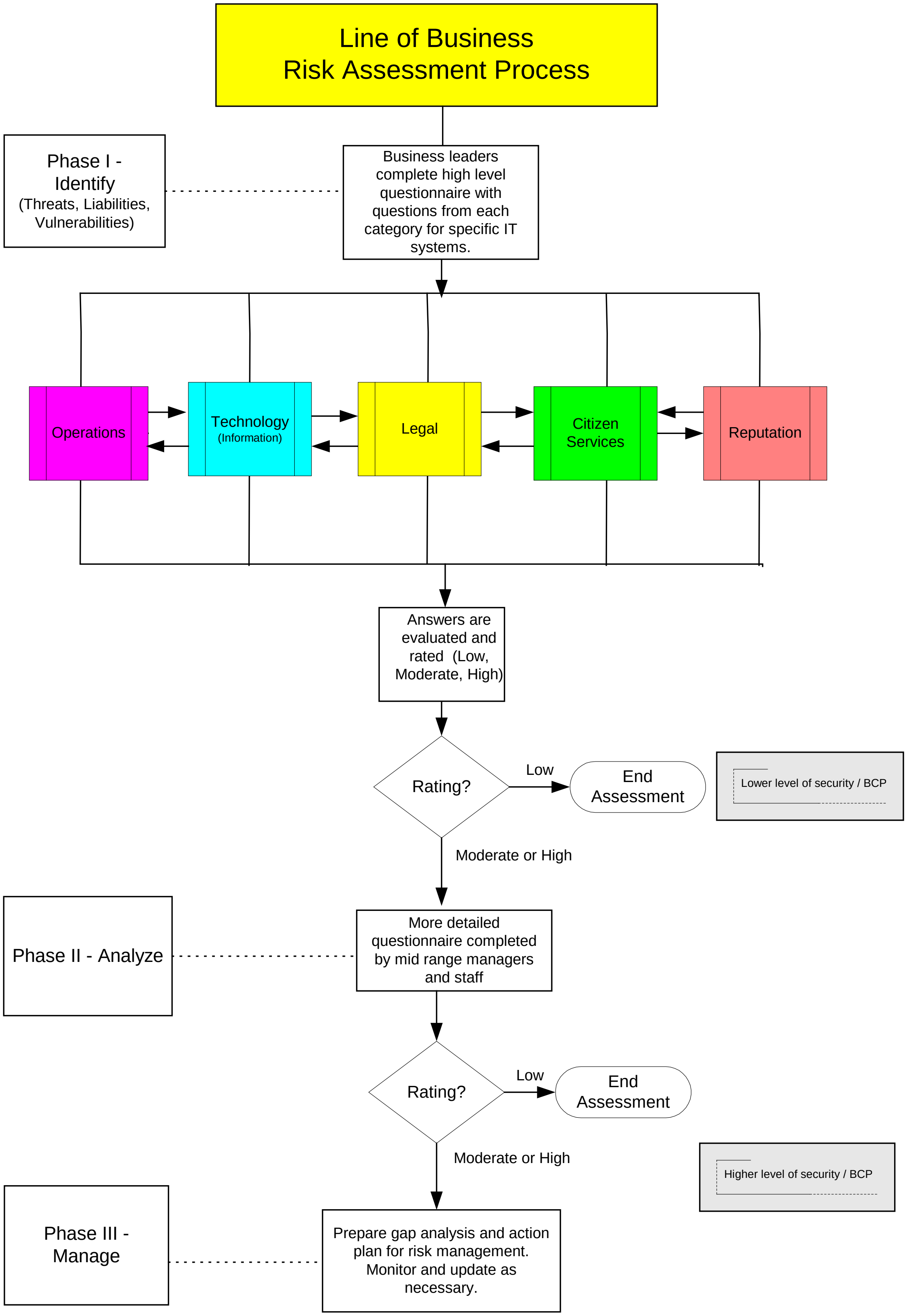
Operations – Functions that support delivery of agency business services (facilities and space allocation, personnel, purchasing, financial, communications, etc.)

Technology – Information assets that support the IT Infrastructure (security, hardware, software, middleware, network and communication systems, etc.)

Legal – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.

Citizen Services – Program services mandated by charter, legislation, or policy that provides for the delivery of the state's business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.)

Reputation – General estimation, by the public, on how state services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement.)


Line of Business
Risk Assessment Process
Phase I - Identify (Threats, Liabilities, Vulnerabilities)
Business leaders complete high level questionnaire with questions from each category for specific IT systems.
Operations
Technology (Information)
Legal
Citizen Services
Reputation
Answers are evaluated and rated (Low, Moderate, High)
Rating?
Low
End Assessment
Lower level of security / BCP
Moderate or High
Phase II - Analyze
More detailed questionnaire completed by mid range managers and staff
Rating?
Low
End Assessment
Moderate or High
Higher level of security / BCP
Phase III - Manage
Prepare gap analysis and action plan for risk management. Monitor and update as necessary.

Phase I – Identify Risks

Purpose – Business leaders identify risks by evaluating threats, liabilities, and vulnerabilities, both known and potential, which may adversely impact a particular line of business.

Participants **–** Individuals responsible and accountable for delivery of a particular line of business will respond to the questionnaire for Phase I. Participants of this group may vary based on agency size, organizational structure, and where leadership roles are recognized. A facilitator (Risk Manager / Business Continuity Specialist) or agency designee will coordinate and lead the team in completing the questionnaire. Potential participants are:

- Department/Division Head
- Chief Financial Officer and/or Chief of Administration/Operations
- Personnel Director
- Public Information Officer
- Chief Technology Officer
- Legal/Audit Staff
- Information Security Officer / Liaison
- Risk Manager / Facilitator

Activity – Participants will identify the following by completing a questionnaire:

- The internal and external threats, liabilities and exposures that could cause a business failure
- The likelihood (probability or frequency) of a threat occurring
- How vulnerable an agency is to the various types of threats and enables their prioritization and control management

Results **–** Risk levels will result in a low, moderate or high rating based on the NIST rating scale supporting the questionnaire.

- Low - requires a lower level of security and/or business continuity planning. This ends the assessment process. The results will be maintained in the risk management tool.
- Moderate or High – proceeds to Phase II for additional analysis

See Risk Management Program website for questionnaire:
http://www.esrmo.scio.nc.gov/riskManagement/default.aspx

Phase II – Analyze Risks

Purpose – Mid-level managers and staff perform a more detailed risk analysis and evaluation of those risks identified in Phase I.

Participants **–** Individuals who are knowledgeable of the particular line of business and who have some responsibility or accountability for its service delivery respond to the detailed questionnaire for Phase II. A facilitator (Risk Manager / Business Continuity Specialist) or agency designee will coordinate and lead the team in completing the questionnaire. Potential participants are:

- Business Recovery Team Members
- Section/Unit Team Leaders
- Technical Experts
- Business Managers
- Project Managers
- Facilities Manager

Activity – Participants must have an understanding of the supporting documentation identified below prior to completing the questionnaire:

- Consider the critical characteristics of each application, database, network, system and business processes supported
- Review agency critical systems, applications, equipment/software inventories, people, facilities, and interdependencies that supports the agencies line of business

Results **–** Risk levels will result in a low, moderate or high rating based on the scoring system supporting the questionnaire.

- A rating of low results in completion of the analysis with this phase. Document will be maintained in the tool for future reference.
- Ratings of moderate or high are subject to a gap analysis and action plan in Phase III.

See Risk Management Program website for questionnaire:
http://www.esrmo.scio.nc.gov/riskManagement/default.aspx

Risk Management Guide

Phase III - Risk Management

Purpose – Appropriate levels of managers and staff perform a gap analysis that focuses on risk mitigation. They will further analyze and identify the differences, effects, and methods required for reducing risk between required capabilities and those that actually exist.

Participants **-** Business leaders, owners and individuals responsible and accountable for the delivery of services for the particular line of business will respond to the questionnaire for Phase III. Potential participants are those identified in phase I and II. A facilitator (Risk Manager / Business Continuity Specialist) or agency designee will coordinate and lead the team in completing the risk analysis results and mitigation plans.

- Business Leaders
- Section/Unit/Team Leads or Managers
- Business Recovery Team Members
- Technical Experts
- Business Manager
- Project Managers

Activity – Participants will perform the following by completing a questionnaire:

- Identify options/countermeasures to mitigate the risk. These options include:
  - Avoid the risk
  - Acknowledge the risk (where it cannot otherwise be cost-effectively managed)
  - Reduce (control) the risk
  - Transfer the risk
- Analyze the cost implications of providing controls to mitigate the risk. Some risks are inherent and will never be controlled when providing a particular service. Others can be controlled, reducing the likelihood of occurrence, or transferred to another organization (outsourcing) or Agency. Residual risk is not mitigated or controlled after applying mitigation
- Determine the benefits and costs of applying risk mitigation options/countermeasures (controls) individually or in combination
- Balance the cost of implementing each option against the benefits derived from it

Results – Risk level identified in phase II of moderate or high results in a gap analysis.

- Select the risk mitigation controls to be included in the business continuity plan
- Update the business continuity plan that documents the chosen risk mitigation controls that are to be implemented
- Management will receive and review risk analysis results and mitigation plan
- Risk management action plan for corrective measures to include development of cost effective prevention recovery strategies (mitigation) must occur.

See Risk Management Program website for gap analysis and risk acceptance:
http://www.esrmo.scio.nc.gov/riskManagement/default.aspx

Appendix A - Glossary

Automated Business System **–** A business line where transactions for service delivery are performed in an automated IT environment.

Best Practices – Methodologies that provide beneficial results. Some best practices are general in nature and can be applied to almost every industry; other best practices are industry specific.

Change Management - A set of techniques that aid in evolution, composition and policy management of the design and implementation of an object or system.

Critical Application / Function – An application, activity or business function that, if unavailable, would negatively impact an agency's timely delivery of critical automated business services to the state's citizens.

Information Technology (IT) – Electronic data processing of goods and services as well as telecommunications goods and services, microprocessors, software, information processing, office systems, any services related to the foregoing and consulting or other services for design or redesign of information technology supporting business processes.

Liability - A condition or situation where reprimand or penalty could be assessed for lack of technical, legal or financial responsibility.

Line of Business (LOB) **–** A particular function or service that supports an agency's organizational mission.

Memorandum Of Understanding / Memorandum Of Agreement (MOU / MOA) - A short written statement outlining the terms of an agreement, transaction, or contract between two or more parties.

Residual Risk – The level of uncontrolled risk remaining after all cost effective actions have been taken to lessen the impact and probability of a specific risk or group of risks, subject to the organizations risk appetite.

Risk - A chance that an event will occur that will impact the State's objectives. It is measured in terms of consequence and likelihood.

Risk Appetite – The willingness of an organization to accept a defined level of risk in order to conduct business cost effectively. Different organizations at different stages of their existence will have different risk appetites.

Risk Assessment (RA) – The process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined acceptable levels of risk.

Appendix A – Glossary - continued

Risk Avoidance – An informed decision not to become involved in a risk situation.

Risk Management - The systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, assessing, treating and monitoring risk.

Risk Mitigation - Steps taken to prevent and/or eliminate the risk. Risk mitigation = policy + technology + process + training. The absence of any one element creates a major gap in your risk mitigation.

Service Level Agreement SLA – An agreement among two or more parties that establishes measurable levels of service and expectations for that service. The SLA defines users' expectations and serves as a guidepost for establishing and measuring performance goals.

Threat – An event or situation that would cause financial or operational impact to the organization. These are measured in possibilities, such as "may occur one time in 10 years." Each threat has a duration of time that the business or operation would not be able to function in its normal manner, if at all.

Vulnerability - A weakness in information systems and procedures including technical, organizational, procedural, administrative, or physical.

Appendix B - Pre-Risk Assessment Form

Base criteria required prior to performing a risk assessment.

Line of Business Services	Business Process Owner	Automated System(s) that support the business process	Critical IT Infrastructure involved (Application, database, network system, virtual enviroment)	Critical Infrastructure Dependencies (Equipment, applications, people, facilities)
1)				
2)				
3)				
4)				
5)				

Critical: An application, activity or business function that, if unavailable, would negatively impact an agency's timely delivery of critical automated business services to the state's citizens.

Notes:

Appendix C - References

DRI International – Disaster Recovery Institute International – http://www.drii.org

DRI International *Critical Infrastructure Protection Brochure*
http://www.itl.nist.gov/ITLCIPBrochure.pdf

NIST – National Institute of Standards and Technology – http://www.nist.gov/

NIST – *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems* - http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

NIST – Risk Management Framework -
http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html

State of NC General Statutes 147-33.89 *Business Continuity Planning*
http://www.ncleg.net/EnactedLegislation/Statutes/pdf/BySection/Chapter_147/GS_147-33.89.pdf

State of NC – Statewide Information Security Manual – See *Chapter 14 - Planning for Business Continuity* https://www.scio.nc.gov/Mission/InformationSecurityManual.aspx

State of NC – *Statewide IT Risk Management Program*
http://www.esrmo.scio.nc.gov/riskManagement/default.aspx

State of NC – Office of Information Technology Services - *Business Continuity Management Program*
http://www.its.state.nc.us/About/Divisions/CS/BCM/SecurityBCDRLinks.asp

State of NC – Office of Information Technology Services - *18.05 Business Continuity Management Policy* - http://www.its.state.nc.us/About/Divisions/CS/BCM/pdf/18.05revision.pdf

SunGard Availability Services -
http://www.availability.sungard.com/ITSolutions/software/Pages/software.aspx

SunGard Availability Services – Risk Assessment -
http://www.availability.sungard.com/Collateral%20Library/RiskAssessment_SEL-144.pdf

SunGard Availability Services - Business Continuity Software - Living Disaster Recovery Planning System - http://www.availability.sungard.com/Collateral%20Library/LDRPS_SEL-106.pdf

SunGard Availability Services – Business Impact Analysis Software - BIA Professional
http://www.availability.sungard.com/Collateral%20Library/BIAProfessional_SEL-111.pdf

U.S. Department of Homeland Security – http://www.dhs.gov/

~End of document~