### Experiment No: 1

### Name: Nikita Kulkarni Roll No: 29

### Aim: To study Project Failure Analysis

**Case Study**: 3.3 Canadian Cancer Therapy Machine Therac-25 Failure

**Case Study:**

3.3. Case Study Canadian Cancer Therapy Machine (Therac-25, 1986) Designed by Atomic Energy of Canada, Ltd. (AECL): Therac-25 was a software controlled radiation therapy machine used to treat people with cancer. Between 1985 and 1987 Therac-25 machines in four medical centers gave massive overdoses of radiation to six patients. An extensive investigation and report revealed that is some instances operators repeated overdoses because machine display indicated no dose given. Some patients received between 13,000 - 25,000 rads when 100-200 needed. The result of the excessive radiation exposure resulted in severe injuries and three patients deaths[5]. Causes of the errors were attributed to lapses in good safety design. Specific examples are cite failure to use safety precautions present in earlier versions, insufficient testing, and that one key resumption was possible despite an error message. The investigation also found calculation errors. For example, the set-up test used a one byte flag variable whose bit value was incremented on each run. When the routine called for the 256th time, there was a flag overflow and huge electron beam was erroneously turned on. An extensive investigation showed that although some latent error could be traced back for several years, there was an inadequate system of reporting and investigating accidents that made it hard to determine the root cause. The final investigations report indicates that during real-time operation the software recorded only certain parts of operator input/editing. In addition, the radiation machine required careful reconstruction by a physicist at one of the cancer centres in order to determine what went wrong.

**Reason for Failure:**

* Lapses in good safety design.
* Improper use of component based development:

Use safety precautions present in earlier /older versions which are sufficient for current version.

* Improper implementation Testing Phase: Insufficient testing is conducted.
* Calculation errors.
* Inadequate system of reporting and investigating accidents because of which root cause can’t be determined.
* Real-time operation the software recorded only certain parts of operator input/editing.
* Poor Communication between development team and expert:

Radiation machine required careful reconstruction by a physicist at one of the cancer centers in order to determine what went wrong which was not done.

**Actions to mitigate the failure:**

* **Conduct Software Reliability testing:**

**Software reliability testing** is a field of software testing that relates to testing software’s ability to function, given environmental conditions, for a particular amount of time. Software reliability testing helps discover many problems in the software design and functionality.

**1) Regression test**

Regression testing is used to check if any new bugs have been introduced through previous bug fixes. Regression testing is conducted after every change or update in the software features.

* **Use of advance safety precautions : Invest in third party audits**

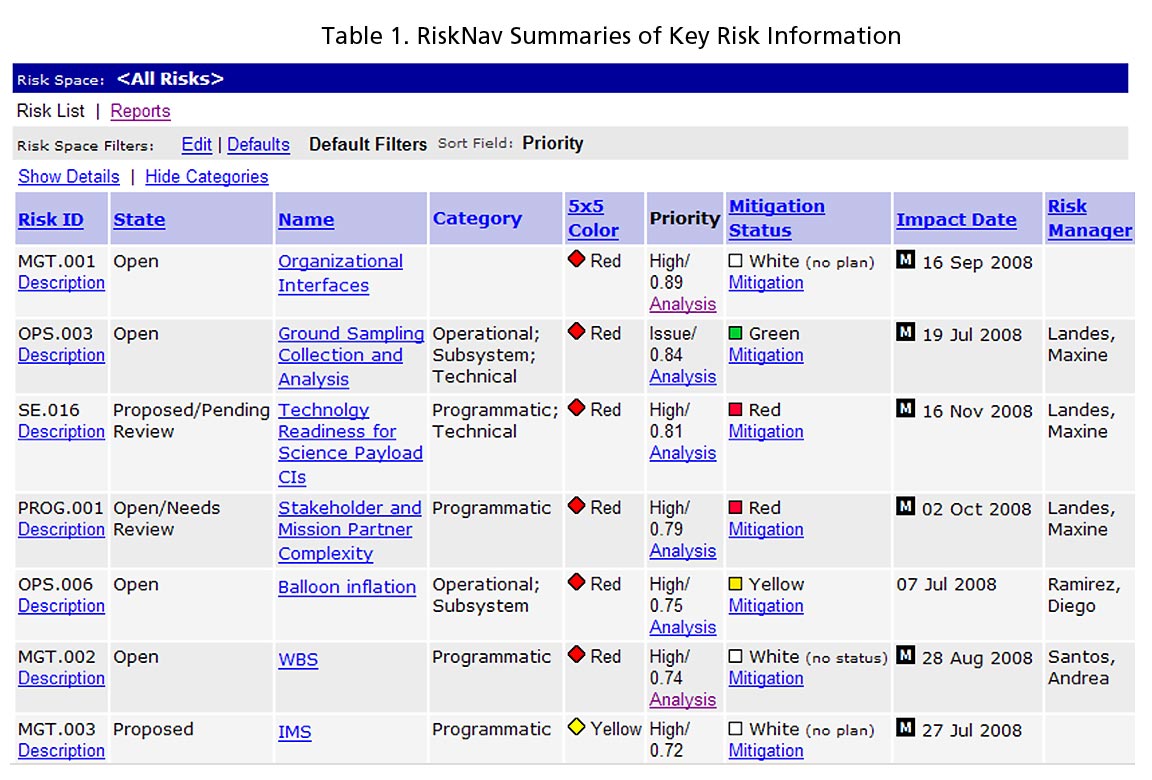
Investing in SOC2 Type 2 or ISO 27001 certifications will give you additional assurances that your security controls have been correctly designed and implemented. This is important because it takes a tremendous amount of work to successfully manage all the individuals responsible for required security controls. Things do fall through the cracks and having an external auditor identify gaps will ensure you are following your controls.

* **Usage of effective reporting and investigating system for risk analysis and management:**

MITRE Developed Tools

**RiskNAV**is a well-tested tool developed by MITRE to facilitate the risk process and help program managers handle their risk space. RiskNav lets you collect, analyze, prioritize, monitor, and visualize risk information in a collaborative fashion. This tool provides three dimensions of information graphicallyrisk priority, probability, and mitigation/management status.

RiskNav presents the risk space in tabular and graphical form. The tabular form presents key information for each risk, and allows the risk space to be filtered and sorted to focus on the most important risks. The information in the tables and figures is artificial and for illustrative purposes only. It does not represent real programs, past or present.



* Active participation of physicist in requirement, designing and periodic meetings of developer, physicist, client or stakeholder.

**Technical feasibility:**

Theproject is technically feasible but needs following changes:

1) Proper Implementation of testing phase

2) Improve Communication between development team and expert

3) Usage of effective reporting and investigating system for risk analysis and management.

**Conclusion:**

As software has become integral part of every product and process so there is a need to make a full proof system so that the software failures could be avoided. There is further requirement of root cause analysis of these software failures to understand the problematic area and suggest the areas of improvement in the current process as several corrective & preventive actions needs to be taken while developing products and software systems.