Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

A Prototype Software Application for Risk Data Analytics within the Canadian Safety and Security Program

Darrell O'Donnell, P.Eng.
Continuum Loop Inc.

Prepared by:
Coradix Technology Consulting Ltd.
151 Slater St., Suite 1010, Ottawa, ON K1P 5H3

PSPC Contract Number: W7714-135734

Contractor's Date of Publication: June 2017

Technical Authority: Shaye K. Friesen

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2017-C210
September 2017

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the Defence Production *Act*.

A PROTOTYPE SOFTWARE APPLICATION FOR RISK DATA ANALYTICS WITHIN THE CANADIAN SAFETY AND SECURITY PROGRAM

Darrell O'Donnell, P.Eng.
Continuum Loop Inc.

Prepared By:
Coradix Technology Consulting Ltd.
151 Slater St., Suite 1010
Ottawa, ON K1P 5H3

PWGSC Contract Number: W7714-135734
Technical Authority: Shaye Friesen, Defence Scientist, DRDC Centre for Security Science (CSS)

Contract Report DRDC-
RDDC-2017-C210
June 2017

Abstract

Under a Canadian Safety and Security Program (CSSP) targeted investigation (TI) project (CSSP-2015-TI-2130), the Defence Research and Development Canada (DRDC) Centre for Security Science (CSS) began development of a prototype web application to assist in managing risk-related information in its portfolios. This report summarizes the development efforts and the prototype application that was created.

The application provides methods for Portfolio Managers and Risk Analysts to gather basic risk-related information. It provides visualization tools that allow CSS leadership to see where risk measures are being applied in portfolios.

Table of Contents

List of Figures

1 Background

Under a Canadian Safety and Security Program (CSSP) targeted investigation (TI) project, establishing a Risk and Capability Based Framework for Assessing CSSP Investments (CSSP-2015-TI-2130), the Defence Research and Development Canada (DRDC) Centre for Security Science (CSS) led an examination of industry software to assess its suitability for internal use for portfolio managers. As part of this project, one of the outcomes was to recommend options and provide advice for acquiring a commercial-off-the-shelf (COTS) tool, or developing in-house a prototype "dashboard" with a graphical user interface and searchable database, which would allow users / risk analysts to compare risks and investment choices across CSSP Portfolios, and support decision making within the Centre (e.g., prioritization of investment, data collection, analysis, etc.).

This report summarizes the feasibility of using COTS software to provide visibility into the CSS use of risk for investment prioritization. Requirements were gathered, industry software examined, and results have been summarized and recommendations made. The report documents and describes the development of a centralized repository (i.e., Risk Dashboard) for tracking and monitoring risk assessment information (and scenario library) available to Portfolio Managers and Communities of Practice (CoPs). This Risk Dashboard – the first of its kind to be developed in the CSSP – facilitates risk comparison across the organization at an enterprise-wide level, enables roll-up and reporting of information, and informs long-term trend analysis. The Risk Dashboard is an interactive, web-based application (built in Node.js and Angular for front end) that lists Portfolios with risk exposure and maturity levels, and enables users to store, edit and manage information on risks, uncertainties and notes.
COTS software products are aimed at providing deep risk management and visibility into those risks. They are not tailored to provide the CSS with the visibility into how risk is being considered as one of many variables in setting portfolio investment priorities. A basic development project was recommended in a formal contract report (O'Donnell, Software Applications Support for All Hazards Risk Analysis within the Centre for Security Science 2016) to further explore the CSS requirements.

This contractor report describes the results of a short development project that created a Portfolio Based Risk Dashboard application for use in exploring future application of risk to CSS' portfolio and project decisions. It provides a "leave-behind" capability in the form of a CSSP Risk Dashboard application for internal-to CSSP use by risk analysts and Portfolio Managers to track / monitor risks within their specific research domain, thereby improving visibility and risk communication. The Risk Dashboard provides preliminary considerations for framing the development of an Enterprise Risk Management (ERM) solution or tailored application that can be further matured to support the CSSP or other defence excellence and security programs.

2 Approach

An Agile approach was used in this project to ensure that the learned and emergent requirements could be capitalized upon while ensuring regular delivery of basic functioning tools.

The project used an Agile SCRUM-based approach to ensure that as learning continued it was applied to subsequent development and design. Daily stand-up meetings with the development team and regular meetings with the Technical Authority allowed the team to adapt to learning.

To develop the Risk Dashboard project performed the following tasks:

- Review industry tools[1].
- Creation of mockups explaining general User Experience (UX) concepts
- Development of Data Model in MongoDB
- Creation of MEAN.io based application
- Development with iterative feedback based on deployed application

The project used an Agile SCRUM-based approach to ensure that as learning continued it was applied to subsequent development and design. Daily stand-up meetings with the development team and regular meetings with the Technical Authority allowed the team to adapt to learning. Additionally, approach built upon previous work and DRDC CSS knowledge and experience in other risk assessment projects, such as the federal All Hazards Risk Assessment (AHRA); the automated tools and templates associated with the SharePoint instance of the AHRA that currently resides on the DRDC CSS Technical Operations Portal (CSS-TOP); the chemical, biological, radiological/nuclear and explosive (CBRNE) Consolidated Risk Assessment (CRA) that is applied to malicious threats/hazards for relevant counter-terrorism communities; capability assessment rating tools such as the Capability Assessment Management System (CAMS); literature reviews that consider other tools and frameworks, such as the United Kingdom's Office of Government Commerce's *Portfolio Management Guide*;[2] as well as consultations with key stakeholders and senior management in DRDC CSS.

The project approach also stemmed from diversity of portfolios, each of which manages risks separately (see Figure 1 below) and establishes the need for a more coordinated approach to applying capability and risk based assessment best practices to inform planning, S&T investments and the CSSP priority setting process.

[1] (O'Donnell, Software Applications Support for All Hazard Risk Analysis Within the Centre for Security Science 2016)

[2] United Kingdom, Cabinet Office, Office of Government Commerce, *Portfolio Management Guide* http://www.epmgroup.dk/files/u2/PfM_Guide_OGC.pdf. Accessed June 2017.

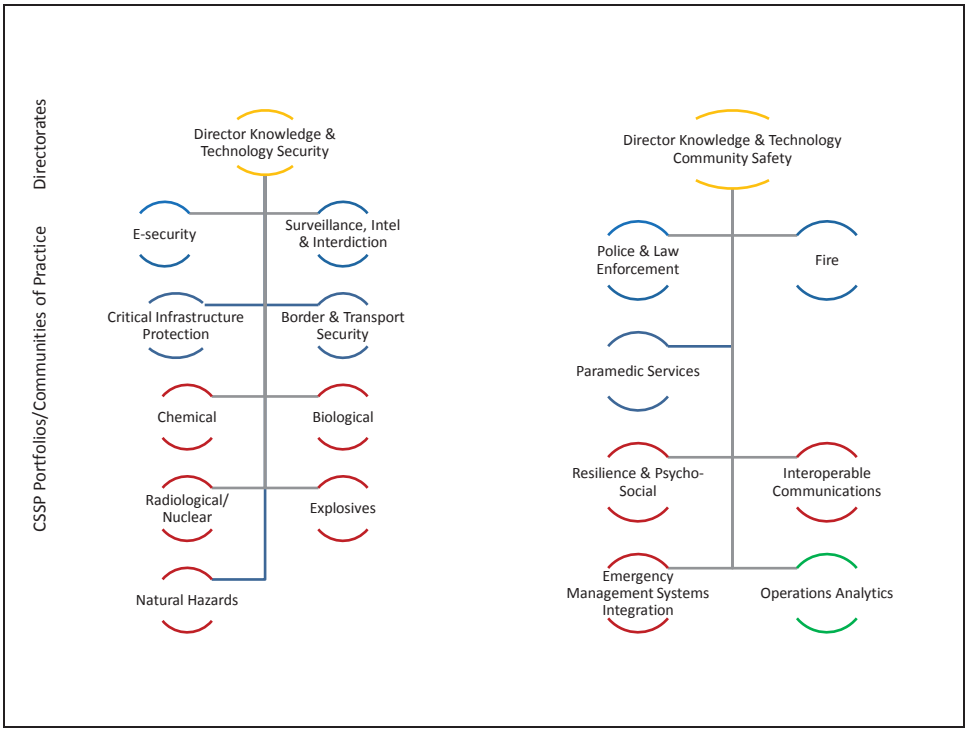

Figure 1 - Project Motivation: Diverse Portfolios (Areas of Focus)

2.1 Data Modeling

After examining the business requirements, a Conceptual Data model (Figure 2) was created that explain the hierarchy and interaction of Portfolios, Projects, and Risks in the CSSP context.

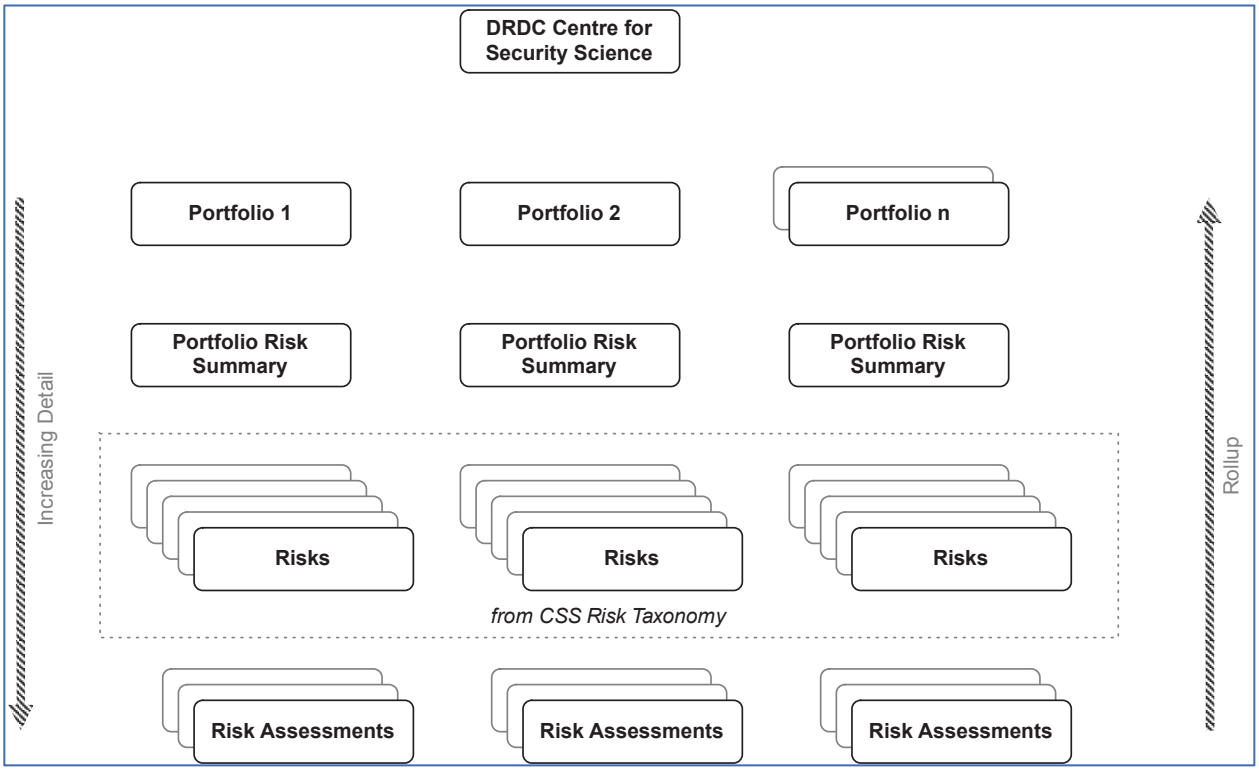

Figure 2 - Hierarchy of Portfolios, Projects, and Risks

A further Concept Model (Figure 3) was created that explained the linkages and relationships in a higher level of detail.

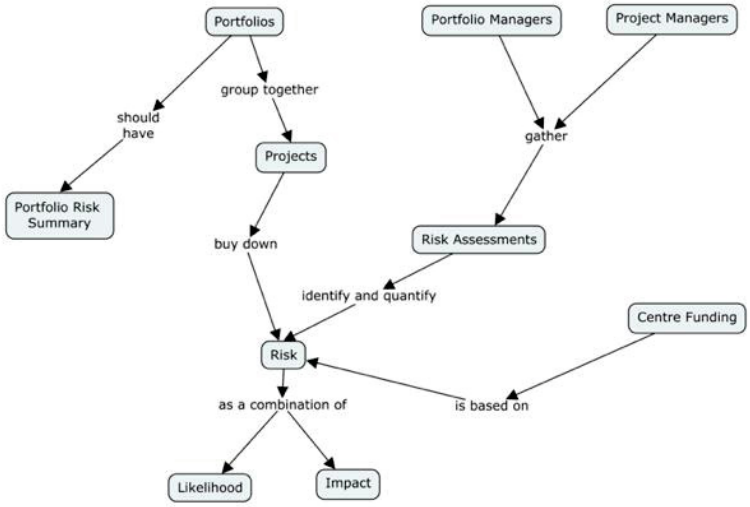

Figure 3 - Conceptual Data Model (Some Linkages Hidden for Clarity)

2.1.1 Logical Data Model

Following the Conceptual and Concept models a full data model was created.

Given the variability of the data sources and source-varied attribute schema a NoSQL database was created in MongoDB. The following diagram (Figure 4) displays the main data types.

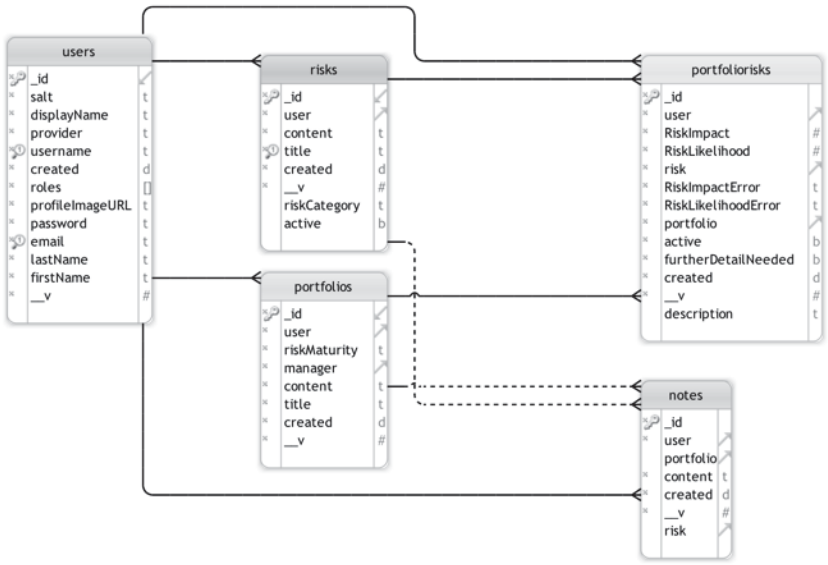

Figure 4 – Logical Data Model

The five main tables in the system are described below. For each table both key fields (some fields are ignored) and the linkages between tables are explained.

- **Users** – Users are discussed first as the simple role-based security system has impacts to the subsequent tables.
    - Fields:
        - *displayName* – this is the text that will be used for other users to see.
        - *username* – this is the username used to log in to the system
        - *password* – this holds an encrypted hash of the user's password (note: the "*salt*" attribute creates a unique hashing salt for each user)
        - *firstName* and *lastName* – the user's first and last name
        - *email* – the user's email address (NOTE: email is not hooked up to the prototype system so this value is not crucial).
        - *profileImageURL* – optionally allows a user to assign a photo to their account.
        - *roles* – Array of the roles that a user is a member of. Roles are discussed in more detail in User Roles (Section 3.2.4.3.1 on page 32).
    - Key Linkages:

        - Each table has a link back to the user that created or edited the item last. This applies to **Risks**, **Portfolios**, **Portfolio Risks**, and **Notes**.

- **Risks** – Risks are created at the system-level by a user with role of RiskAdministrator. These Risks can be applied to any Portfolio.
    - Key Fields:
        - *title* – the main Risk name as displayed throughout the system.
        - *content* – the HTML description of the Risk
        - *active* – true if this Risk is active, false if not. If the value is false, the Risk will not be available to be added to Portfolios but it will remain in Portfolios that used it before it became inactive.
        - *created* – the date that this Risk was created in the system.
        - *riskCategory* – the category of the risk – not currently used as this was an idea that didn't warrant completion.
    - Key Linkages:
        - **Risks** links principally to **Notes** and **PortfolioRisks**.

- **Portfolios** – holds Portfolio level information
    - Key Fields:
        - *manager* – links to the User that is the Portfolio Manager
        - *title* – the name of the Portfolio
        - *riskMaturity* – the Risk Maturity level of the Portfolio (see Section 4.1 for detail on Risk Maturity levels supported in the system).
        - *created* – the date that the Portfolio was created in the system.
        - *Content* – the HTML description of the Portfolio.
    - Key Linkages:
        - **Portfolios** link principally to **Notes** and **PortfolioRisks** tables.

- **PortfolioRisks** – this table serves to create a many-to-many linkage that provides a Portfolio-centric view of a Risk, with corresponding detail.
    - Fields:
        - *RiskImpact* & *RiskImpactError* – The estimated Impact of the Risk in the context of the Portfolio. Impact and the associated Error are described in further detail in Section 4.2
        - *RiskLikelihood* & *RiskLikelihoodError* – The estimate Likelihood of the Risk in the context of the Portfolio. Likelihood and the associated Error are described in further detail in Section 4.2
        - *risk* & *portfolio* – provide the foreign key link back to the **Risk** and **Portfolio** tables respectively.
        - *Description* – provides the HTML description of this Portfolio Risk.
        - *active & furtherDetailNeeded* – not used. These fields were being considered for future use.

- Key Linkages:
  - PortfolioRisks always link back to 1 Risk and 1 Portfolio.

- **Notes** – this table holds basic HTML for capturing Notes for both Portfolios and Risks
  - Key Fields:
    - *Content* – holds the HTML of the Note
    - *risk & portfolio* - provide the foreign key link back to the **Risk** and **Portfolio** tables respectively.
  - Key Linkages:
    - Notes are linked to Risks and Portfolios

2.2 Early Prototype

Once the data model and general API concept was understood effort began to create a prototype application.

The prototype efforts were started with a mocked-up user experience using Balsamiq to provide an early concept of how the application would look and feel.

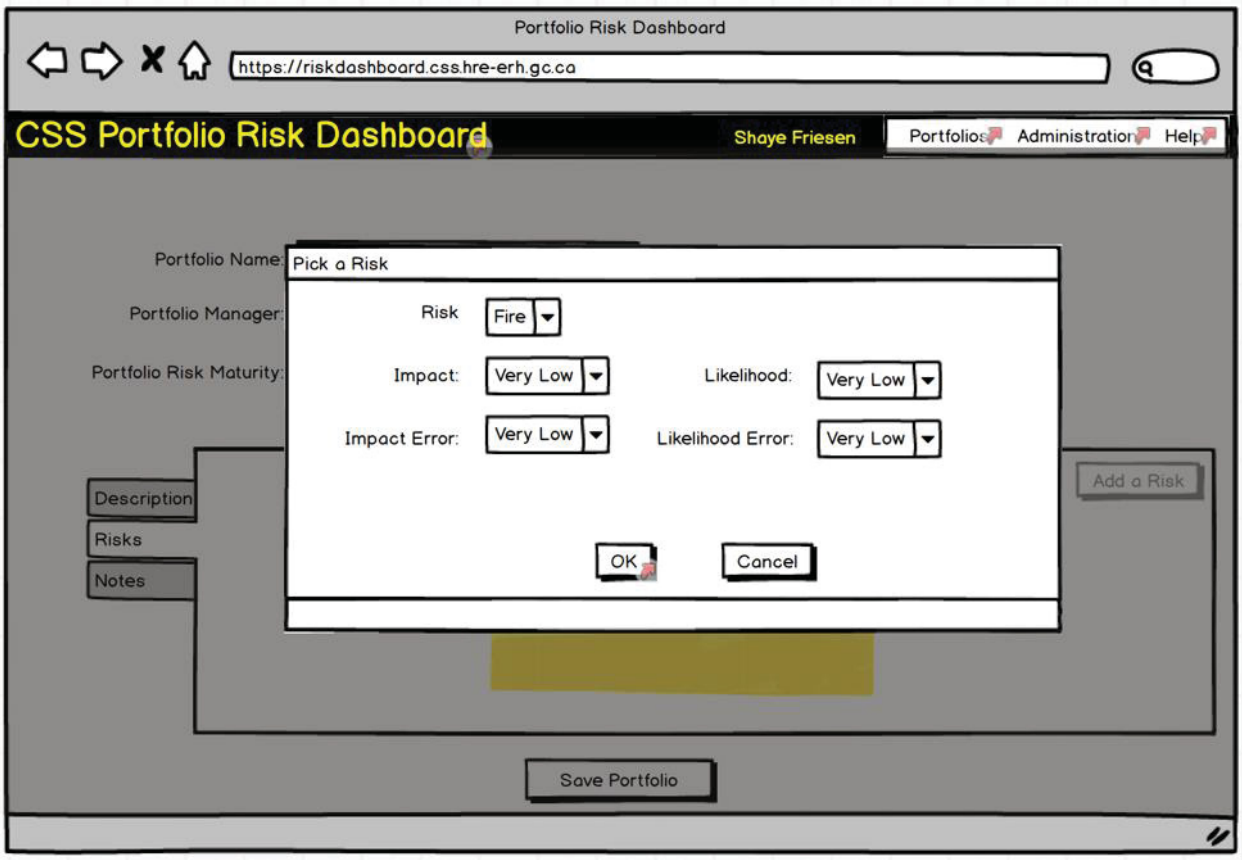

Figure 5 - Balsamiq Mockup Example

Figure 5 shows an example of a Balsamiq mockup from the earlier stages of development. Low fidelity semi-interactive mockups allowed for multiple rapid iterations of concepts while exploring how the Risk Dashboard could capture and display various information.

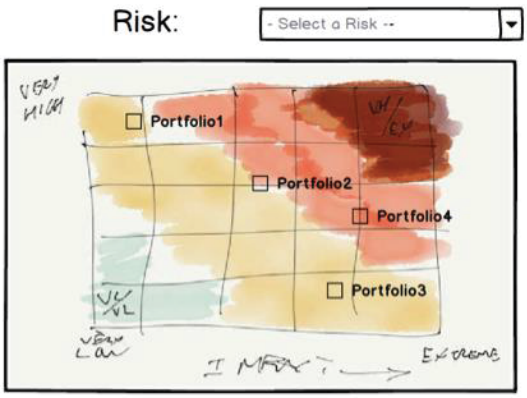

Figure 6 - Portfolio Risk Mockup

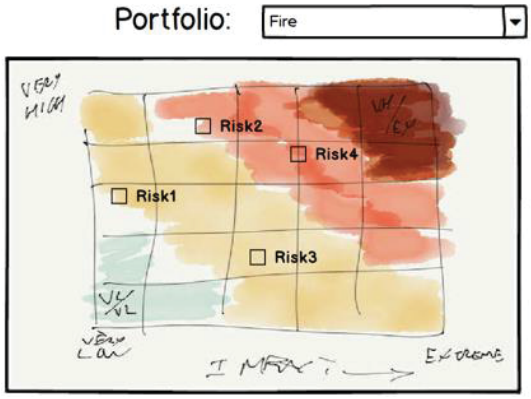

Figure 7 - Risk Portfolio Mockup

The two charts above show an early stage of the graphical concept that allow looking at Portfolios from a Risk perspective (Figure 6) or looking at Risks from a Portfolio perspective (Figure 7).

After an iteration of mockups development began. A web application was created using the MEAN.io (MongoDB, Express, AngularJS, Node.js) framework. The MEAN.io stack was used due to its widespread adoption in the web development community.

The goal of the application was intended to explore how Risk and Portfolio information could be managed by Portfolio Managers and Risk Analysts and then presented for senior leadership review.

Development efforts were focused on two main areas:

- Back-end API and Database – the server side routines, processing and API.
- User Experience – the visible portions of the system. UX efforts focused on data not cosmetics, though the use of Bootstrap themes and well-supported components provided a fairly consistent look & feel.

3 Risk Dashboard

The Risk Dashboard application is documented in this section. Features are discussed briefly and then they are presented with screenshots and basic instructions.

3.1 Features

The key features of the Risk Dashboard are:

- Management of Portfolios – Allowing Creation and Editing of a Portfolio for use.
- Management of Risks
    - Create/Edit Risk Detail – allows creation of a Risk and editing of it.
    - View Risk Information:
        - See the portfolios that have assigned this risk to it
        - Gather information (notes) about the risk
        - View a Chart that shows the Portfolios
- Portfolio Focus
    - Portfolio Listing – Lists all active Portfolios
    - Portfolio Editing
    - Portfolio Details – Portfolio Managers can assign risks to their portfolio, add Notes about various projects and studies that pertain to the portfolio and view the Risk Chart for the portfolio.
    - Visualization of Risks that pertain to a Portfolio
- Management of Users
    - Roles for Users:
        - Administrator
        - Portfolio Administrator – Manages the portfolio and projects and risks that are
        - Risk Administrator – Manages the List of Risks that the system support.

Each Feature listed above is described in Section 3.2 (User Interface) with screenshots and an explanation of how the page is used.

3.2 User Interface

The following sections explain the main application with screenshots and instructions.

3.2.1 Logging In & Landing Page

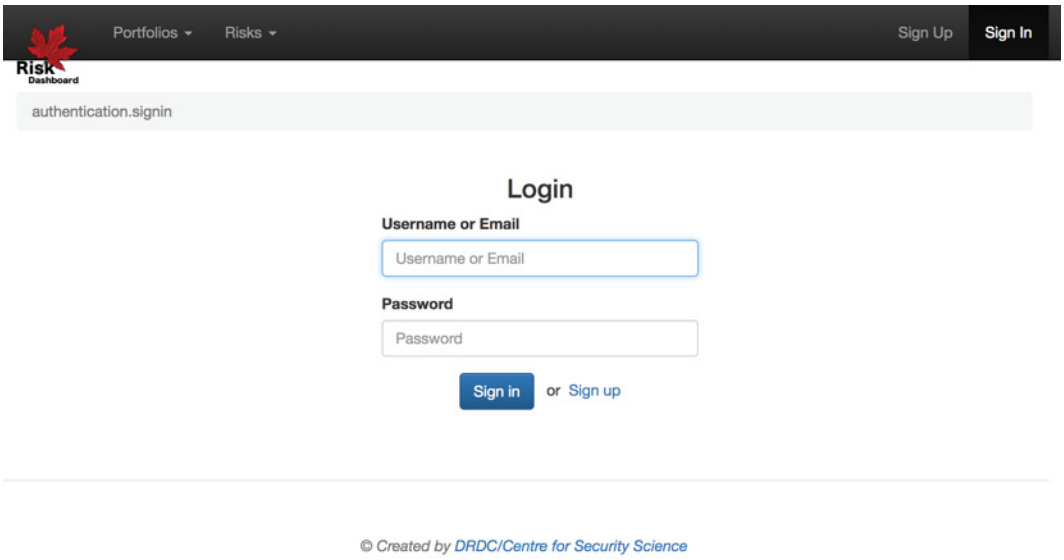

Figure 8 - Login Page

To log into the system you will need a system administrator to provide you with account credentials (username and password). These are entered on the Login page (Figure 8). You may also Sign Up for an account from this page but won't be able to access the system until your account is approved.

After logging in to the system, approved users will see a Landing Page (Figure 9) where they can access the main Portfolio and Risk pages.

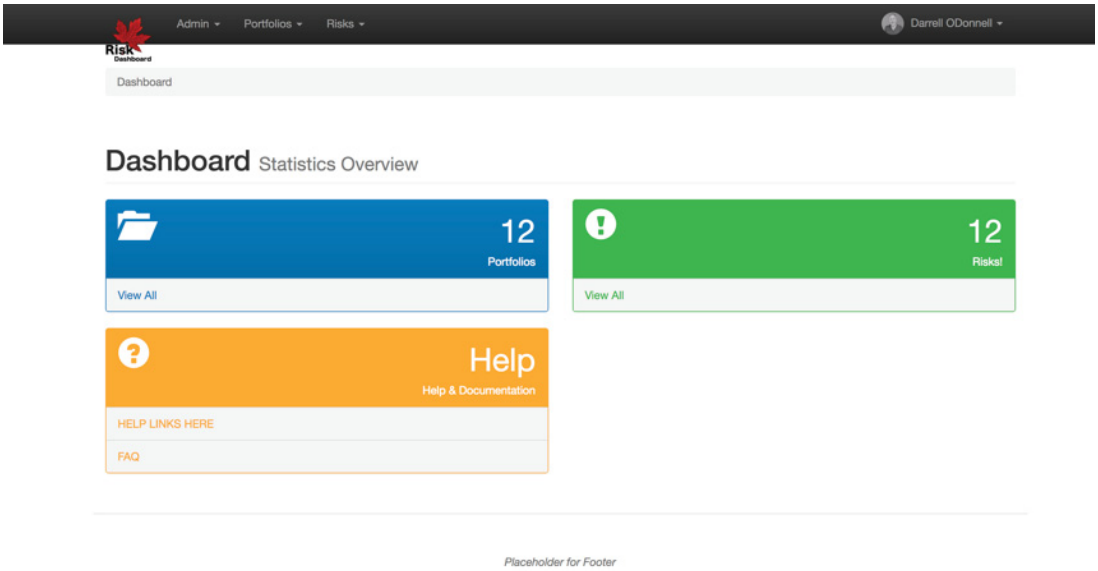

Figure 9 - Landing Page of the Risk Dashboard Application

There are two ways to approach the Risk Dashboard:

- Portfolio-Centric View - looking at a Portfolio and managing (adding and updating) the risks that apply to that portfolio. See Section 3.2.2 for full detail on using this view.
- Risk-Centric View – looking at a risk and viewing how portfolios are impacted by that risk. See Section 3.2.3 for full detail on using this view.

To access the Main User Pages, you have two main choices:

- Portfolio Centric View – click “View All” in the blue Portfolios section or use the Portfolios menu in the top bar and select *List Portfolios*.
- Risk-Centric View – Click “View All” in the green Risks section or use the *Portfolios* menu in the top bar and select *List Risks*.

The following pages are intended for the Portfolio and Project Managers that are managing the risk information for their portfolios.

3.2.2 Portfolio-Centric View

The most common use of the Risk Dashboard will be to examine and update Portfolios. Most Portfolio Managers will use this view of the system as they are primarily concerned about their own portfolio.

Accessing a List of Portfolios is done by clicking the Portfolios menu in the top toolbar and selecting *List Portfolios*, or from the main landing page. This action will bring up a list of the Portfolios that are active in the system (Figure 10).

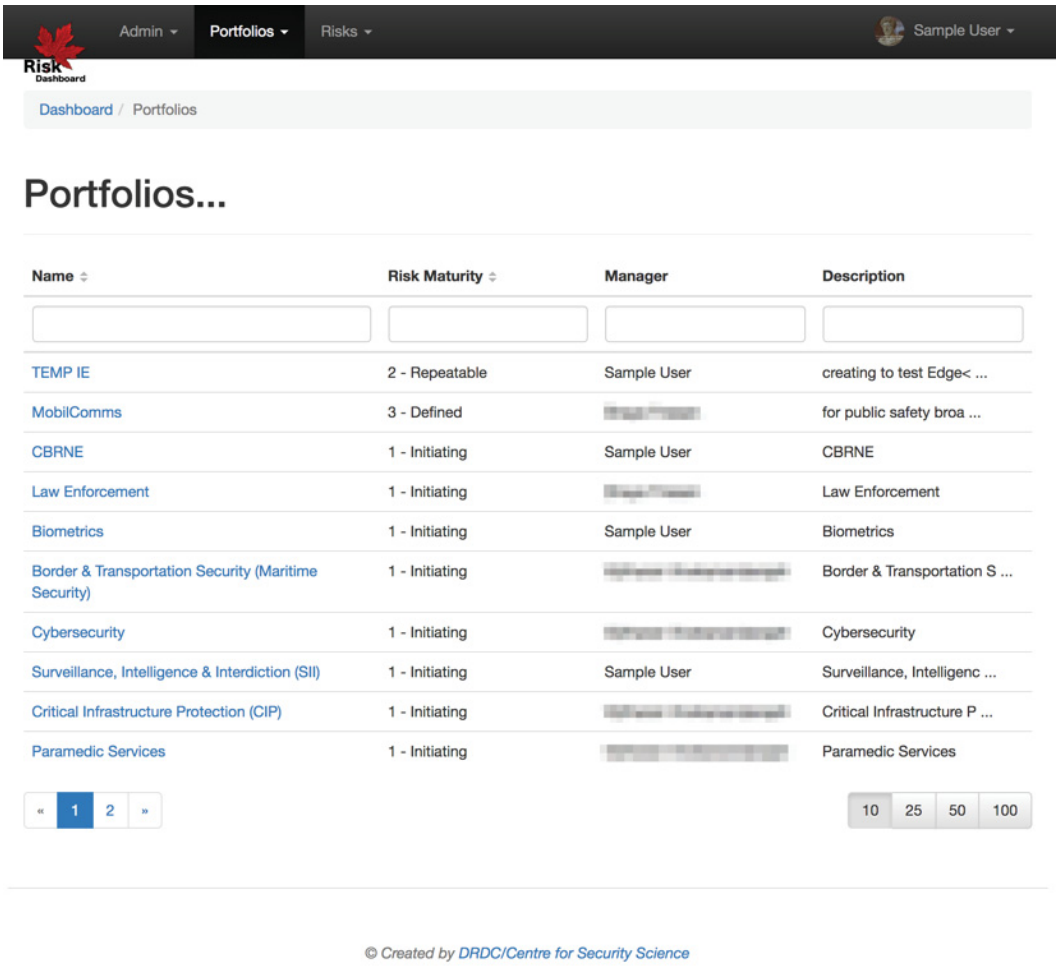

Figure 10 - Portfolio List

NOTE: Throughout this user guide some contents are blurred out to protect privacy as they reflect real accounts. See Figure 11 below for an example.

Figure 11 - Example Blurring for Privacy

3.2.2.1 Portfolio Detail

To access a portfolio, click the portfolio name. You may need to page through the results to find a portfolio. You can also type in the top of a column to search through by test (of portfolio

name, maturity, manager, or description). Once you do you will see a Portfolio Detail page (Figure 12 below).

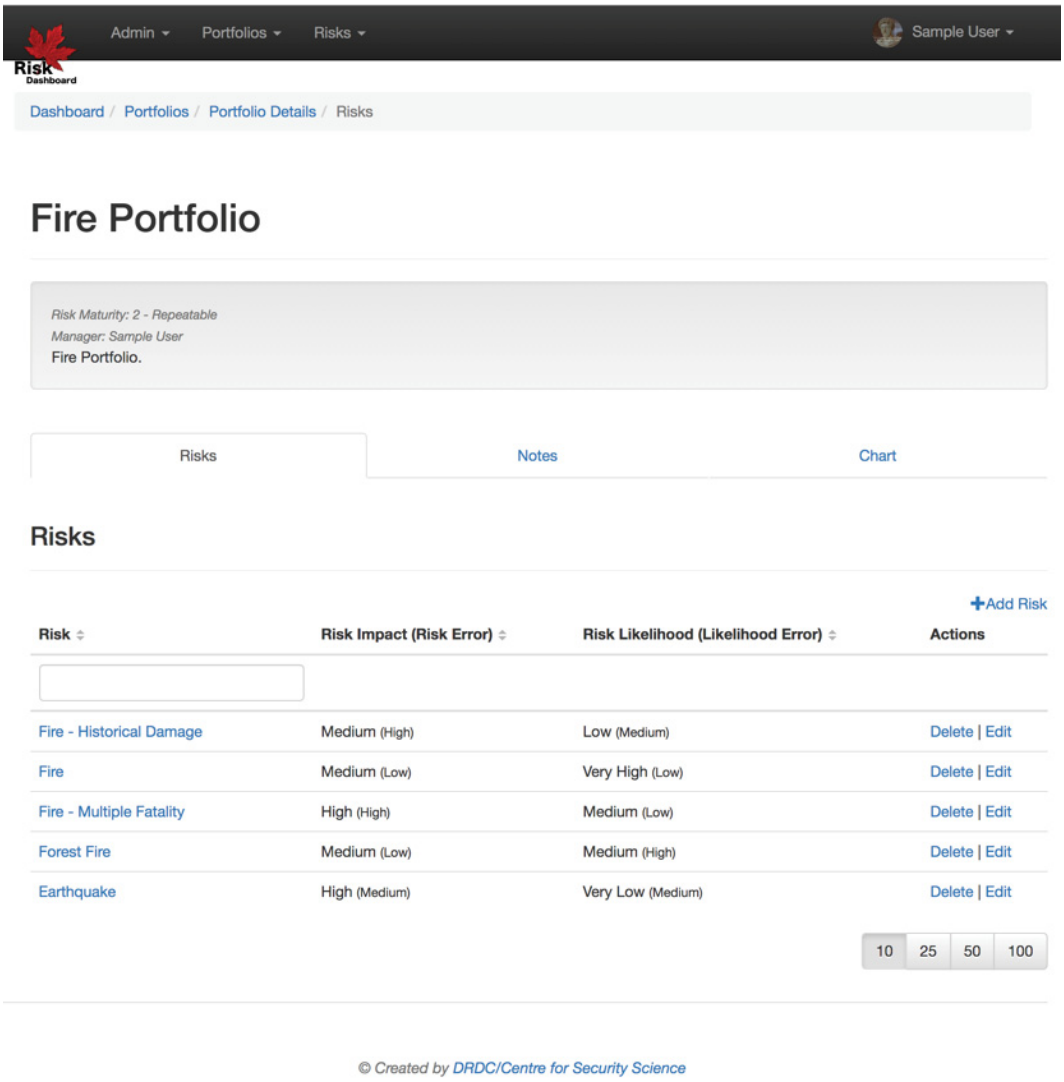

Figure 12 - Portfolio Detail

The Portfolio Detail page provides a brief description of the Portfolio and a list of the Risks that have been assigned to the Portfolio.

3.2.2.2 Adding a Risk

To add a Risk to a Portfolio, press the Add Risk link and a New Risk modal window will appear (see Figure 13 below).

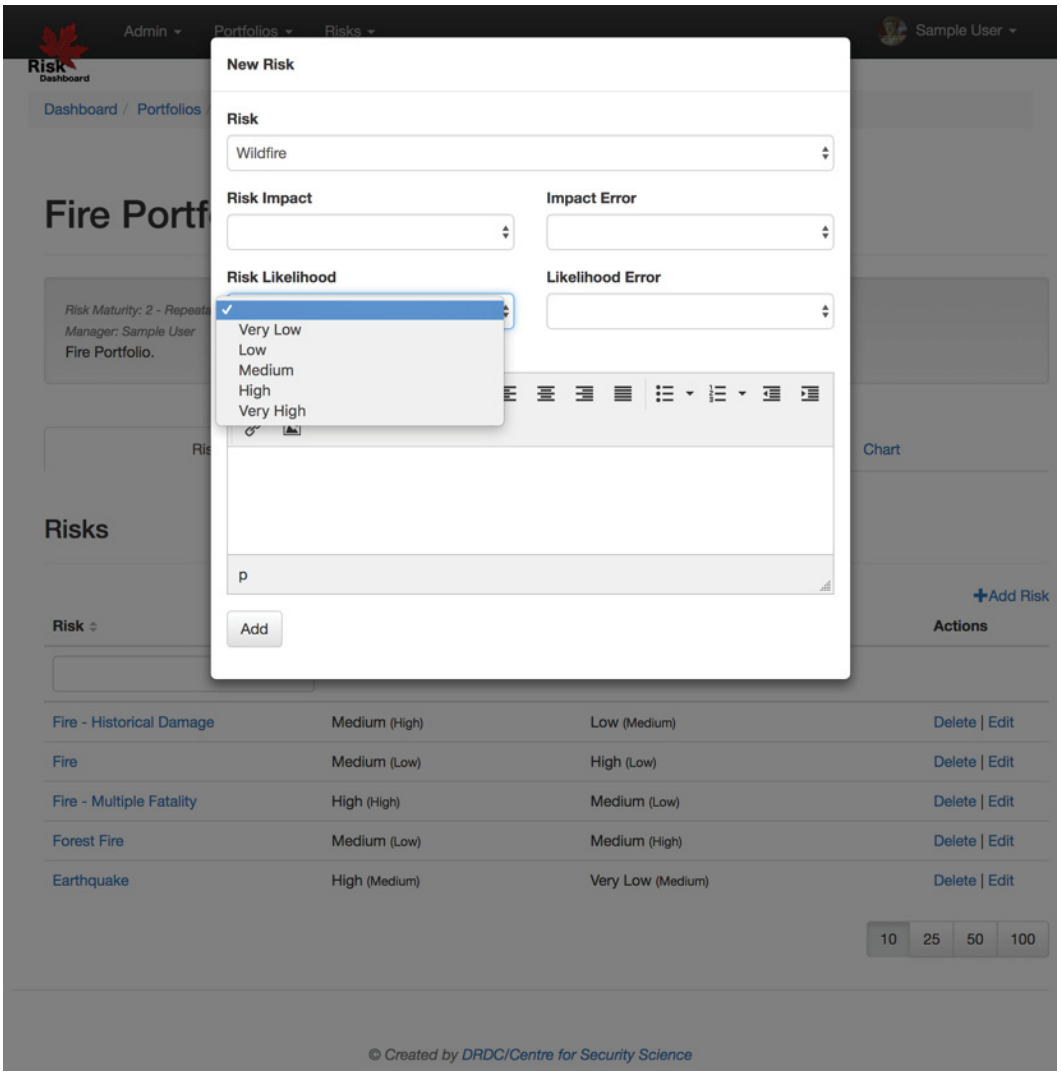

Figure 13 - Add a Risk to a Portfolio

Adding a Risk, as shown in Figure 13 requires multiple steps:

- Select a Risk from the Risk drop down list. Only Risks that are not already part of the Portfolio will appear here.
- Select the Risk Impact and Impact Error.
- Select the Risk Likelihood and Likelihood Error.
- Optionally add some text in the Description area to explain how the Risk applies to the Portfolio, listing any key inputs (e.g. Risk Assessments, reports) that may be relevant.

Once a Risk has been assigned to a Portfolio it can be:

- Viewed – the Impact and Likelihood values and their associated errors are displayed in the table.
- Edited – by clicking the Edit link on the right side of the table for that Risk you will be brought to the Portfolio Risk Edit page (Figure 14 below).

3.2.2.3 Editing a Risk in a Portfolio

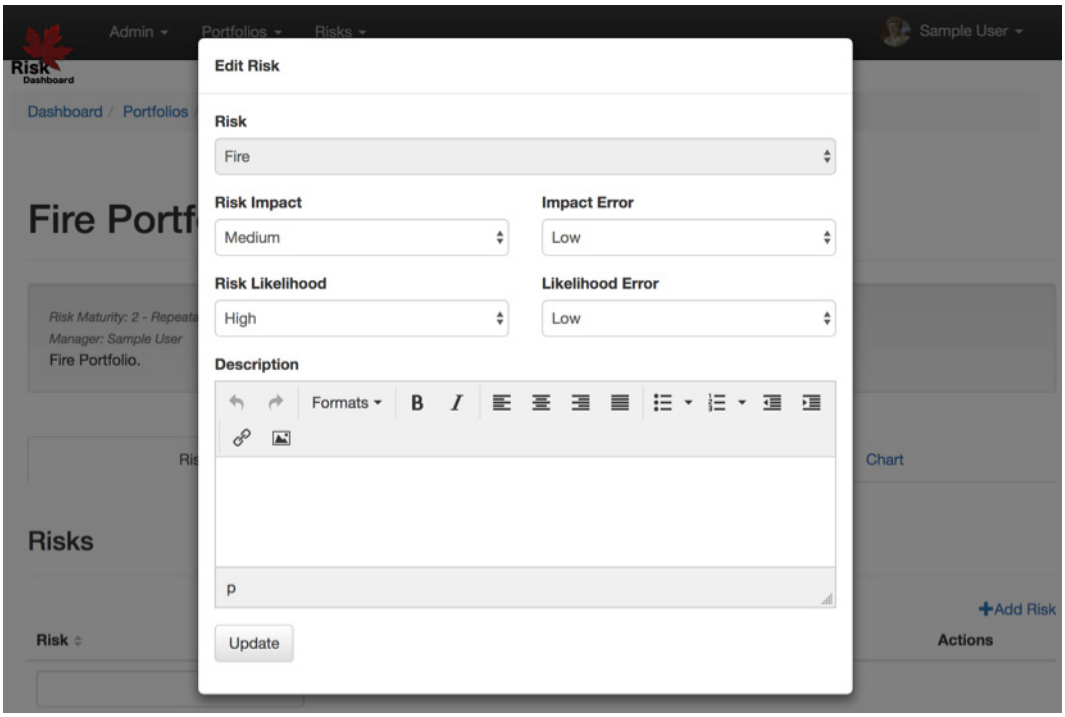

Figure 14 - Edit a Risk in a Portfolio

Figure 15 shows the Portfolio Notes page where notes can be added (press Add Note link) and viewed/edited.

Notes are intended for capture of very basic information about a Portfolio.

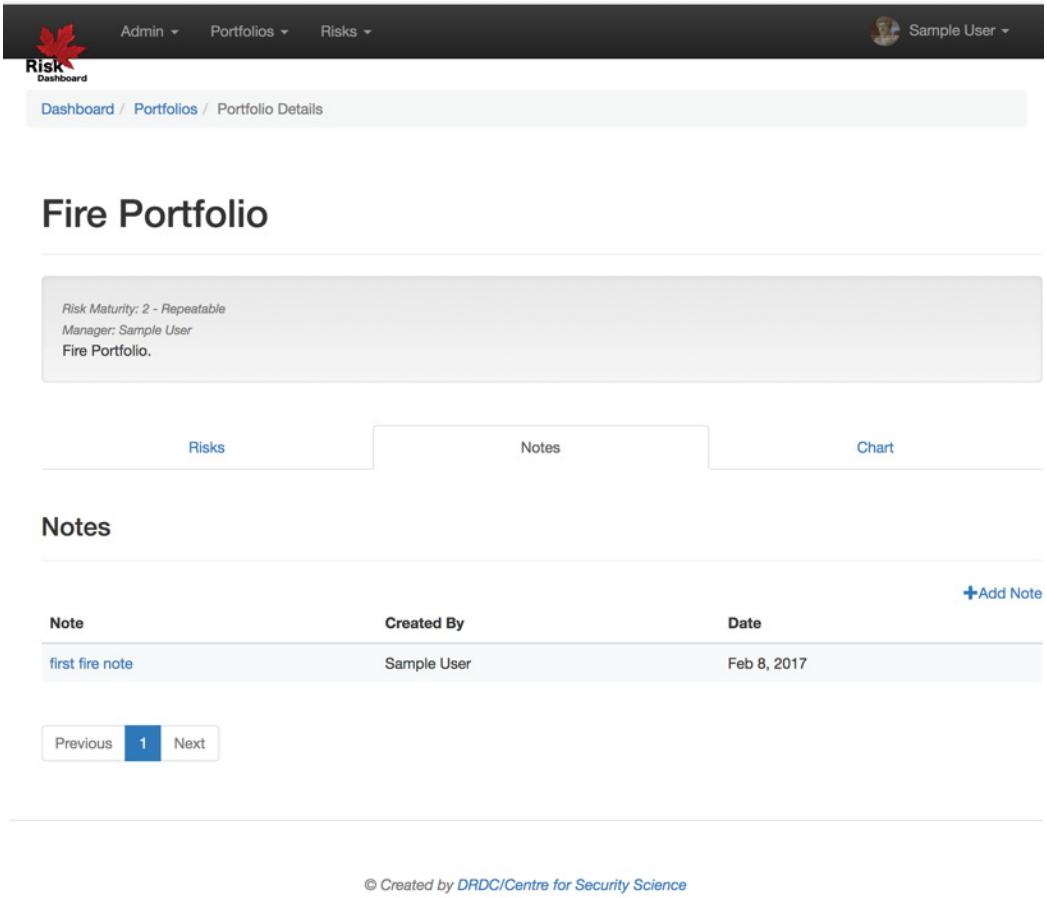

Figure 15 - Portfolio Notes

3.2.2.4 Notes – Adding and Editing

Editing (click the note link in the table) or Adding a Note (click the *Add Note* link) will display the Add/Edit Note modal window (see Figure 16 for example). If a Note is new, there will be a Create button at the bottom. If a Note is being edited an Update button (shown in Figure 16 below) will be displayed.

Basic formatting can be applied to a note including text formatting (bold and italic), alignment, indenting, lists (basic bullets, numbered), and hyperlinks can be added.

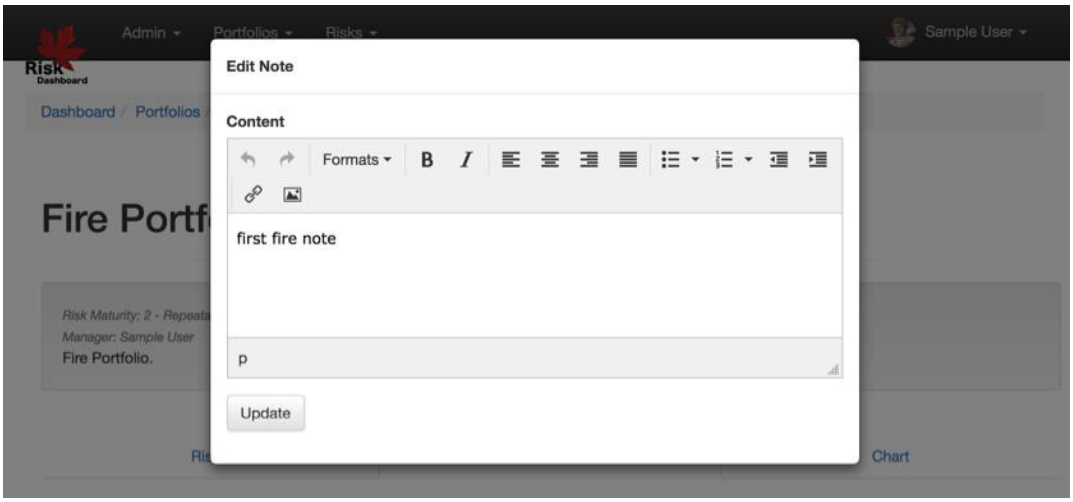

Figure 16 - Portfolio Edit/Add Note

3.2.2.5 Portfolio Risk Chart

Once a Portfolio has at least one Risk assigned to it the Risk Chart will be available and present a pictorial view of the Risks that apply to the portfolio in terms of the Likelihood and Impact values and the errors associate with them.

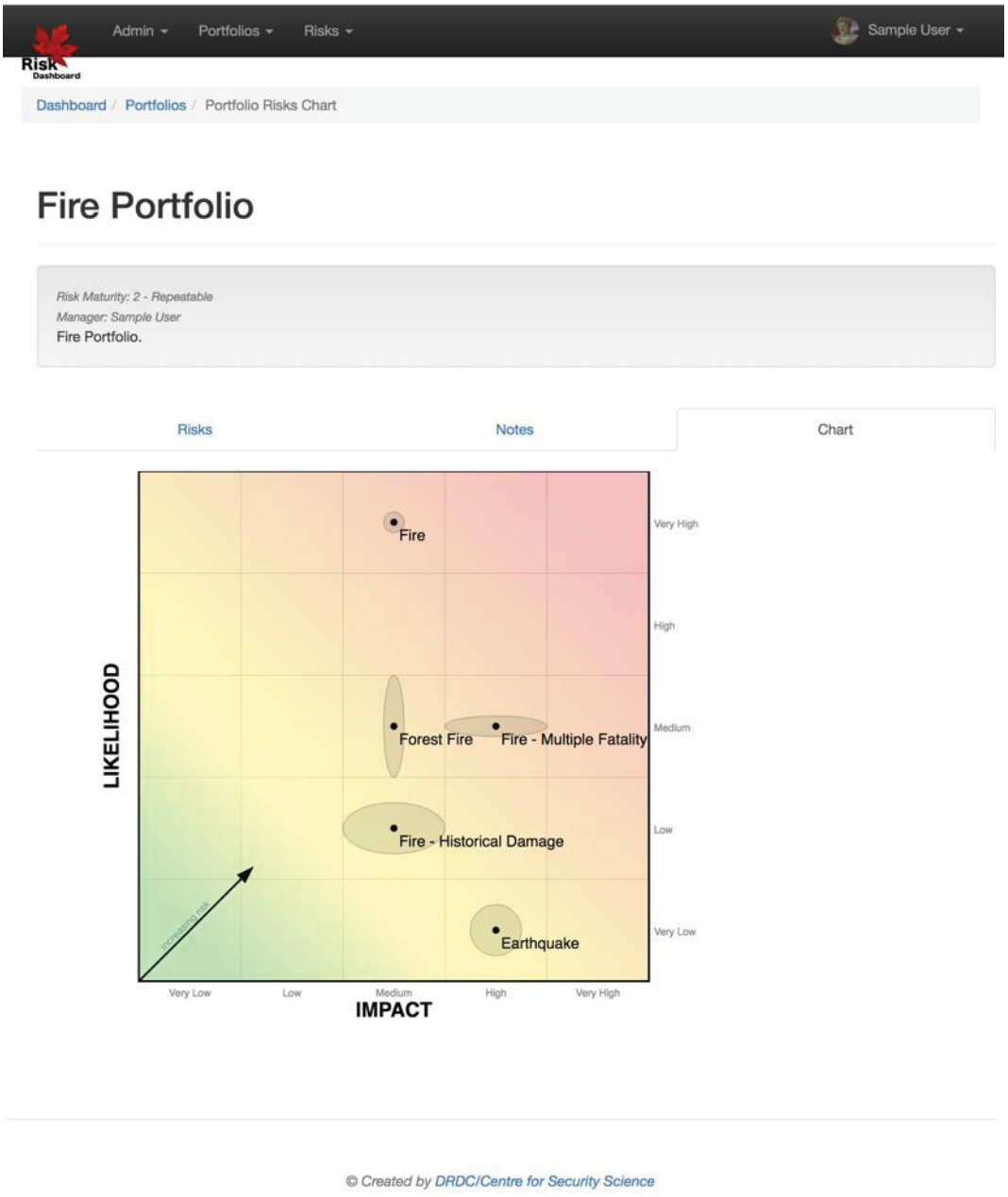

Figure 17 - Portfolio Graphical View

Figure 17 is a sample output of a Portfolio Risk chart. It visually displays multiple risks as they apply to a Portfolio. In this example, the Risk values are as listed in Figure 12. Error ellipses are used to indicate the amount of error in each dimension. Impact Error is shown horizontally and Likelihood Error vertically. The size of the error results in smaller (lower error) or larger (higher error) axes for the error ellipse).

3.2.3 Risk-centric View

Many risks are cross-cutting – they apply to multiple portfolios in the Centre. Looking across CSS there is a need to assess how CSSP leadership understands how a Risk is being handled by various Portfolios.

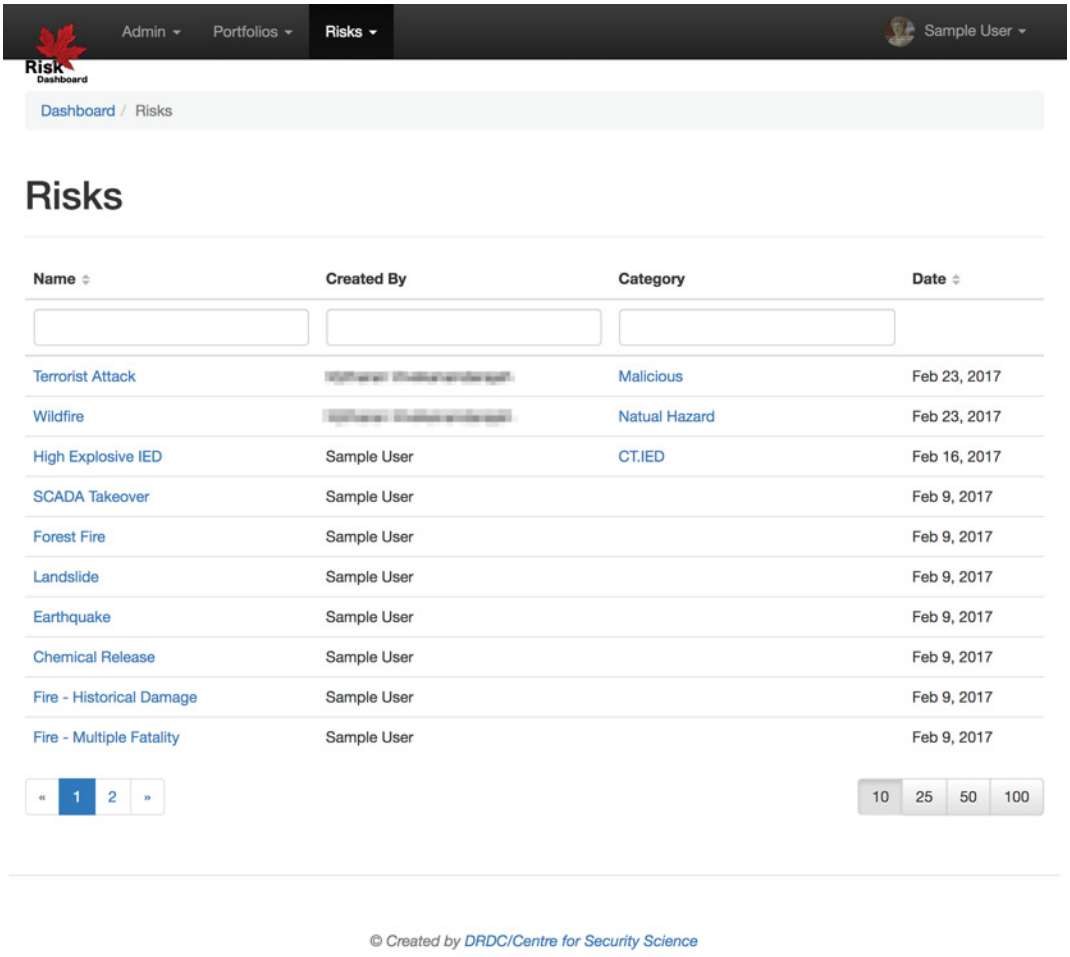

Figure 18 - List of Risks

Clicking a Risk in the list (Figure 18) will present the Risk Details Page.

3.2.3.1 Risk Details

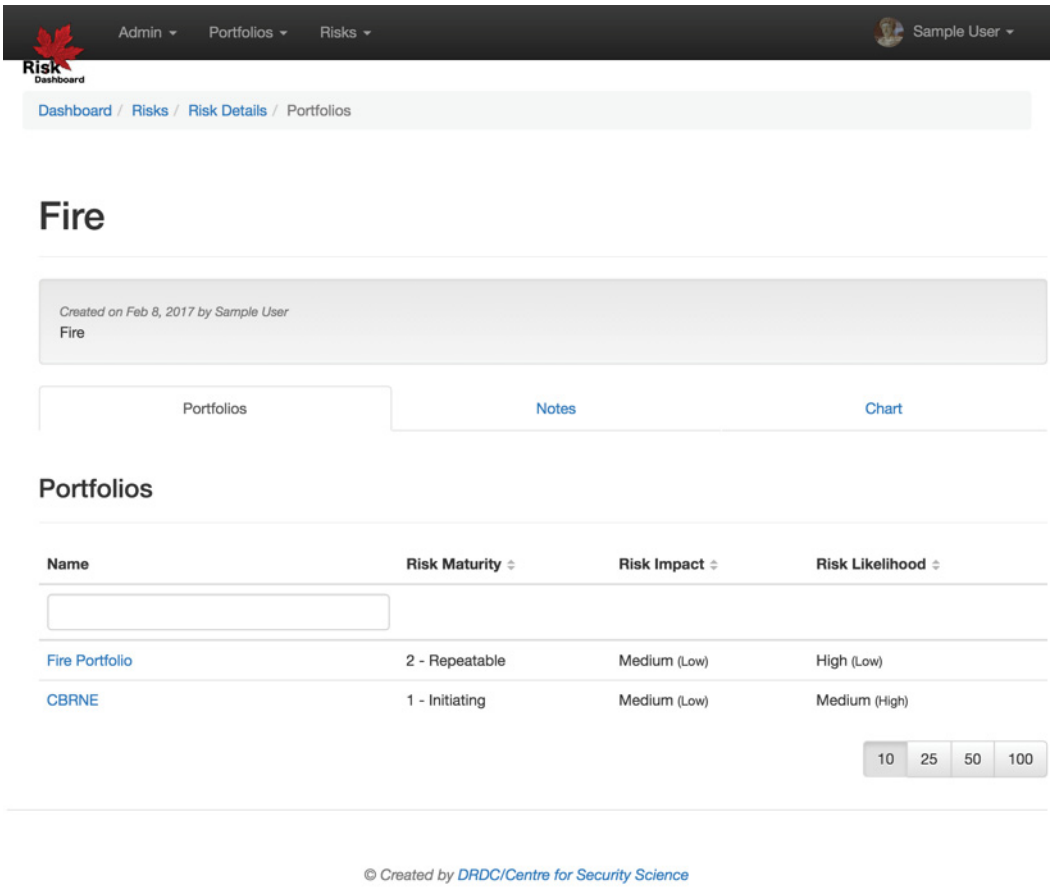

Figure 19 - Risk Detail

The main difference in the user interface for Risks is that one does not add a Risk to a Portfolio from here. Users can see (Figure 19) the Portfolios that have added this Risk but cannot add one here.

3.2.3.2 Risk Notes

Clicking the Notes tab will display a list of the Notes that have been assigned to this Risk (Figure 20).

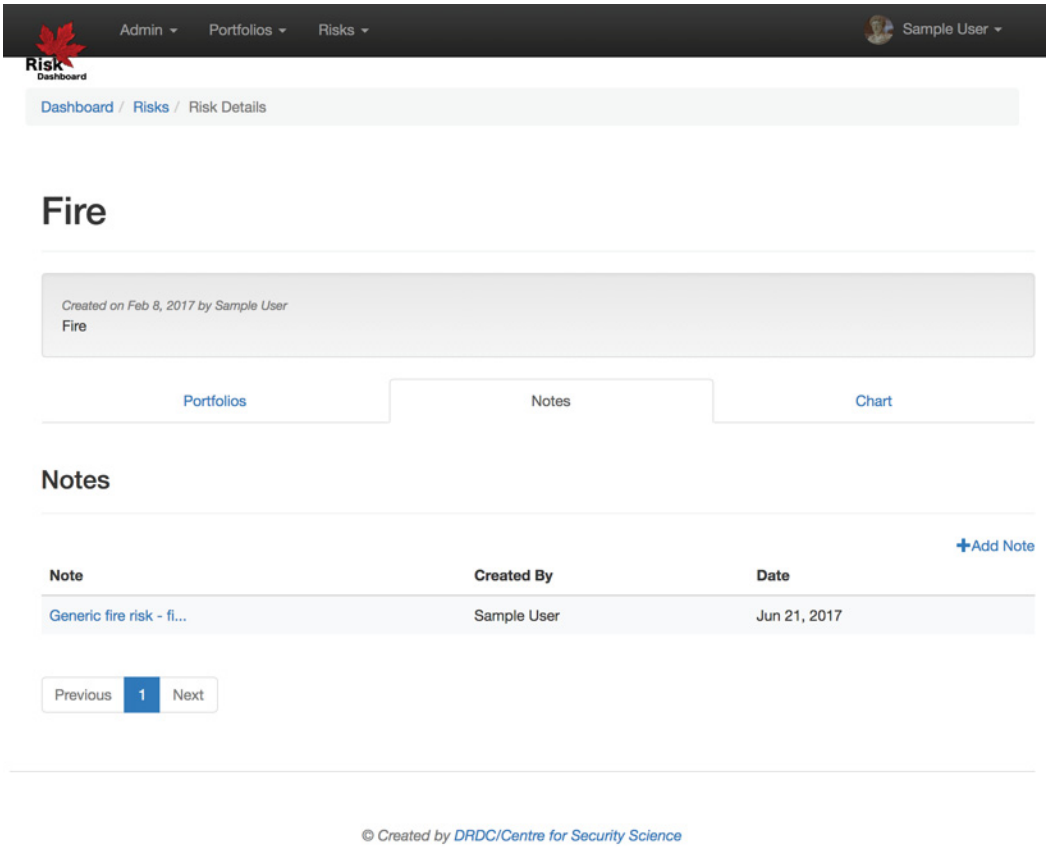

Figure 20 - Risk Notes

Notes for Risks are intended to allow gathering of cross-cutting Risk information for the Centre. If there are details about a Risk that may be relevant. Editing and Adding Notes for a Risk are done as described in Section 3.2.2.4 on page 20.

3.2.3.3 Risk Portfolio Chart

Clicking the Chart tab for a Risk will display a chart of all the Portfolios that have provided Likelihood and Impact values for this Risk (Figure 21).

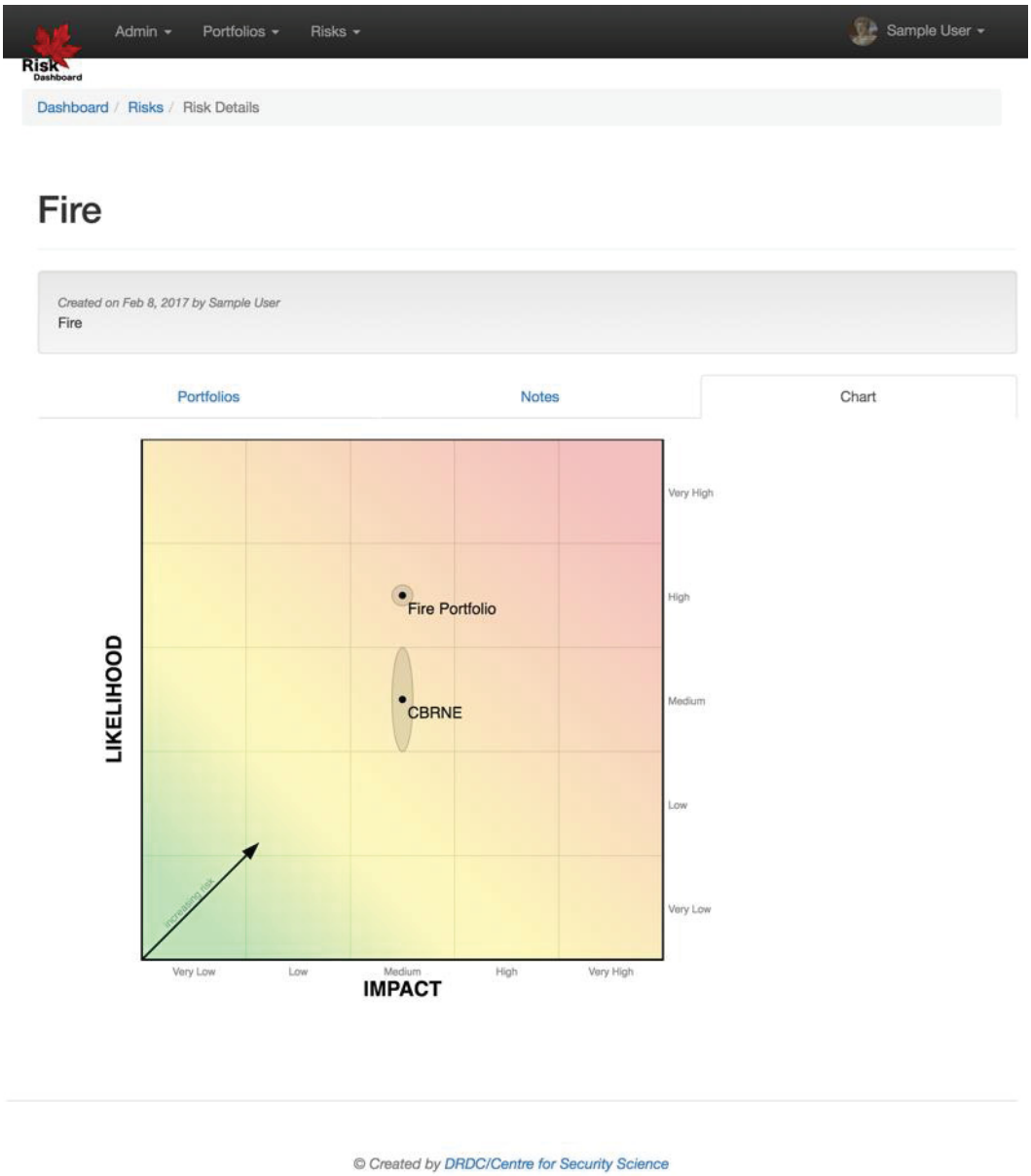

Figure 21 - Risk Portfolio Chart

Figure 21 is a sample output of a Risk Portfolio chart. It visually displays multiple Portfolios as they apply to a Risk. In this example, the Portfolio values are as listed in Figure 19. Error ellipses are used to indicate the amount of error in each dimension. Impact Error is shown horizontally and Likelihood Error vertically. The size of the error results in smaller (lower error) or larger (higher error) axes for the error ellipse).

3.2.4 Administration Pages

The following pages are primarily intended for the administrators of the Risk Dashboard. The main functionality is to manage Portfolios, Risks, and Users for the system.

3.2.4.1 Portfolio Administration

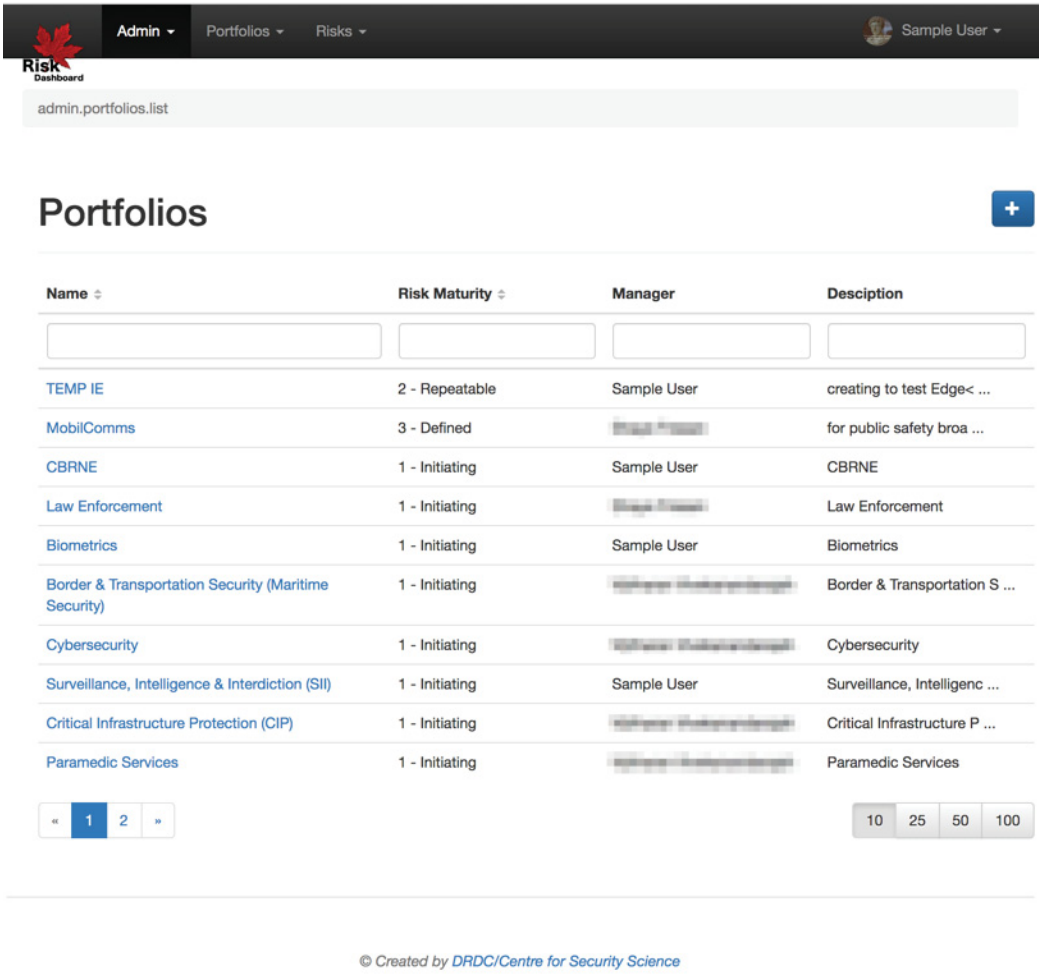

Figure 22 - List Portfolios for Administration

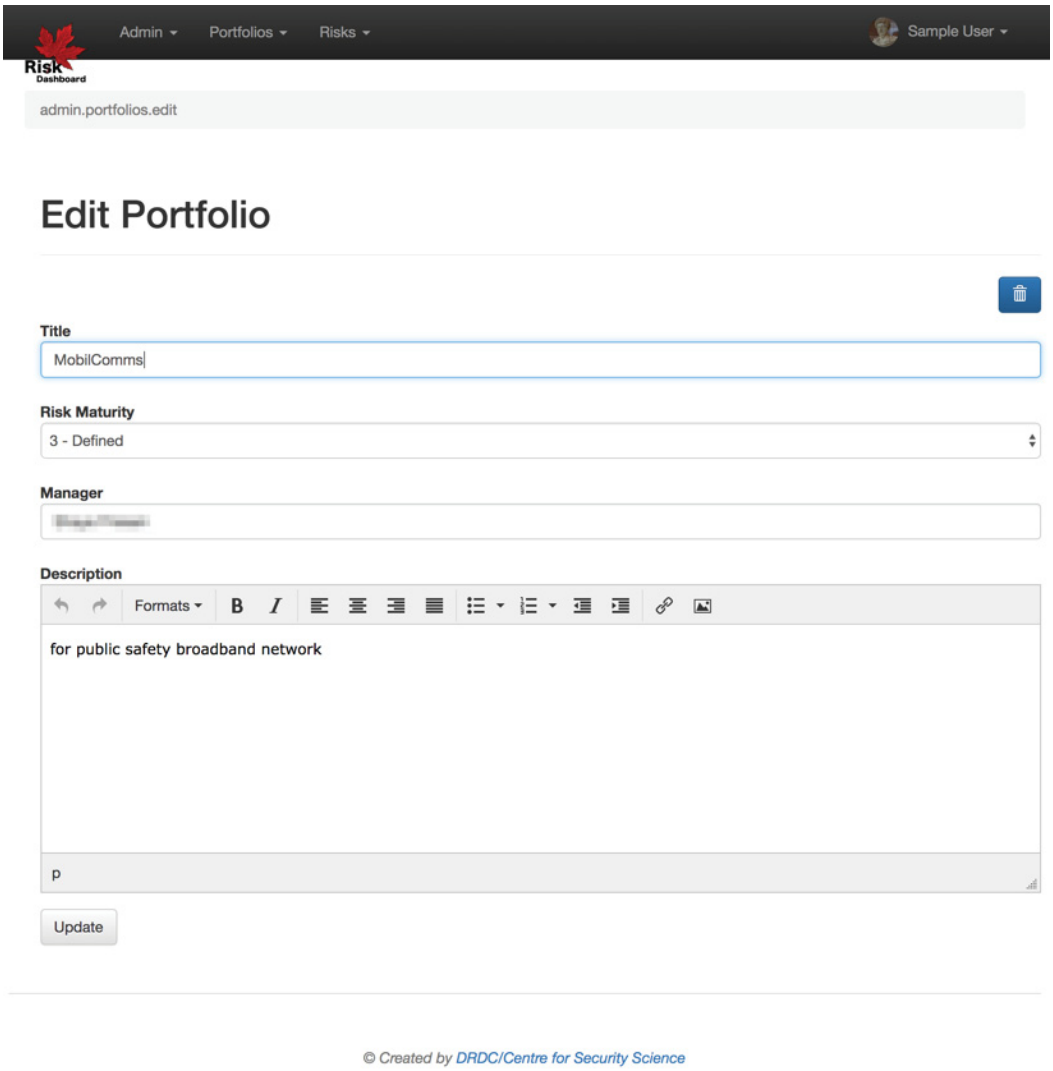

Figure 23 - Edit/Create Portfolio Page

To Create or Edit a Portfolio provide the following inputs:

- Give the Portfolio a Title.
- Set the Risk Maturity level for the Portfolio. The values range from Very Low to Very High. Section 4.1 of this document provides a reference for the values (page 33).
- Assign a Manager (note: only users that are in the role of PortfolioAdmin will show in this drop-down list).
- Add a Description if desired.

3.2.4.2 Risk Administration

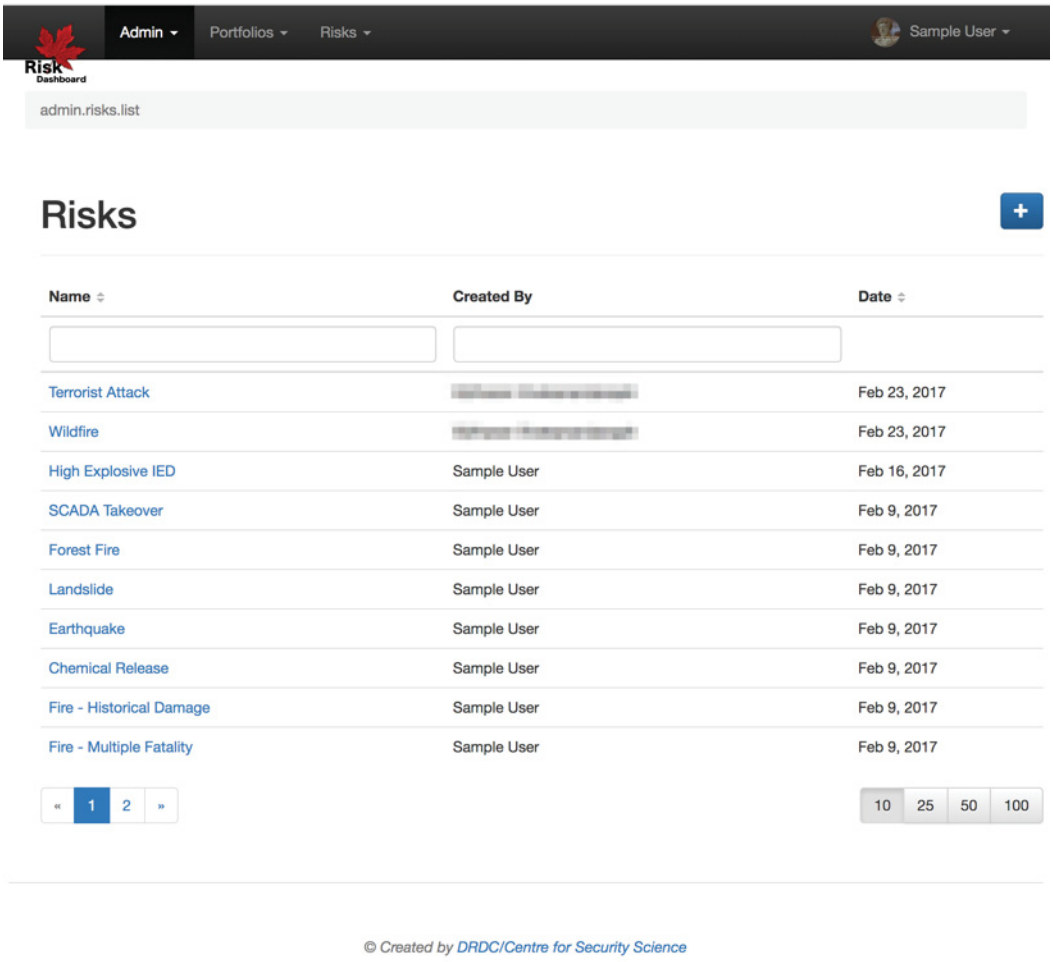

Figure 24 - List Risks for Administration

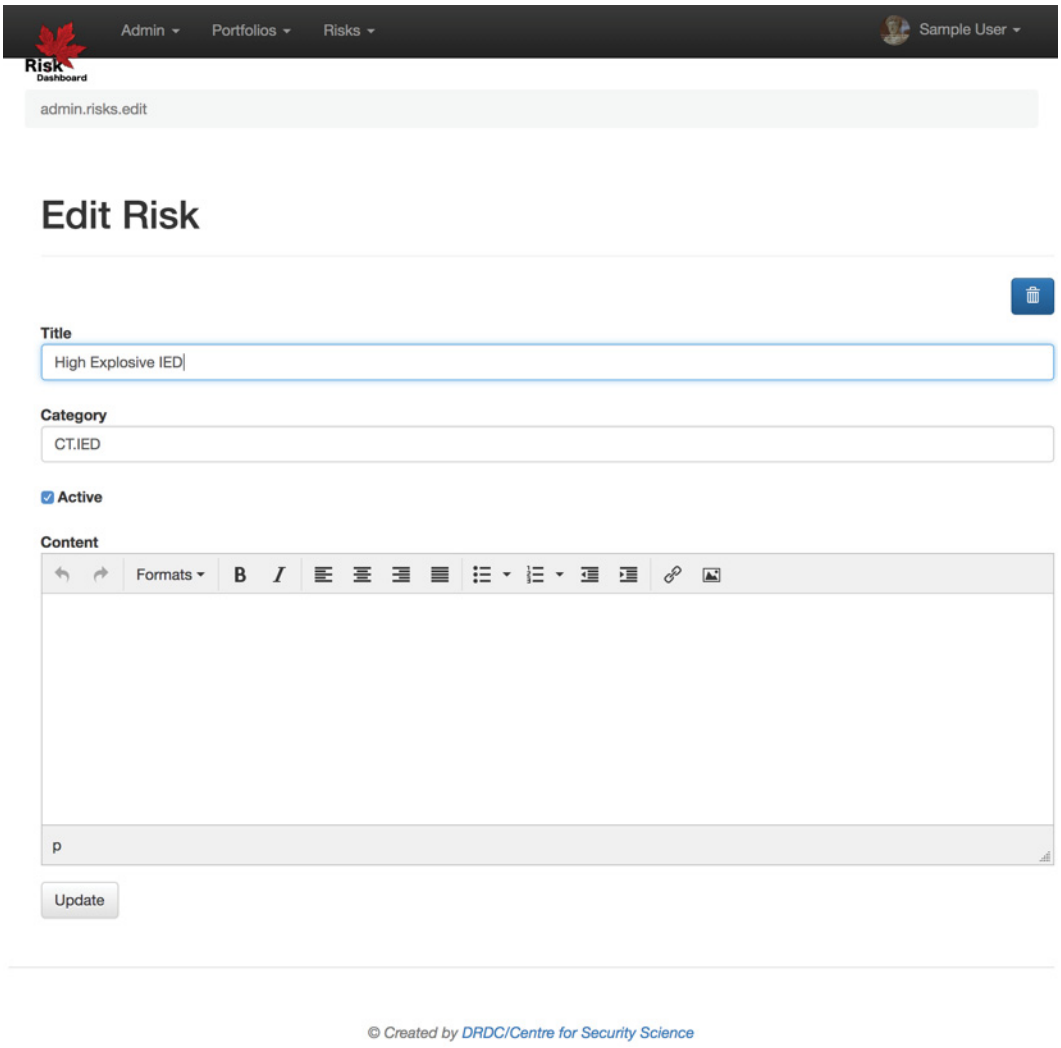

Figure 25 - Edit/Create Risk Page

3.2.4.3 User Administration

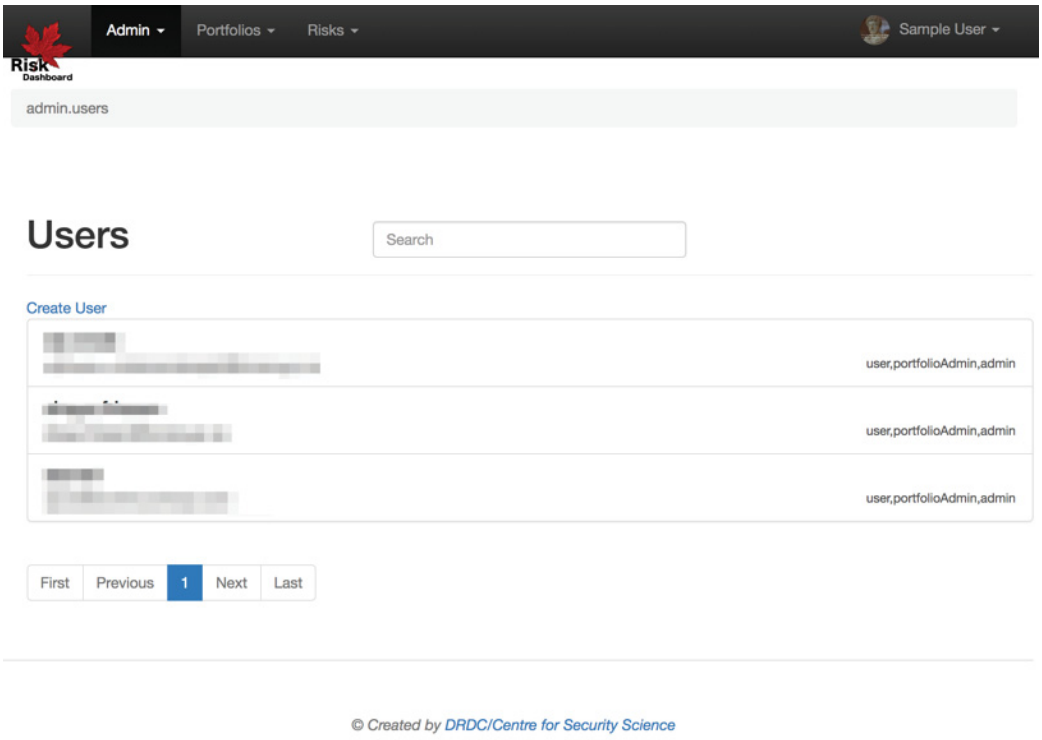

Figure 26 - List Users

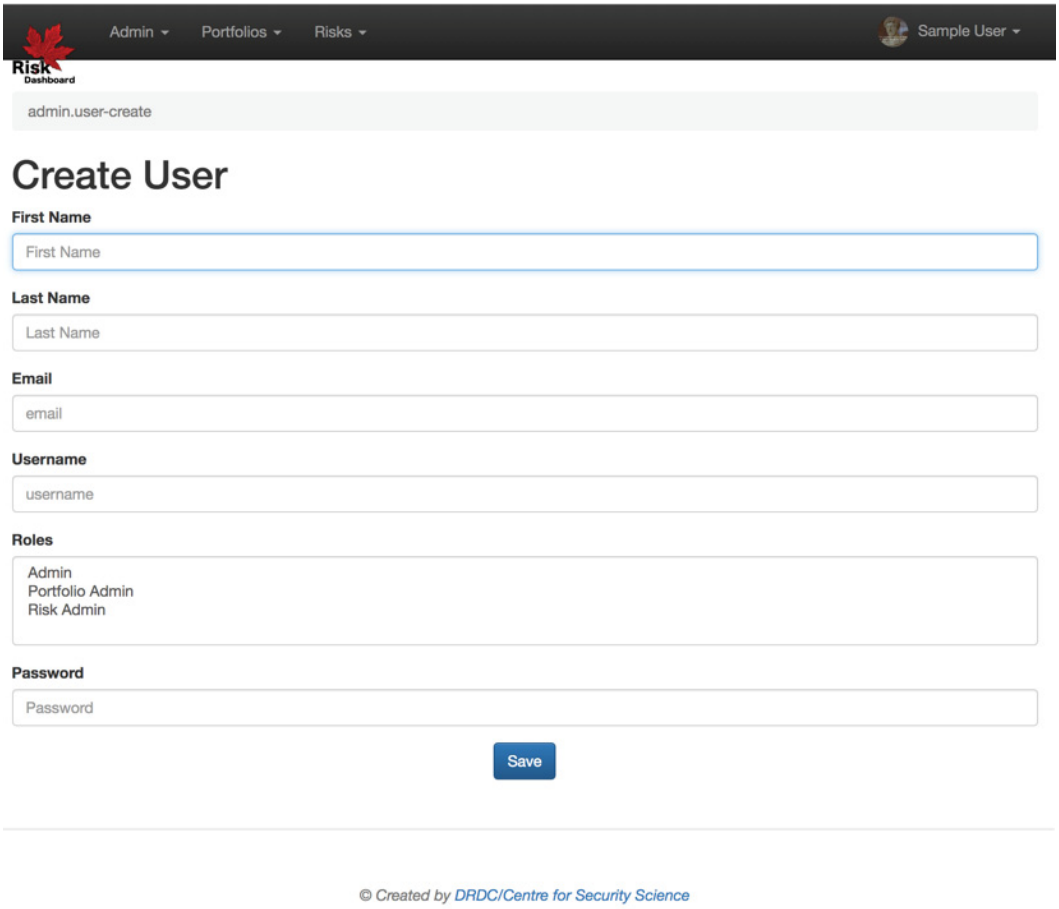

Figure 27 - Create User Page

3.2.4.3.1 User Roles

The Risk Dashboard has 3 main user types:

- Administrator – full system administrator that is able to create new Users.

4 Definitions & Concepts

The following section outlines some of the key concepts

4.1 Risk Maturity

The Risk Dashboard uses a concept of Risk Maturity Model to apply a metric at a Portfolio level. This metric, the Portfolio's Risk Maturity is intended to capture how the Portfolio uses Risk.

The following levels are based loosely on the Capability Maturity Model for Software (Paulk 1993), and has been adapted for Risk and the Risk Dashboard:

- **Initial (Level 1)** – Risk is being applied in an undocumented and ad hoc manner.
- **Repeatable (Level 2)** – Risk approaches have been used and some risk-based processes are repeatable, possibly with consistent results. However, process discipline is not likely to be rigorous.
- **Defined (Level 3)** – Risk plays a role in a defined and documented standard process for the Portfolio.
- **Managed (Level 4)** – Risk processes are used with concrete metrics throughout the Portfolio. Risk is used as a deciding factor in how the Portfolio operates.
- **Optimizing (Level 5)** – Risk is being examined throughout the Portfolio and being applied to optimize investment results to buy down risk or to mitigate its consequence.

4.2 Likelihood and Impact

Likelihood: The chance of an event or an incident happening, whether defined, measured or determined objectively or subjectively.

Impact: The extent to which a risk, should it occur, influences population, economy, environment, government structure or functioning, or the society as a whole. The impact per occurrence may be assessed quantitatively (quantitative units are flexible; they include monetary units, time units, number of fatalities, number of casualties, etc.) or, in more complex cases, qualitatively (in qualitative units such as None, Low, Medium and High).

Likelihood and Impact Values - The Risk Dashboard uses values of Very Low, Low, Moderate, High, and Very High for both Likelihood, Impact, and the associated errors.

Figure 28 presents the preliminary definitions for impacts, likelihood and error levels that are used for each rating in the tool. [3] Note, the ratings are preliminary and can be adjusted/modified to reflect the evolution of the risk dashboard and requirements of end users.

[3] The definitions were drawn from a number of sources: the CSEC/RCMP Harmonized Threat/Risk Assessment; the federal AHRA; and the U.S. Army Field Manual Risk Management (FM100-4).

Value	Impact	Likelihood	Error
Very Low	Negligible Negligible < $1 thousand	1,000-10,000 Days. Occurs very rarely (almost never or highly improbable).	Small to insignificant body of knowledge on the issue, quantity and quality of relevant data and/or inconsistent relevant assessments
Low	Discomfort Minor Embarrassment > $1 thousand	100-1,000 Days. Occurs rarely, often as an isolated incident(s).	Relatively small body of knowledge on the issue, the relatively small quantity and quality of relevant data and somewhat consistent relevant assessments.
Moderate	Injury/Illness Public Suspicion/Doubts > $100 thousand	10-100 Days. Occurs sporadically (irregularly, sparsely, or sometimes).	Considerable body of knowledge on the issue, the considerable quantity and quality of relevant data and consistent relevant assessments.
High	Potential Loss of Life Serious Stress/Trauma > $10 million	1-10 Days. Occurs at a high rate, but intermittently (regular intervals, generally often).	Large body of knowledge on the issue, the large quantity and quality of the relevant data and very consistent relevant assessments.
Very High	Widespread Loss of Life Widespread Trauma > $1 billion	Daily. Occurs continuously during an event, mission or operation.	Thorough knowledge of the issue, the very large quantity and quality of the relevant data and totally consistent assessments.

Figure 28 - Likelihood and Impact Value Definitions

5 Conclusions and Recommendations

The CSSP Risk Dashboard provides an interface through which risk analysts / Portfolio managers can track and monitor their risks, and link investment decisions to the outputs of the risk priorities. As the population of the Risk Dashboard commences, the information on risks across the Centre can be collated into single location, to allow for comparison at the Portfolio level. The aggregation of information allows stakeholders to visualize which public safety and security risks are most pressing to organization.

The Risk Dashboard serves as a mechanism that links risks in the public safety and security environment to Portfolio management, and contributes to optimizing distribution of investment decisions. The CSSP has created a systematic process for Portfolio review, analysis, prioritization, tracking, sharing and reporting of risks, moving beyond Enterprise Risk Management, program audit and compliance assessment. In doing so, the Risk Dashboard provides another tool that supports traceable, defendable and well-documented S&T program priorities.

The following recommendations resulted from this project:

- DRDC CSS should consider using the Risk Dashboard to provide visibility into the application of Risk principles to portfolio management.
- Database population: there is a need to ensure the data is reliable (i.e., avoid “garbage-in” and “garbage out”). DRDC CSS should consider taking at least 1 or 2 Portfolio Managers through the exercise of fully filling out and populating the application.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

A Prototype Software Application for Risk Data Analytics within the Canadian Safety and Security Program

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

O'Donnell, D

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
September 2017	35	0

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
	W7714-135734

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2017-C210	

11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

12. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Under a Canadian Safety and Security Program (CSSP) targeted investigation (TI) project (CSSP- 2015-TI-2130), the Defence Research and Development Canada (DRDC) Centre for Security Science (CSS) began development of a prototype web application to assist in managing risk-related information in its portfolios. This report summarizes the development efforts and the prototype application that was created.

The application provides methods for Portfolio Managers and Risk Analysts to gather basic risk-related information. It provides visualization tools that allow CSS leadership to see where risk measures are being applied in portfolios.

13. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Risk; risk assessment; prototype; software development; app