IC3S

Risk Management

(STQC/CC/P11)

Issue : 02

CC Certification Body, STQC Directorate,
Indian Common Criteria Certification Scheme (IC3S),
MeitY, Government of India
INDIA

Table of Contents

0.1 FOREWORD

This document describes the risk management process in the Indian Common Criteria Certification Scheme (IC3S). It specifies the risk their impact and mitigation strategy.

0.2 APPROVAL AND ISSUE

Reviewed by : Management Representative

Approved by : Head, IC3S Scheme

Note:

- Management Representative is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

0.3 AMENDMENT RECORD

Sl. No.	Date	Issue	Reason of Change /Change Details
1.	August 2018	01	First Issue
2	15-04-21	02	Add Mitigation in Risk Register table

1.0 INTRODUCTION

1.1 BACKGROUND

Indian Common Criteria Certification Scheme (IC3S) is operated by STQC Directorate, Ministry of Electronics and Information Technology (MeitY), Govt. of India. Under supervision of CB, the Evaluation Laboratories or Common Criteria Test laboratories (henceforth will be referred as CCTL) perform evaluations of Information Technology (henceforth will be referred as IT) security products against the requirements of ISO 15408 or Common Criteria Standards.

1.2 PURPOSE

2 This document provides the consistent method to manage risks to ensure success.

3 Risk management is the processes for identification, assessment, mitigation, tracking, control and management of the risks. It drives decisions that affect the operation of CB. The purpose of this document is to describe the risk management process in the operation of CB activities.

1.3 REFERENCE

STQC/CC/DO2 : Quality Manual of the Certification Body

ISO/IEC 17065 : Conformity assessment -- Requirements for bodies Certifying products, processes and services

ISO/IEC 17025 : General Requirements for the Competence of Testing and Calibration Laboratories.

*(Please refer **Master List of Documents** for latest version of the documents)*

1 RISK MANAGEMENT PROCESS

Risk management involves four major phases: risk identification, risk analysis, risk response planning, and risk monitoring and control.

1.1 RISK IDENTIFICATION

The risk identification process is to identify the potential risk, which can hamper the operation of certification body. The ultimate purpose of risk identification is to minimize the negative impact and threats, and to maximize the positive impact. Only identification of risk will not be sufficient; however, awareness of potential risks reduces the number of surprises during the delivery and, thus, improves the chances of success, allowing the team to meet the time, schedule, and objectives.

Risk Identification will involve the CB team and appropriate Stakeholders. Careful attention will be given to the deliverables, assumptions, and key CB documents.

1.1.1 METHODS FOR RISK IDENTIFICATION

The following methods may be used to assist in the identification of risks associated with CB:

- Brainstorming
- Assumption and Constraint Analysis
- Strengths, Weaknesses, Opportunities, Threats (SWOT) Analysis
- Lessons Learned
- Delphi Technique
- Etc.

A Risk Register will be generated and updated as needed. (Pls. see the risk register)

The potential risk in the operation of CB are identified and are listed in **risk register.**

1.2 RISK ANALYSIS

All risks identified will be assessed to identify the range of possible outcomes. Risks will be prioritized by their level of importance.

2.2.1 Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk will be assessed by the PM, with input from the Project Team using the following approach:

- Probability - is the likelihood that a risk will occur.
- Impact - is the consequence the risk will have on the CB when it does occur.

Risks are evaluated against a standard impact/probability scale using a clearly defined range.

The table below is Risk Scoring Matrix that provides a standard method to calculate grading based upon combination of probability and impact ratings.

	Impact (Seriousness)					
		Very Low	Low	Medium	High	Very High
Probability (Likelihood)	Very High					
	High					
	Medium					
	Low					
	Very Low					

Score	Definition
High	An event that is extremely or very likely to occur and whose occurrence will impact the CB so severely and harm his reputation; this risk should be escalated (where possible) and reviewed frequently
Medium	An event that has a 50-50 chance of occurring and, if it occurs, will cause noticeable loss; this risk should be reviewed regularly
Low	An event that is unlikely or very unlikely to occur and, if it occurs, will

	cause small or no harm, in most cases, can be absorbed by the CB

1.3 RISK RESPONSE PLANNING

Each major risk (those falling in the Red & Yellow zones) will be assigned to a Risk Owner for monitoring and controlling purposes to ensure that the risk will not "fall through the cracks".

For each major risk, one of the following approaches will be selected to address it:

- **Risk Avoidance**: Make changes eliminate the risk or to protect the objectives from its impact by eliminating the cause. It may be change in scope, change in technical approach, or the addition of resources to avoid or eliminate the risk.
- **Risk Transference**: Transfer responsibility and ownership of the risk to an outside resource or organization. It may be contracting out a specialized technical component when the Team lacks the skills.
- **Risk Acceptance**: Acknowledge the existence of the risk and accept its consequences if it occurs.
- **Risk Mitigation (Controlling):** Incorporate the ongoing monitoring and handling of risks throughout the life of the activity to reduce the impact or probability of the risk. These mechanisms involve the use of reviews, possibly adding milestones, and development of counter measures. Introducing new processes or procedures to lessen the probability of occurrence of risk.

For each risk that will be mitigated, the Team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the schedule, adding resources, etc. Any secondary risks that result from risk mitigation response will be documented and follow the risk management protocol as the primary risks.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined in the event that the risk does materialize in order to minimize its impact.

1.4 RISK MONITORING AND CONTROL

The identified risks will be reviewed in management review meeting. These will be reviewed for the following:

- That all requirements of the Risk Management are being implemented.
- Assess currently defined risks as identified.

- Evaluate effectiveness of actions taken.
- Identify status of actions to be taken.
- Validate previous risk assessments (likelihood and impact).
- Validate previous assumptions and state any new assumptions.
- Identify new risks.
- Track risk response.
- Validate risk mitigation strategies and alternatives.
- Take corrective action when actual events occur.
- Assess impact on the project of actions taken (cost, time, resources).
- Identify new risks resulting from risk mitigation actions.
- Ensure change control addresses risks associated with the proposed change.
- Revise risk management documents to capture results of mitigation actions.

Risk Register

Risk ID	Description of Risk	Impact	Probability	Mitigation	Remarks
CB-01	CCTL empanelment: Favour to some lab. For empanelment	High	Low	D04– Requirements for Testing Laboratories has fixed Rules and procedure.	Impartiality
CB-02	Assignment of Product evaluation to some specific CCTL	High	Low	Section 6.5 of P09– Application Handling address the issue	Impartiality
CB-03	Sharing of product specific documents	High	Low	Confidentiality is maintained as per section 2.5 of D02- Quality manual	Confidentiality