### C:\Users\zhct1.NCCADMIN\Downloads\NCC_BRANDMARK_cmyk.jpg

# ICT Risk Management Standard and Procedure

|  |
| --- |
| **Revision History** |
| **Version** | **Date**  | **Detail** | **Author** |
| 0.1 | 28/02/2014 | First Version | Kevin O’Connor |
| 0.2 | 01/11/2017 | Copy Document to new format | Susan Horobin |
| 0.3 | 09/01/2020 | Update of Document ready for Process review in April 2020 | Susan Horobin |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **Background**

Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Risks can come from various sources including uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustaining of life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities.

Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all the potential or actual consequences of a particular threat.

In Information Technology, Risk management includes "Incident Handling", an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. For Cyber Security Events this will include the ICT Cyber Security Incident Process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

## **Purpose**

This Standard is the Management of Risks for the ICT Operational Delivery Group within NCC (Nottinghamshire County Council). The Procedure follows the M\_O\_R (Management of Risk) Methodology.

## **Scope**

The scope of this document is to specify the overall standard, procedure and Roles and Responsibilities for the M\_o\_R Risk Management Process.

# Method and Principles

## **Method**

For the most part, these methods consist of the following elements, performed in the following order.

1. Identify the threats
2. Assess the vulnerability of critical assets to specific threats
3. Determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
4. Identify ways to reduce those risks
5. Prioritize risk reduction measures

## **Principles**

Risk management should:

* Create value – resources expended to mitigate risk should be less than the consequence of inaction
* Be an integral part of organizational processes
* Be part of a decision making process
* Explicitly address uncertainty and assumptions
* Be a systematic and structured process
* Be based on the best available information
* Be tailorable
* Take human factors into account
* Be transparent and inclusive
* Be dynamic, iterative and responsive to change
* Be capable of continual improvement and enhancement
* Be continually or periodically re-assessed

# Procedure

This involves:

1. observing the context
	* the social scope of risk management
	* the identity and objectives of stakeholders
	* the basis upon which risks will be evaluated, constraints.
2. defining a framework for the activity and an agenda for identification
3. developing an analysis of risks involved in the process
4. mitigation or solution of risks using available technological, human and organizational resources

## **Identification**

Risks are about events that, when triggered, cause problems or benefits. Risk sources for the ICT Operational Delivery Risk Management Process are the ICT employees of NCC (Nottinghamshire County Council).

The risks that are raised are from identified threats, incidents, issues or problems related to the ICT systems and services within NCC and are classified as:

* Security Risks - Those of unauthorized access, alteration or use of information
* Availability Risks - Those of inaccessible business processes or data
* Performance Risks - Those of delayed access to business processes or data
* Compliance Risks - Those of violating legal, regulatory or IT policy requirements
* Reputational Risks – Those that have the potential of loss to financial capital, social capital and/or market share resulting from damage to a firm's reputation

## **Assessment**

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of an unlikely event, the probability of occurrence of which is unknown. Therefore, in the assessment process, the initial assessment for every risk is to place it at a Very High status, so that it is communicated to Management and evaluated by the Operational Delivery Management Team (ODMT). Even a short-term positive improvement can have long-term negative impacts.

The primary sources of information for risk assessment is made up of best educated opinions and available statistics. To better understand and communicate risks to senior executives the most widely formula for risk quantification is: "Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude."

### **Severity and Impact**

 **LIKELIHOOD**

1. Rare 0 - 5 % Chance
2. Unlikely 6 to 20% Chance
3. Possible 21 to 50% Chance
4. Likely 51 to 80% Chance
5. Almost Certain 81% + Chance

**IMPACT**

1. Insignificant 0 - 5% Chance
2. Minor 6 to 20% Chance
3. Moderate 21 to 50% Chance
4. Significant 51 to 80% Chance
5. Catastrophic 81% + Chance

## **Potential risk treatments**

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

* Avoidance (eliminate, withdraw from or not become involved)
* Reduction (optimize – mitigate or control)
* Sharing (transfer – outsource or insure)
* Acceptance (accept and budget)

#### **Risk avoidance**

This includes not performing an activity that could present risk. Avoidance may seem like the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.

#### **Risk reduction**

Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

#### **Risk sharing**

Briefly defined as "sharing with another party or team (including external vendors) the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk."

The term of 'risk transfer' is often used in place of risk sharing which means you can transfer a risk to a third party, or to another team.

Some ways of managing risk will fall into multiple categories.

#### **Risk Acceptance**

Risk acceptance involves accepting the loss, or benefit of gain, from a risk when the incident occurs. Risk retention is a viable strategy for Low risks or for Risks where there is a long term strategy and a workaround in place.

## **Risk Register and Risk Report**

Risks are raised by ICT and added to the Operational Delivery Group Risk Register. Risk mitigation needs to be approved by Operational Delivery Management Team and updated on the Register and Report.

The risk management register and report should propose applicable and effective security controls for managing the risks and contain a schedule for the controlled implementation and responsible persons for those actions.

All the decisions about how each of the identified risks should be handled must be documented on the Register and Report.

## **Review and Evaluation of the ICT Risks on the ICT Operational Delivery Group Risk Register and Risk Reports**

The Risk Analysis on the Risk Register is updated bi-weekly and the Top 5 Very High categorized risks are presented at the Operational Delivery Management Meeting bi-weekly.

Risks are measured by impacts × probability. With bi-weekly reviews, the Very High Risks are re-evaluated depending on the completion of mitigations or acceptance and can be downgraded for monitoring.

Risks are reported on the Monthly Performance Reporting.

Cost formulae can be associated with Risks to determine budget:

* the cost associated with the risk if it arises, estimated by multiplying employee costs per unit time by the estimated time lost (*cost impact*, *C* where *C = cost accrual ratio \* S*)
* the probable increase in time associated with a risk (*schedule variance due to risk*, *Rs* where Rs = P \* S):
	+ Sorting on this value puts the highest risks to the schedule first. This is intended to cause the greatest risks to any process or project to be attempted first so that risk is minimized as quickly as possible.
	+ This is slightly misleading as *schedule variances* with a large P and small S and vice versa are not equivalent. (The risk of the RMS *Titanic* sinking vs. the passengers' meals being served at slightly the wrong time).
* the probable increase in cost associated with a risk (*cost variance due to risk*, *Rc* where Rc = P\*C = P\*CAR\*S = P\*S\*CAR)
	+ sorting on this value puts the highest risks to the budget first.
	+ see concerns about *schedule variance* as this is a function of it, as illustrated in the equation above.

Risk in a project or process can be due either to Special Cause Variation or Common Cause Variation and requires appropriate treatment.

# Roles and Responsibilities

## **Risk Identifier**

The Risk Identifier is anyone who puts forward to the Risk Manager (Via the process) a “*Potential Risk”*. The Potential Risk can be anything that the raiser believes will have an impact on the business.

## **Risk Manager**

The Risk Manager is the owner of the Risk process and is responsible for:

* Appointing ownership of risks
* Chair of the Risk Forum Review Meetings
* Reviewing, Rejecting, Logging, Activating and Escalating any potential risk.
* The management and update of the Risk register, ensuring that actions are delivered.
* Communications and feedback to all stake holders (via the Risk Report).
* Closing completed risks
* Gaining sign off for “Accepted “risks.

## **Risk Owner**

The Risk Owner is responsible for:

* Defining the specific risk.
* Defining any mitigations in the short term
* Creating solutions in the long term
* Communicating with all stakeholders
* Updating the Risk log and Risk manager in a timely and accurate manner.

## **Operational Delivery Group Manager**

The Operational Delivery Group Manager is responsible for:

* Providing Guidance
* Escalating to the IT Director
* Reporting to the IT Director
* Chairing the Operational Delivery Group Management Team (ODMT) Meetings
* Signing off Risk Acceptance