White Paper

Developing an IT Risk Management Program

WP0196 | July 2015

Russel Jones

Russel Jones is an Orbus consultant with more than seven years experience in business and IT architectures, design and planning.

He has broad industry and region experience spanning financial services, natural resources and retail.

His Education and Certifications include: COBIT 5, TOGAF 8/ 9, ITIL 2011, Prince 2, ArchiMate 2 and B.Com Economics

Executive Summary

IT Risk Management is an important capability for any organization that relies on information technology. IT-related risks can be defined and the business risks associated with the adoption and use of IT.

The use of IT to support many core functions in business today has led to an increase in cyber-crime. This has resulted in an increased focus on properly securing businesses information and technology resources, and identifying and controlling security risks timeously. As such, the identification, management and control of IT-related risks requires a formal risk management program.

In order to define, implement and manage an effective risk management program, the following activities and outcomes should be in place:

- Identification and understanding of IT related risk;
- Developing and implementing risk management processes;
- Defining a risk model and using various tools and techniques for risk management
    - Including the implementation of principles and policies for risk mitigation and controls;
- Developing a risk assessment approach
    - Making use of risk management tools and techniques.

In this paper we will discuss these activities in more detail, and identify the key outcomes of a well-defined IT-related risk management program.

Understanding IT-related Risk

IT-related risk, according to ISACA, can be defined as the business risk associated with the adoption and use of IT. Taking this perspective on IT-related risk allows us to first consider the business impact of risks associated with the IT portfolio, as opposed to focusing on IT specific risks that may not have any substantial or material impact on the business operations. In order for a risk to be material it should have a potential negative impact on an asset, such as business information. The materiality or significance of an IT-related risk can be calculated by assessing the likelihood and impact of the risk to business information.

There are levels of risk that some organizations may be willing to accept, depending on the context of the risk and the organization. The level of acceptable risk depends on a number of factors such as the:

- Type of business;
- Corporate strategy and culture;
- Size of the organization;
- Competitor environment;
- Operating model.

IT risk is measured in terms of a combination of the probability of occurrence (likelihood) of an event and its consequence (impact).[i] We will go into more detail on this in the risk assessment approach further on in this paper.

According to NIST[ii], IT-related risks arise from liability or loss due to the following broad scenarios;

1. Intentional or accidental unauthorised disclosure, modification or destruction of information;
2. Unintentional errors or omissions;
3. IT disruptions due to disasters;
4. Failure to exercise due care when implementing and operating IT systems.

Risk identification is a core outcome of an effective risk management program, and there should be well defined processes in place to investigate and define risks. Risk management processes will be discussed in the next section.

When identifying IT-related risks, the organizational context should be considered in order to understand the holistic impact of the IT Risk to the business. The below image sourced from NIST[iii] is a simplistic overview of risks in all areas of an organization:

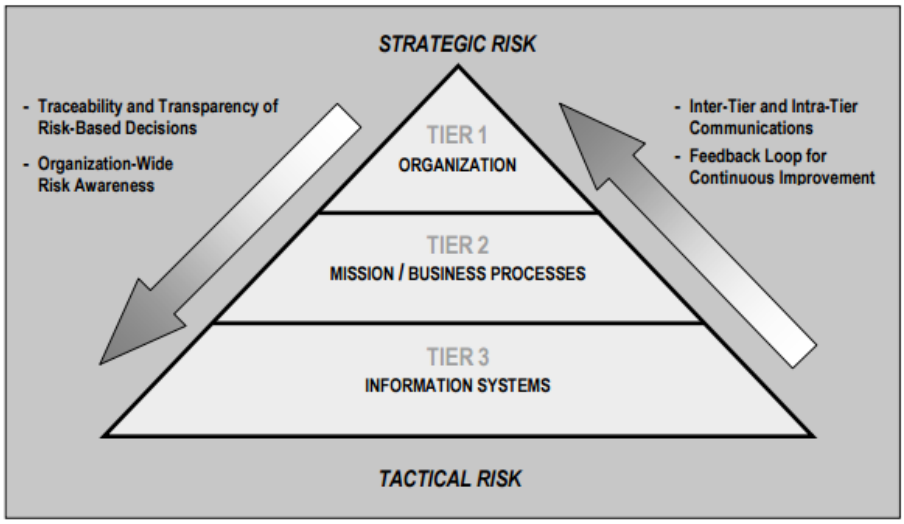

Figure 1 - Risk Management Hierarchy (Source: NIST)

This framework identifies three distinct tiers of organization risk. Tier 3 Information System risks can be mostly classified as tactical risks. In order for IT-related risks to be significant they should have some material impact on business processes, and the mission.

Traceability of tactical risks back up to strategic risks is important in order to determine materiality of risks.

IT Risk Management Processes

Risk management is about identifying potential risks and managing ways to prevent them[iv]. Defined risk management processes need to be in place in order to support the identification and management of IT-related risks.

Risk management need to be a cyclical and iterative process. The following three steps should form the main phases of any risk management process:

1. Identify risks that might prevent business objectives being achieved. This is where the traceability of tactical IT-related risks back up to strategic business risks is important. Without this view, understanding the impact on business objectives will be impossible.
2. Assess risks to see how likely or severe they will be if they do occur, in other words, assessing the risk impact and probability;
3. Manage risks to reduce their likelihood of occurring and the severity of their occurrence.

The COBIT 5 risk management processes defined in the COBIT 5 Enabling Process module are a good baseline for defining comprehensive risk management processes.[v]

The Manage Risk process (APO12) in COBIT 5 falls under the Align, Plan and Organize domain of the process reference model. This process consists of the following sub-processes or – as COBIT refers to them – management practices:

COBIT 5 Process Reference	Process Name
APO12.01	Collect data
APO12.02	Analyze risk
APO12.03	Maintain risk profile
APO12.04	Articulate risk
APO12.05	Define a risk management action portfolio
APO12.06	Respond to risk

Each sub-process further decomposes into detailed activities.

Also included in the COBIT 5 Process Assessment Model (PAM)[vi] are the following artifacts:

1. Defined process outcomes or objectives:

Process Outcome Reference	Process Outcome Description
APO12-01	IT-related risk is identified, analyzed, managed and reported.
APO12-02	A current and complete risk profile exists.
APO12-03	All significant risk management actions are managed and under control.
APO12-04	Risk management actions are implemented effectively

2. Process inputs:

Process Input Reference/Source	Process Input Description
EDM03-WP3	Evaluation of risk management activities APO12-BP1
EDM03-WP4	Risk management policies
EDM03-WP5	Key objectives to be monitored for risk management
EDM03-WP6	Approved process for measuring risk management
DSS02-WP13	Incident status and trends report
Outside COBIT	Threat advisories
DSS04-WP4	Business impact analyses
DSS05-WP2	Evaluations of potential threats
EDM03-WP1	Risk appetite guidance
EDM03-WP2	Approved risk tolerance levels
APO10-WP7	Identified supplier delivery risk
DSS05-WP2	Evaluations of potential threats
EDM03-WP7	Remedial actions to address risk management deviations

3. Process Outputs:

Process Output Reference	Process Output Description
APO12-WP1	Data on the operating environment relating to risk
APO12-WP2	Data on risk events and contributing factors
APO12-WP3	Emerging risk issues and factors
APO12-WP4	Scope of risk analysis efforts
APO12-WP5	IT risk scenarios
APO12-WP6	Risk analysis results
APO12-WP7	Documented risk scenarios by line of business and function
APO12-WP8	Aggregated risk profile, including status of risk management actions
APO12-WP9	Risk analysis and risk profile reports for stakeholders
APO12-WP10	Review results of third-party risk assessments
APO12-WP11	Opportunities for acceptance of greater risk
APO12-WP12	Project proposals for reducing risk
APO12-WP13	Risk-related incident response plans
APO12-WP14	Risk impact communications
APO12-WP15	Risk-related root causes

Defining Risk Ownership

The next step in defining effective risk management processes is to identify process ownership. Ownership ensures responsibility and accountability of identified risks within the organization. For each of the risk management processes defined in COBIT, there are recommended owners and overseers.

APO12 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Each sub-process or management practice is responsible (R), accountable (A), consulted (C), or informed (I) by a number of generic roles in a typical organization.

The IT Risk Management Toolbox

An IT risk management toolbox provides a set of templates and techniques that can be used by risk managers and auditors to assess, define and control material IT-related risks in an organization. Tools and techniques should support the risk management process.

Example categories of tools and techniques may include:

1. Risk management policies and procedures;
2. Asset identification and risk assessment templates;
3. Reporting;
4. Document management and relational database systems.

Risk Management Policies and Procedures

Risk management policies and procedures allow the risk management process to be governed and structured, and provides guidance on how to classify business risk, what assets to focus on, how to determine courses of action and what information to report. Some example policy and procedure documents include[vii]:

1. Risk Management Policy;
2. Risk Register Classification/ Categorization Procedure;
3. Risk Assessment Procedure and Checklists;
4. Risk and Control Report;
5. Risk Management Program Organization Chart;
6. Risk-based Appraisal of Change and Development Activities or Projects;
7. Requirements for the Annual Statement on Risk Management Activities.

Asset Identification and Risk Assessment Templates

Risks are associated with organizational assets. Templates to allow users to identify critical assets in the organization allow for the prioritization of IT-related risks, and help show where to focus control and mitigation efforts. This is the first step in the risk management processes, APO12.01 – Collect Data. A simple questionnaire can be completed for each asset to determine the impact on business strategy. Business objectives and strategic KPI's would be a good starting point for developing this questionnaire; develop questions to assess the business information assets supporting KPI's and objectives, for example.

Example risk assessment templates to include in the IT risk model may include:

1. Business Information/ Strategic Objectives support matrix;
2. Risk/ Control Matrix;
3. Risk Classification Matrix (likelihood vs. severity);
4. Risk Identification Questionnaire or Survey;
5. Strategic Objective > Business Unit > Risk > Control traceability view.

Reporting

An important output of a risk management program is to communicate the IT-related risks identified, assessed and mitigated to the organization on a regular basis. Reporting should be tailored to the target audience, including only pertinent information. A comprehensive report detailing every risk and control for all IT assets will not be effective if presented to a Chief Information Security Officer (CISO) for example. This high power stakeholder should only be presented with a summary of actions taken in risk areas such as security and compliance. Other stakeholders such as IT auditors may be interested only in compliance type risks.

Additionally, certain categories of risk may require more or less frequent reporting intervals. An example table below identifies four risk categories, interested parties, and reporting intervals:

Risk Category	Interested Parties	Reporting Interval
Security Risks	CISO, Auditor	Bi-monthly
Availability/ Operational Risks	COO, Business Unit Leader	Monthly
Performance Risks	CTO	Monthly
Compliance Risks	CEO, COO, Board, Auditor	Quarterly

Reporting templates should be defined to ensure information presented is targeted and consistent. Reports should be archived for future reference and audit purposes.

Document Management and Relational Database Systems

A mature and structured IT risk management program cannot be properly managed using excel spreadsheets and disparate documents and reports. A central storage point for risk management work product, reports and assessment data needs to be put in place. The iServer Governance, Risk and Compliance solution from Orbus Software offers a number of useful capabilities to support a risk management program.

All the COBIT 5 risk management processes, along with process owners (RACI) mentioned previously are predefined in the repository, allowing organizations to reference and tailor them to their requirements. These

processes can be related to other components of your risk management program such as goals and objectives, as well as other technical and business components such as applications, information, strategic level goals etc. This provides the ability to perform traceability analysis and ensures risk assessments take the organization's context into consideration – an important function for determining the materiality of identified risks.

The iServer toolset also provides support and integration for all Microsoft Office documentation providing risk management documentation management support. Reporting capabilities with pre-defined risk management reports are included in this solution.

Performing an IT-Risk Assessment

As mentioned earlier, an IT-risk assessment is an iterative process. Coupled with these processes are a number of policies, procedures and outputs which form the risk management framework.

Performing a risk assessment within the defined risk management framework can be broken down into the following phases:

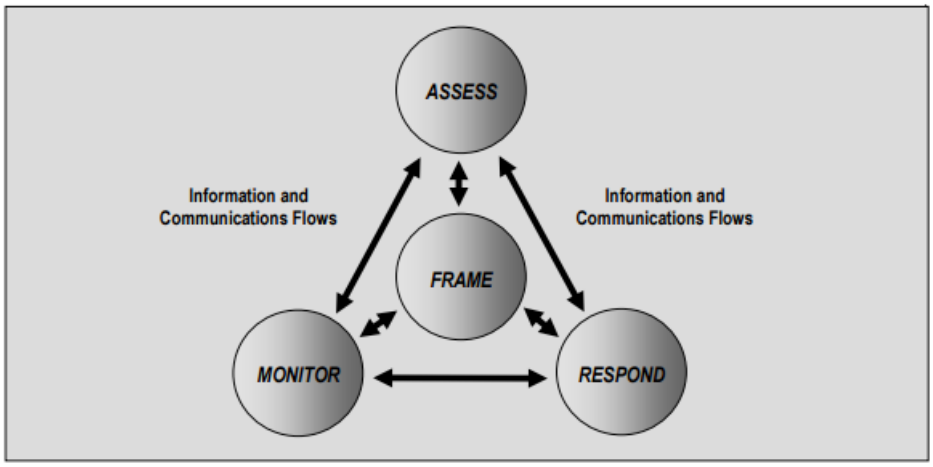

Figure 3 - Performing an IT-Risk Assessment (Source: NIST[viii])

The framework (processes, procedures and policies) guides the assessment with predetermined outputs and templates.

1. Risk assessment is the first step in the approach. COBIT 5 risk management processes involved in this phase include:
    a. APO12.01 - Collect Data
    b. APO12.02 - Analyse Risk
    c. APO12.03 - Maintain Risk Profile
    d. APO12.04 - Articulate Risk

    Each of these processes decompose into detailed steps to be carried out, with defined owners, inputs and outputs.

    Once risks have been identified, they should be quantified based on the impact of the risk (severity) on the business should it occur, and likelihood of the risk occurring.

This matrix is an example of how identified risks can be prioritized using the severity and likelihood:

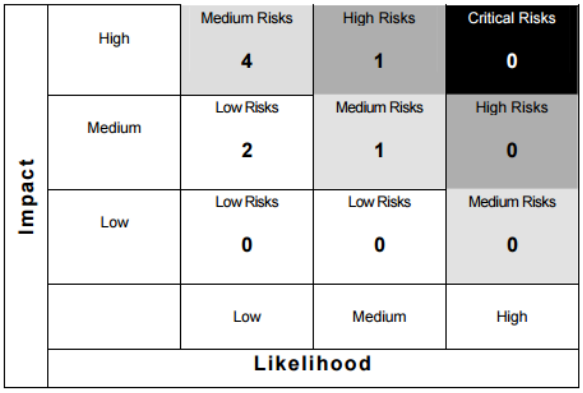

Figure 4 - Risk Prioritization Matrix

Critical risks will be those in the top right hand corner of the matrix, with high likelihood of occurring, and a high business impact (materiality). Risks in this area of the matrix should be closely monitored and responses to these risks should be prioritized.

2. Identified risks should be responded to according to predefined categorizations, policies, processes and procedures. Risk responses may include risk acceptance, risk transfer and mitigation. COBIT 5 risk management processes applicable in this phase include:
    a. APO12.05 Define a risk management action portfolio
    b. APO12.06 Respond to risk
3. Accepted and transferred risks should be monitored to ensure materiality or potential impact has not changed. The risk register should be continuously monitored and maintained. Monitored risks may need to be reassessed based on changing business priorities or projects. These will feed back into the Assess phase, and may require further response in the Respond phase – enforcing the need for an iterative risk assessment approach.

Summary

IT risk management is an increasingly important capability within almost all organizations today. Understanding the business impact of IT-related risks is at the core of an effective risk management program. In order to understand this traceability, a structured, formalized and iterative framework needs to be in place. The building blocks of this framework discussed in this paper included:

- Defined risk management processes with inputs, outputs and organization involvement (RACI),
- Tools and techniques such as templates, categorization, surveys,

reports and software tool support.

A phased and cyclical risk management program then needs to be implemented in order to implement this framework which we discussed in the Performing and IT-Risk Assessment section.

Basing your risk management program on best practices such as COBIT 5 for Risk, the Process Assessment Model (PAM) and the Enabling Process module ensures a comprehensive approach, and may improve the auditability of the program.

Toolset support for your IT risk management program ensures compliance and governance of the program, and aids analysis and reporting of the risk register. The iServer Governance, Risk and Compliance (GRC) solution offers a range of out the box risk management features.

References

[i] ISO/IEC 27001:2005 - Information technology—Security techniques—Information security management systems—Requirements reference: www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103

[ii] Information Security (2012). National Institute of Standards and Technology (NIST) – Technology Administration, U.S. Department of Commerce.

[iii] Information Security (2012). National Institute of Standards and Technology (NIST) – Technology Administration, U.S. Department of Commerce. Chapter 2, Page 17.

[iv] Risk Management Program (2006). University of London. Page 1.

[v] COBIT 5 Enabling Processes (2012): www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx

[vi] Process Assessment Model (PAM): Using COBIT 5 (2013): www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx

[vii] Risk Management Program (2006). University of London. Page 5.

[viii] Information Security (2012). National Institute of Standards and Technology (NIST) – Technology Administration, U.S. Department of

Orbus Software UK
London

Orbus Software US
New York

Orbus Software AUS
Sydney

Orbus Software RSA
Johannesburg

enquiries@orbussoftware.com | **www.orbussoftware.com**

Seattle Software Ltd. Victoria House, 50-58 Victoria Road, Farnborough, Hampshire, GU14 7PG. T/A Orbus Software. Registered in England and Wales 5196435