strategies for complex organizations

Risk Management Program Manual

DATE: 2017

Prepared For: BVES Users

BEAR VALLEY ELECTRIC SERVICE

Risk Management Program
Table of Contents

Table of Figures

Table of Tables

Revisions Log

Section	Date	Change Overview	Name

Executive Summary

This program manual describes the requirements, roles, and responsibilities for risk management. It provides direction to the Bear Valley Electric Service Company (BVES) on implementing the Company's Risk Management Framework.

BVES's risk management process consists of six high-level processes (in bold below) that are described in detail in this document. The following summarizes what must be accomplished in each step:

Risk Identification

- Gather an initial list of risk events in a brainstorming session
- Review and categorize brainstormed risk events (e.g., link risk events to asset classes)
- Select priority risk events for initial analysis
- Document work involved in Risk Identification

Risk Analysis

- Perform initial analysis on selected risk events (e.g., is impact high, medium, or low?)
- Select risk events for full analysis
- Perform full analysis on selected risk events (e.g., assess frequency and impact)
    - Assign an impact rating in six impact categories
- Develop Basis Document to capture assumptions and rationale behind scoring
- Communicate analysis results to affected parties
- Document work in Risk Register

Risk Evaluation and Scoring

- Conduct calibration session to review total score for each fully analyzed risk
- Examine outliers and prepare for mitigation
- Communicate results to affected parties
- Document work in Risk Register

Risk Mitigation

- Review existing controls for adequacy
- Develop new mitigations (if necessary)
- Document work in Risk Mitigations and Controls portion of Risk Register

Risk Informed Investment Decisions (Annual and Periodic)

- Consolidate portfolio of proposed controls and risk mitigations
- Examine alternative solutions
- Conduct cost/benefit analysis on controls and risk mitigations
- Produce budgetary estimates for controls and risk mitigation
- Provide impact summary of any budget adjustments (if necessary)
- Apply constraints to prioritize/optimize

Risk Monitoring

- Review risk register on a periodic basis
- Consider new and emerging risk events
- Direct new and emerging risk events to Risk Analysis and Risk Evaluation and Scoring process

Our goal is that all employees become "risk managers" who are encouraged to identify and ultimately help mitigate risks.

Background

As a result of several major incidents across the utility industry, there has been an increased focus on risk management. Incidents such as Superstorm Sandy, the Metcalf substation attack, and the San Bruno pipeline explosion have heightened the awareness of risks and the need for more in-depth risk management practices in utilities. Further, regulators, customers, and elected officials around the country are demonstrating more interest in our work.

BVES's interest in risk management led to the development of a risk management framework. When fully implemented, the framework will introduce a transparent, auditable, and repeatable process for risk management. The risk management framework includes the following products, all of which are addressed in the program manual:

- Risk Lexicon
- Risk Management Process
- Risk Register
- Risk Evaluation Matrix (aka 7 x 7 heat map)
- Risk Impact Category Descriptions
- Risk Scoring Methodology

Implementing this risk management process will have the following benefits:

- Establishes governance structure to support risk management
- Promotes more effective allocation of capital to projects and programs that reduce risks
- Enhances our ability to prevent risks before they occur
- Addresses aging infrastructure and asset renewal

Manual Purpose and Objectives

Risks affecting organizations can have safety, environmental, and societal consequences in addition to impacting economic performance and professional reputation. Managing risk effectively helps organizations to perform better in an environment full of uncertainty.

This manual describes the requirements, roles, and responsibilities for risk management. It provides direction on implementing the Company's Risk Management Framework.

The key objectives are to:

- Establish a common understanding of BVES's Risk Management process;
- Document employee guidance on risk management processes;
- Promote a risk-aware culture through consistent application and training on risk management principles and practices; and
- Educate and inform BVES stakeholders.

EVERY EMPLOYEE A RISK EMPLOYEE

Our goal is that all employees become "risk managers" who are encouraged to identify, analyze, and ultimately help mitigate risks.

Key Terms

Everyone should speak the same "risk language" when discussing risks. Become familiar with BVES's Risk Lexicon in Appendix A. This lexicon is consistent with the lexicon recommended by the California Public Utility Commision Risk Lexicon Working Group (CAPUC RLWG).

Risk Management Scope

Risk is inherent in all utility operations, and risk management should become a part of routine management activity across all levels of the Company. ***Our goal is that all employees become "risk managers" who are encouraged to identify and ultimately help mitigate risks.***

The risk management framework is broadly applicable to all operating environments at BVES. It can be applied to operational risks as well as strategic, regulatory, and people risk.

Roles and Responsibilities

Director-BVES is responsible for providing strategic direction for the risk management program. This includes:

- Reviewing and approving strategic objectives.
- Reviewing and approving top risks to BVES including new and emerging risks.
- Reviewing and approving risk informed investment recommendations. These may include implementing recommended mitigations to top risks and/or modifying existing controls to top risks.

Operations and Planning Manager is responsible for overseeing the implementation of the BVES risk management program. This includes:

- Reviewing the processes, people, assets, infrastructure, and technology that support the risk program strategic objectives.
- Working with the System Safety and Reliability Engineer, Subject Matter Experts (SMEs) and other sources to identify and assess risk events.
- Facilitating the process to make decisions relative to the projected risk reductions and estimated costs.
- Assigning SMEs to work with the System Safety and Reliability Engineer on risk management program items.
- Assigning Risk Owners to the top BVES risks.
- Reviewing and recommending top risks to BVES including new and emerging risks.
- Reviewing existing controls and proposed mitigations to top risks to BVES in the risk register.
- Reviewing and recommending risk informed investments. These may include implementing recommended mitigations to top risks and/or modifying existing controls to top risks.
- Reviewing assessments on the effectiveness of mitigations and/or modifications to controls that are implemented by BVES.

System Safety and Reliability Engineer is responsible for implementing and managing the BVES risk management program. This includes:

- Reporting directly to the Operations and Planning Manager on all matters and aspects of the BVES risk management program while keeing the Engineering and Planning Supervisor informed.
- Leading and facilitating all risk management program efforts as outlined in this manual.
- Developing and maintaining the BVES risk register of top risks.
- Implementing and executing the risk management processes of this manual.
- Identifying and/or causing to be identified the top risks and forwarding to BVES management for approval. This includes new and emerging risks.
- Identifying and/or causing to be identified existing controls for the top risks.
- Developing and/or causing to be developed proposed mitigations to the top risks.
- Quantifying and/or causing to be quantified the impact scores for proposed mitigations.
- Quantifying and/or causing to be quantified the impact scores for proposed changes to existing controls.
- Calculating and/or causing to be calculated the risk-spend efficiency for proposed mititgations and/or changes to existing controls to support risk informed investment decisions by BVES management.
- Monitoring the implementation of approved mitigations and/or changes to existing controls.
- Monitoring the effectiveness of mitigations and/or changes to existing controls, determining adjustments as necessary, and reporting the progress and results to

management at least quarterly. This includes developing and monitoring Key Risk Indicators (KRIs) to monitor risks as needed and developing and monitoring Key Performance Indicators (KPIs) to measure effectiveness of BVES's overall risk management program as needed.

- Facilitating the process to periodically (at least every six months) review and refresh the BVES risk register to keep it current by identifying and/or re-evaluating threats and characterizing sources of risks.
- Ensuring that as the risk register is updated that risk measures to mitigate identified risks developed or modified as applicable; risks (consequences and likelihood/probability of occurrence) are quantified or re-quantified; and risk mitigation impacts (risk reduction) are quantified or re-quantified.
- Recommending to management based on the periodic evaluations and implementing new risk mitigations and allocating resources as applicable using the risk informed investment process.
- Facilitating an annual evaluation for each authorized mitigation measure the risk reduction achieved against that predicted and use that information to help assess the effectiveness of the mitigation measure as well as to improve the risk-based decision-making process.
- Monitoring changes to the planned budget to mitigations and existing controls to top risks in the risk register and alerting management and the risk team to the impact, if any.
- Leading risk program meetings and sessions. This includes ensuring agendas and minutes are produced for the meetings.
- Acting as Risk Owner for all BVES top risks unless these duties are specifically assigned to other BVES Staff. See below for Risk Owner responsibilities.
- Requesting the assignment of SMEs and Risk Owners as needed to support the risk management program.

Risk Owner is assigned by the Operations and Planning Manager and is responsible for working closely with the System Safety and Reliability Engineer to apply the risk management process as identified in this manual to the assigned risk(s). This includes:

- Populating the identified risk in the risk register
- Analyzing the risk potential consequences and likelihood.
- Identifying and assessing the existing risk controls.
- Identifying and assessing the proposed mitigations.
- Developing the risk implementation plan if it is decided that the risk will mitigated.
- Overseeing the implementation of the risk plan.
- Monitoring and reporting on the results of the risk mitigation activities.
- Requesitng SME support as needed. Normally, the selected Risk Owner is the SME in the specific area of the risk.

Subject Matter Expert (SME) is assigned by the Operations and Planning Manager and is responsible for providing technical knowledge and assistance to the System Safety and

Reliability Engineer and/or Risk Owners as applicable in the application of the requirements of this manual to assigned risk(s). This includes providing technical assistance in determining:

- Reasonable worst case event for a top risk.
- Fequency of the reasonable worst case event and impact scores.
- Existing risk controls in place.
- Mitigations and effect on frequency and impact scores.
- Other technical information as needed to support the System Safety and Reliability Engineer and/or Risk Owners as applicable in applying the risk management process to specific risks.

Risk Management Overview

BVES's approach to risk management is grounded in the basic tenets of the International Standardization Organization's (ISO) "Risk Management – Principles and Guidelines" (ISO 31000). Following ISO 31000 is said to help organizations achieve objectives, improve the identification of risks, and more effectively allocate resources for risk reduction.

BVES's risk management process, pictured in Figure 1, consists of six high-level processes.

Figure 1 - BVES's High-Level Risk Management Process

Risk Management Framework

The following sections describe the six processes of BVES's Risk Management Framework in detail. The processes are:

1. Risk Identification
2. Risk Analysis
3. Risk Evaluation and Scoring

4. Risk Mitigation
5. Risk Informed Investment Decisions
6. Risk Monitoring

Investment management

Investment management (capital and O&M) is related to risk management. Investment management is the process of allocating financial resources (capital and O&M) to manage risks in the most cost efficient manner. Investment management is also key in integrated risk management. Investment management optimizes investment strategies to fund risk mitigation efforts, which are informed by asset management processes.

The work of investment management is done within a constrained resource environment. Typically, utilities establish criteria for evaluating and prioritizing how to invest in potential projects and programs.

BVES Vision for Integration of Risk, Asset, and Investment Management

BVES's long-term vision for operational risk management is to integrate the risk management, asset management, and investment management processes with business continuity management in order to have a consistent approach across the operational risk management spectrum. The inputs and outputs of risk, asset, and investment management inform and support the others.

Integration of risk, asset, and investment management is evident when a company:

- Identifies its risks, including risks associated with operational assets;
- Develops mitigations that include the asset strategies to address failures; and
- Makes investments based on the risks identified.

Process 1: Risk Identification

Risk identification is the "process of finding, recognizing, and describing risks."[1] The risk team should begin its work with a clear understanding of the organization's business objectives and strategies. Once the team understands strategies and objectives, they can evaluate which risk events could most affect BVES.

Issue Guidance for Risk Gathering

The first step in risk identification is to issue guidance for risk gathering. The guidance defines the portion of the risk taxonomy being examined and describes the level of detail expected in the risk gathering. The guidance also addresses the schedule for the risk management process.

Sources to Collect Risk Events

Brainstorming sessions will initially be the primary source of identifying risk events. Brainstorming is not the only source, however. Other sources include:

- Interviews;
- Surveys;
- Questionnaires;
- Subject matter expertise;
- Field observations (e.g., safety practices);
- Industry benchmarking;
- Lessons Learned
- Incident data collection (internal or external)

Above all, the goal here is to develop a comprehensive list of risk events that could endanger the safety of BVES personnel or the general public, or the reliability of BVES' systems and equipment.

Brainstorming Session(s)

A brainstorming session will be used to identify an initial list of risk events. The sessions will be conducted to place some natural parameters on the number and types of risk events considered. Brainstorming is the most interactive and educational tool an organization has to

[1] International Organization for Standardization, ISO 31000: Risk management – principles and guidelines (Geneva, Switzerland: 2009), 4.

collect risks. It encourages participants to consider "black swan events"[2] that may reveal new risk events. In addition, brainstorming involves key stakeholders and SMEs, thereby exposing a wider audience to the BVES Risk Management Framework.

Good planning and preparation are keys to an effective session. The steps described here increase chances that the sessions will be successful:

Guidance for Brainstorming Session(s)

Decide How to Organize the Sessions: The System Safety and Reliability Engineer will decide how many sessions to conduct. The approach for brainstorming is at the System Safety and Reliability Engineer 's discretion with guidance from the Operations and Planning Manager. The BVES risk team must stay within the schedule for the risk management process. The team must avoid becoming overwhelmed by a long list of brainstormed risk events.

Identify Participants: Participants should be SMEs who represent a broad cross-section of the BVES organization. These SMEs may be a larger and broader group than those SMEs on the risk team. The System Safety and Reliability Engineer should also consider how many participants are optimal for a productive session.

Decide Length of Session: Schedule at least two-three hours for brainstorming sessions. There may also be a need to conduct multiple sessions.

SUCCESSFUL BRAINSTORMING

Develop an agenda with clear goals and objectives for the session.

Consider risk events that could occur, regardless of whether they have occurred to BVES or in the industry

Ask participants to complete some "homework" ahead of time.

Have participants come prepared to discuss two or three risk events along with an example risk event that may have occurred in the industry.

Ask participants to review the BVES Risk Lexicon before the meeting. This can help reduce the amount of discussion on key terms.

[2] Black swan events are low probability, high consequence events. These events come as a surprise and are hard to predict.

Facilitate Meeting: The System Safety and Reliability Engineer or a trusted SME should facilitate the session. Observing the following guidelines for effective brainstorming is important:

- Encourage the free flow of ideas (e.g., state there are no bad ideas);
- Promote innovative thinking;
- Encourage the participation of all invitees;
- Discourage participants from criticizing each other's ideas;
- Limit outside interruptions (e.g., e-mail); and
- Capture all input.

Describing a Risk Event:

When presenting a potential risk event, encourage participants to document or state their risks in a somewhat descriptive manner. For instance, some participants may first identify hazards, threats, or mitigations as a risk event. This is to be expected. The facilitator can use those inputs to elicit a risk event and should feel free to ask follow-on questions if needed to elicit the level of detail desired.

Review and Categorize Risk Events

The risk team reviews the list of risk events developed in the brainstorming session(s). This review will eliminate any duplications and combine similar risk events. Next, risk events should be categorized. An example of categorization is to align risks with asset classes (e.g., poles, transformers, conductors). Categorization helps to identify risk events that more directly affect the Company objectives. Those risk events likely require more attention.

Enter Risk Events into Risk Register

Categorized risk events should be documented in Microsoft Excel or in the risk register.

DESCRIBE A RISK EVENT

A description should contain enough detail to allow the Risk Team to understand the true risk.

For instance, "Distribution System Safety" is not a clear risk. What is the risk event? What will BVES be trying to mitigate?

Avoid confusing hazards, threats, and mitigations with risk events. Hazards and threats can lead to a risk event but are not the same as the event itself.

Also, use clear language. Using "pole failure" in a risk event description can lead to confusion. Is the risk that the pole will fail inspection or will fall down?

Here is an example of a good risk description: "contact with a live wire because of distribution pole falling down." This is more descriptive and makes it less likely the risk team will have to untangle a vague risk event.

Select Priority Risk Events for Initial Analysis

By this step, the risk team has already collected an initial set of risk events, reviewed those risk events, and categorized them. The initial brainstormed list has been reduced to a more manageable number. The risk team will next select a subset of risk events they want to take into initial analysis. If the risk team still has too many risks for initial analysis, it should focus on a subset of risks and should document its rationale for selecting those risks.

WORST REASONABLE CASE

Risk Event: Failure of or contact with energized substation circuit breakers and switchgear (Risk Event)

Worst Reasonable Case: Oil-filled breaker failure in a medium-sized substation injures employee, damages nearby equipment and impacts >1,000 customers until station is restored

Process 2: Risk Analysis

Risk analysis is the "process to comprehend the nature of risk and to determine the level of risk."[3] This process provides a basis for risk evaluation and decisions about risk mitigation.

Initial Analysis

Initial analysis requires the risk team to begin examining the priority risks selected during risk identification. In this step, SMEs collect basic information about a risk. This analysis will be entered into the risk register by the System Safety and Reliability Engineer. This information includes the following:

- Title of Risk
- Worst Reasonable Case
- Risk Owner
- Asset Class
- Quick Evaluation of the risk event (High, Medium, or Low)

The quick evaluation reflects the SME's "gut reaction" to potential impacts of the risk event. No rigorous analysis is yet required.

Developing Worst Reasonable Case

The worst reasonable case evaluation is ideally based on plotting a range of outcomes along a distribution and, for purposes of the risk discussion, choosing a scenario that identifies a reasonably probable worst-case outcome.

[3] International Organization for Standardization, ISO 73: Risk management – Vocabulary (Geneva, Switzerland: 2009), 6.

Once the risk team agrees on a Worst Reasonable Case, the impacts are defined on the most likely outcome of that Worst Reasonable Case. *Given the worst reasonable case scenario, what is the most likely outcome in the six impact categories?*

If sufficient data does not exist to produce a distribution to define the worst reasonable case, then the risk team will develop the worst reasonable case scenarios based on expert judgement.

Select Top Tier Events for Full Analysis

This requires organizations to select top tier risks for full analysis. The hierarchy below provides guidance for categorizing risk events into three tiers. Tier 1 risk events present the greatest vulnerability to the company. Organizations focus on Tier 1 risks before addressing Tiers 2 and 3.

- Tier 1
    - Has the potential to impact many processes;
    - Could affect more than 4 risk categories;
    - Risk velocity[4] is high; or
    - Could affect corporate level policies or goals and/or have effects across multiple parts of the company
- Tier 2
    - The risk event affects several processes;
    - The risk velocity is moderate; or
    - Could affect policies or goals and/or have effects across multiple facilities or operating regions within the company.
- Tier 3
    - Impacts one process;
    - The risk velocity is slow; or
    - Could affect a single department level policies or goals and/or be unique to a facility or operating region.

***NOTE**: Risk velocity of operational risks is generally faster than the velocity of other sorts of risks.*

Conduct Full Analysis

Full risk analysis involves a comprehensive examination of a risk event. This analysis focuses on residual risk. Questions that will be addressed when analyzing risks are:

- Has this risk event happened before?
    - Consider risk events that occurred at BVES and peer utilities
    - Consider risk events that have not occurred anywhere

[4] Risk velocity is defined as "Speed of onset; the speed with which a risk manifests itself."

- What caused the risk event?
- When did this risk event last occur?
- How often (frequency) has the risk event happened?
- What was the outcome (consequence) of the risk event?
    - How long did it last?
    - How long did recovery take?
    - How much did it cost?
- Can the probability of the risk event be modeled?
- Can the risk event be related to another risk?

SMEs judgment is crucial to full analysis. Each part of full analysis is described in the following sections (in bold below):

Evaluate Risk Impact Categories

BVES has established Risk Impact Categories to assess the impact of an event. Table 1 defines these risk categories. BVES has also established descriptions in each category that describe increasing levels of severity from level 1 (negligible) to level 7 (catastrophic). These Risk Impact Category Descriptions provide the risk team with guidance for analyzing and scoring risk events. The descriptions provide a consistent framework to assign an impact value (level 1 to 7) to risk events across all five impact categories.

Table 1 – Risk Impact Categories and Descriptions

Impact Category	Definition	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extensive (5)	Severe (6)	Extreme (7)
Reliability	Ability of a process, asset, or system to perform its normal functions. eliability is measured by end customer impact.	**Customer Impact:** Less than 20 customers affected (e.g., 1 transformer out)	**Customer Impact:** 20-500 customers affected (e.g., loss of 1 section of a 4KV circuit.)	**Customer Impact:** 500-1500 customers affected (e.g., loss of partial circuit or entire circuit.)	**Customer Impact:** 1500-5000 customers out (Loss of a section of a transmission line.	**Customer Impact:** 5000-10,000 customers affected (e.g., loss of a section of a transmission line.) Shutdown of a major business customer.	**Customer Impact:** 100% of customers out for less than 24 hours.	**Customer Impact:** 100% of customers out for more than 24 hours.
Compliance	Ability to meet regulatory/legal requirements. Impact seen in increased regulatory oversight, adverse regulatory actions, or penalties.	Informal complaint without fine or penalty	**Regulatory:** Formal complaint from arbitrator (JPA) Notice to correct deficiency **Legal:** Civil lawsuit filed	**Regulatory:** Regulatory prescription on Company 3rd party complaint **Legal:** Civil lawsuit is filed but is settled out of court	**Regulatory:** Adverse regulatory mandates and fines **Legal:** A civil lawsuit with verdict or enforcement actions against the company or a lawsuit with criminal charges.	**Regulatory:** Imposed direct regulatory oversight Fines $$ **Legal:** Criminal charges filed but settled out of court.	**Regulatory:** Sarbanes-Oxley compliance violation Fines $$$ **Legal:** Lawsuit with verdict against the company and/or findings of criminal activity.	Company goes out of business Fines $$$$ **Legal:** Criminal charge(s) with conviction

Quality of Service (Cost, Quality, Complaints)	Measure of impact of a risk event on trust in company and company brand. Typically measured by cost, power quality, and customer complaints.	Little to no effects on cost, power quality or customer complaints	**Cost:** Meter failure at a small business **Power Quality:** Customers exposed to power factor or RFI issues **Complaints / Customer Service:** Release of inaccurate information to public	**Cost:** Moderate planning and/or construction cost overruns **Power Quality:** Customers experiencing excessive flicker **Complaints / Customer Service:** Increase in informal customer complaints	**Cost:** Shutdown of a major commercial customer **Power Quality:** Customers affected by BVES noise **Complaints / Customer Service:** Increase in customer complaints to SR management	**Cost:** Poor project decision-making that creates a stranded asset **Power Quality:** Customers experiencing excessive numbers of momentatries **Complaints / Customer Service:** Increase in formal customer complaints to regulators	**Cost:** Unhedged for a one-year period **Power Quality:** Disruptive harmonics issues **Complaints / Customer Service:** Damage to trust/reputation requiring some outreach to state/local political officials.	**Cost:** Unhedged during a major price spike **Power Quality:** Voltage outside of national code (e.g., voltage excursion outside IEEE, STD) **Complaints / Customer Service:** Loss of trust/reputation requiring sustained outreach to state and/or local political officials
Safety	Degree to which a risk event leads to injury to a person (employee, contractor, or public). Typically measured by event severity (workforce or public). Common measure is OSHA recordables.	Unplanned event that did not result in injury, illness, or damage but had the potential to do so (aka Near Miss)	OSHA recordable Public injury requiring first aid/medical care	Lost time accident Public injury requiring hospitalization	Long term disability	Life Altering Injury (A life-altering injury is one that results in permanent or long-term impairment of an internal organ, body function, or body part. Examples include, but are not limited to significant head injuries, spinal cord injuries, paralysis, amputations, or broken or fractured bones.)	Single fatality (public, employees, or contractors)	Multiple fatalities (public, employees, or contractors)
Environmental	Degree to which a risk event negatively affects people, natural resources, or species. Can be measured by duration, hazard level, location, and size of event.	Event resulting in negligible but no long-term damage to the environment (e.g., small oil leak contacting ground but no containment required.)	Event that can be contained in a small area (e.g., oil leak in substation requiring active containment).	Event that is quickly correctable (e.g., small confined fire that can be extinguished by BVES. Improper hazardous waste disposal that is not reportable (e.g., minor event like putting a paint can in wrong bin).	Excessive power plant emissions that is reportable OR improper hazardous waste disposal that is reportable	Events with potential for medium-term impact and/or require outside resources for support (e.g., large leak or emissions release with long-term impact requiring support services.)	Events with potential for long-term impact requiring outside resources for support (e.g., wildfire caused by BVES in a large area requiring public response.) Event could also have an impact on wildlife.	Events with potential long-term impact requiring outside support and resulting in substantial damage to a protected area or species (e.g., large oil spill into navigable waters).

After designing the Risk Impact Category Descriptions, BVES calibrated the definitions both within a particular category and across categories. The horizontal calibration ensured that impacts within particular category increase in severity by a significant magnitude from level to level. The increase from level to level is based on a logarithmic exponential base 10 scale.

For example, a level 3 safety impact is a significant magnitude worse than a level 2 safety impact which is, in turn, a significant magnitude worse than a level 1. Similarly, impacts were calibrated vertically across the five categories. For instance, a level 4 impact is equivalent across Reliability, Compliance, Quality of Service, Safety, and Environmental. Because of this vertical and horizontal calibration, all impact categories are equally weighted when calculating a risk score.

Assess Frequency of Worst Reasonable Case

Frequency is defined as "number of events per unit of time." It is a measure of how often a risk event has occurred or could occur. The frequency being measured is the frequency of the worst reasonable case of a specific risk event. Ensuring that users are measuring the frequency of the worst reasonable case and not the frequency of a risk event itself will help ensure consistency in analysis.[5] BVES's frequency table for risk events appears at Table 2.

Table 2 – Frequency Table

Level	Value	Occurrence
	7	>10 times per year
	6	1-10 times per year
	5	Once every 1-3 years
	4	Once every 3-10 years
	3	Once every 10-30 years
	2	Once every 30-100 years
	1	Once every 100+ years

***NOTE**: When assessing the frequency of a risk event, consider the experience of other peer utilities. Just because BVES has not experienced a risk event does not imply the event will never occur. The key question to consider is "what is the expected frequency of the worst reasonable case?"*

Identify Hazards/Threats (Triggers)

Many risk events result from several different intermediate events. These "triggers" are essentially the causes of a risk. *What factors acting together caused the risk to occur?* Risk triggers can include human error (employee or contractor), mechanical failure of an asset, or a natural uncontrollable event (e.g., storm). For example, the causes or triggers of an aircraft accident could include pilot error, sensor failure, crew fatigue, and inclement weather. Any of these alone might not have caused an accident. Deconstructing the risk event this way may

[5] Suppose the risk event is "exposure to a conductor because of a dig in" and the worst reasonable case is "dig in that results in a fatality." The frequency is based on the latter.

allow the risk team to get a more complete evaluation of the risk event and take a broader view of controls and mitigation actions in place.

Catalog Existing Controls

During Full Analysis, the risk team will also want to catalog the controls that are already in place to address the risk. This information can be added to the Controls and Mitigations portion of the risk register. Controls may apply to multiple risks, so there is a many-to-many relationship between controls and risks events.

Prepare Basis Document and Enter into Risk Register

The information considered in these steps should be documented in a Basis Document and entered into the risk register. The Basis Document provides a rationale for each risk impact category rating and frequency value. SMEs will use the Basis Document to present the risk event during the calibration sessions in the Risk Evaluation and Scoring process.

The Basis Document will capture all the assumptions and background necessary to score the risk. It will have the following information:

- Risk Event
- Risk Description
- Worst Reasonable Case
- Controls in Place
- Frequency and rationale (develop 1-2 sentences describing why the frequency is as defined)
- Risk Impact Categories and rationale for each (develop 1-2 sentences per impact category describing the impact in each category)

Given that we are examining residual risk and not inherent risk,[6] the analysis should consider and document the existence of any controls that are already in place.

Table 3 shows a sample basis document.

***NOTE**: This event has not occurred nor should be taken to reflect any actual historical event experienced by a BVES facility.*

[6] Inherent risk is "the level of risk that exists without risk controls or mitigations." Residual risk is "risk remaining after current controls." Residual risk accounts for the presence of controls such as inspection and maintenance programs where inherent risk does not. Inherent risk represents "raw risk" without any controls.

Table 3 – Sample Basis Document

Risk Event:		**Risk Plot Key:**	
Reasonable Worst Case:			
Controls:			
Risk Scoring			
Frequency Score	**Impact Scores**		
	Reliability		
	Compliance		
	Quality of Service		
	Safety		
	Environmental		
Total Risk Score:			
Additional Mitigations Considered:			

Communicate Results

Upon conclusion of the risk analysis process, the results will be shared with the Director, Operations and Planning Manager, Engineering and Planning Supervisor, Risk Owner(s), Risk Manager, and the initial risk identifier by the System Safety and Reliability Engineer. This communications feedback loop is important to fostering continued engagement of all employees in the risk management process.

Process 3: Risk Evaluation and Scoring

Risk evaluation is the "process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable."[7]

Total Risk Score

The risk register calculates a total risk score from the data collected in risk analysis. The risk scores establish a relative ranking of risk events for discussion purposes. The score is a calculation based on an SME discussion of the impact and frequency associated with the worst reasonable case. The potential impacts of the worst reasonable case across the six impact categories are then scored between 1 and 7 (7 being the greatest severity). Once the impact is articulated, a frequency based on data and subject matter expertise is assigned to each worst reasonable case scenario. The risk register then applies a formula to create a score between 0 and 1,000,000,000. The formula used by BVES is:

$$\text{Risk score} = \sum_{i=1}^{n} weight_i * frequency_i * 10^{impact_i}$$

BVES uses the risk scoring methodology for all risks. The Risk Scoring Methodology is described in Appendix B.

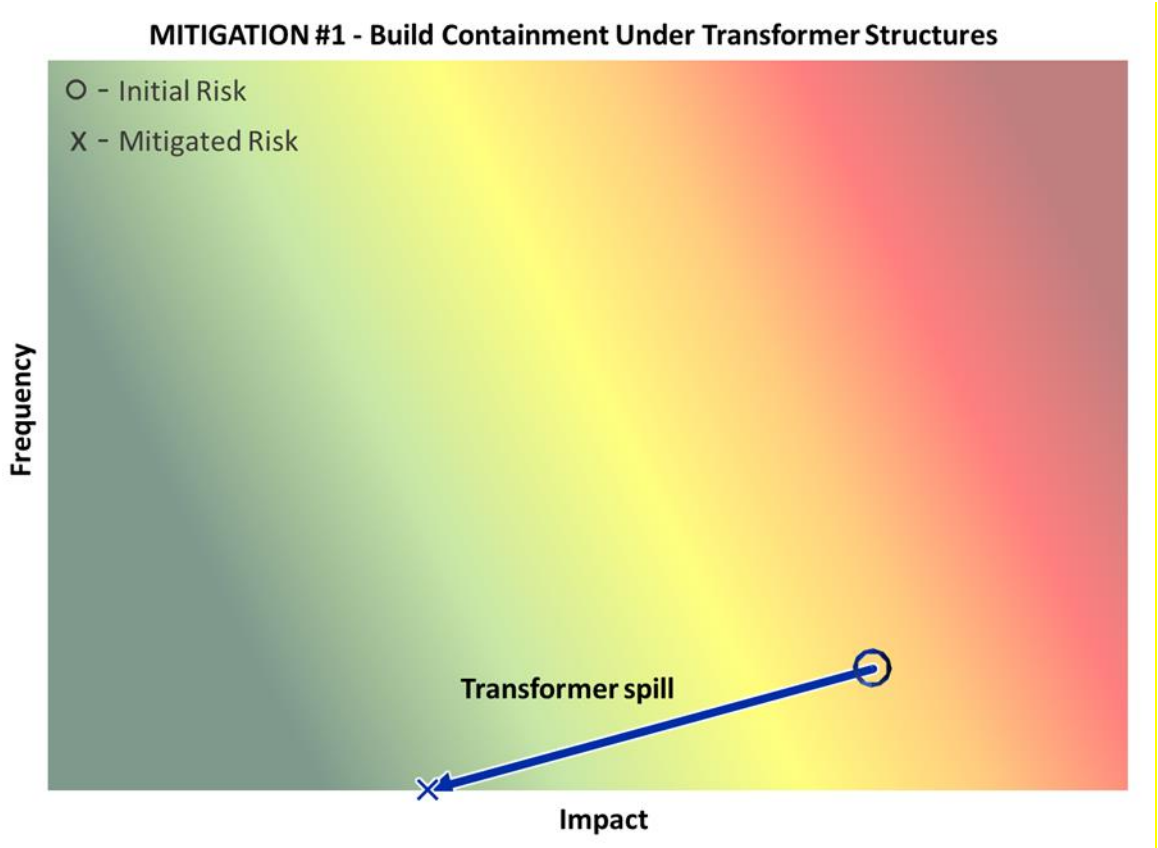
Heat Map

The scores of risk events can be plotted on a heat map matrix (Figure 2). BVES has chosen to use a 7 x 7 heat map matrix. The 7 x 7 matrix is consistent with leading practice in the utility industry. It provides a better differentiation of risk events than a 3 x 3 matrix or a 5 x 5 matrix. Those maps produce a less distinct differentiation of risks. That is, many risks are high impact, low frequency and occupy the same space on the heat map, thereby limiting its usefulness in identifying areas of focus.

A 7 × 7 matrix provides a better view of relative priority of risk events. The scale places a greater value on mitigating risks in the top right quadrant of the matrix rather than the bottom left.

[7] ISO 31000, 6.

Figure 2 – Sample Heat Map



The heat map shown above is a visual display of the relative ranking of risk events. Each green circle represents a specific risk event that has been through full analysis. The numbers inside each circle represent a unique identifier for each risk. The circles are plotted on the heat map based on their risk scores. Risks in the top right quadrant have higher risk scores than those on the bottom left.

Calibration Sessions

Once risk events have been fully analyzed and scored, the risk team conducts an internal calibration session with a broad set of SMEs. The session focuses on those risks that are outliers or for which an SME may question the accuracy of the overall score. The SME or Risk Manager for each risk in question presents the material contained in the Basis Document and offers attendees the opportunity to discuss the risk scoring. Organizers should follow the guidance provided for brainstorming sessions, although the calibration sessions may be longer, depending on the number of risk evaluations that are discussed.

During calibration sessions, participants question assumptions and other inputs to risk scores to ensure alignment in how risks were evaluated. Once the calibration is complete, organizations are allowed to re-score any risk that has been successfully challenged.

Update Risk Register

After the calibration sessions, update the risk register with any adjustments to scoring. Update the Basis Document as well if needed.

Identify Outliers

After the calibration sessions, the risk team once again examines its list of risk events. The team takes one additional look at any outliers to ensure scoring is consistent and outliers are valued appropriately.

Communicate Evaluation Outcome

The results of risk evaluation and scoring are shared with the Director, Operations and Planning Manager, Engineering and Planning Supervisor, Risk Owner(s), Risk Manager, and the initial risk identifier by the System Safety and Reliability Engineer.

Process 4: Risk Mitigation

Risk Mitigation moderates or alleviates a risk to lessen its likelihood or consequence in some way.

Existing Controls

The first step in the mitigation process is to determine whether any existing controls are already established and in place. The risk team may have collected some of this information in the Full Analysis step of Risk Analysis, but will review the data for completeness.

Develop Mitigations

Based on the results of risk evaluation, risk mitigations should be developed and documented for those enterprise risks identified as needing mitigation.

When developing and documenting mitigations, some considerations are:

- Existing controls currently in place to mitigate the risk (these should have been collected in risk analysis but are re-visited);
- Historical or prior controls that have been abandoned;
- External industry or mandatory compliance standards for mitigating the risks;
- Decisions to accept or transfer risks; and
- Sharing of risks

Each risk event should have a documented mitigation plan that provides an overview of the risk, the current mitigation plan, and the proposed future mitigation. The risk team updates the mitigation plan on at least an annual basis to reflect any changes to the status of the risk and the associated mitigations.

Enter Data on Controls/Proposed Mitigations

At this step, the risk team enters the control and mitigations data into the Risk Mitigation and Controls portion of the risk register.

Are controls and mitigations adequate?

The risk team should determine the adequacy of its controls and mitigations. Once the organization has examined its controls and proposed mitigations, it must decide how to characterize the control status of the risk event. The following statuses are possible ways to describe adequacy and can also facilitate reporting on an executive dashboard:

- Red – controls not adequate
- Amber – controls need strengthening
- Green – controls are adequate

The risk status should change toward green as the mitigations are implemented and the controls are strengthened to an adequate level. The risk score will only change if mitigations adjust the impact or frequency levels. In other words, the Risk Impact Category ratings may change only if mitigations can physically prevent or reduce the frequency or impact of the Worst Reasonable Case scenario.

Update Data on Controls/Proposed Mitigations

If necessary, update the information in the risk register.

Process 5: Risk-Informed Investment Decisions (Annual Process)

Process 5 is the investment management (capital and O&M) piece as is described earlier in the Risk Management Framework discussion. The risk-informed investment decision process allows BVES to review all investment opportunities and adjust the recommended portfolio based upon results of the first four processes.

Portfolio of Proposed Controls/Mitigations

In the first step, the risk team will consolidate its lists of projects and programs. There are a number of potential project sources. These include:

- Regulatory mandates/compliance projects,
- Projects and programs begun in an earlier period (i.e., carryovers), and
- New projects/programs.

Because of the implementation of the risk management process in BVES, risk mitigation will be an increasingly important driver of new projects and programs along with the traditional drivers of aging assets, safety, and reliability.

Develop Scope for each Control/Mitigation

Here, SMEs will determine the details of each project, including the initial scope of work (i.e., what is in and out of scope for the work).

Consider Alternatives

These steps involve examining alternatives for all modified or new programs. These steps are essentially a consistency check to determine that any other reasonable alternatives have been evaluated.

Determine Key Information on Controls/Mitigations

Key information includes the following:

- Stakeholders affected/involved
- Initial Resources Required
- Preliminary Cost Estimate (i.e., order of magnitude/rules of thumb)
- In-Service Date
- Quantitative Value Drivers
- Qualitative Value Drivers

This step ensures that the SMEs are collecting the adequate amount of detail to assess the cost and benefits of the controls and mitigations.

Produce Budgetary Estimate by Control/Mitigation

This step calls for the SMEs to identify specific projects and programs. The controls in these projects and programs will be funded or reduced in funding. The budgetary estimate is a "rough order of magnitude" estimate.

Funding Decisions

The portfolio of controls and mitigations is consolidated for review by the BVES senior levels of leadership. Budget constraints are considered. Constraints include, for instance, resource constraints such as availability of trained and qualified personnel, execution constraints such as the time necessary to obtain required permits, and system constraints such as the ability to deliver service to customers while performing the total portfolio of work. Resource and other constraints may drive adjustments to the proposed work portfolio. Portfolio optimization[8]

[8] Portfolio optimization is the process of choosing the proportions of various assets to be held in a portfolio, in such a way as to make the portfolio better than any other portfolio according to an objective criterion.

techniques are applied to choose the appropriate mix of projects and programs to reduce risk. After optimization, funding is allocated. Senior Leadership then sets and approves the budget per the Company's budgeting policies and processes. The budget is finalized and results are communicated to the the Director, Operations and Planning Manager, Engineering and Planning Supervisor, Risk Owner(s), Risk Manager, and the initial risk identifier by the System Safety and Reliability Engineer.

Risk Informed Investment Decisions (Periodic)

This process is applied when the proposed budget is increased or decreased. This process requires the risk team to identify the effects of a budget adjustment and present those impacts to leadership. In doing so, the risk team has the opportunity to demonstrate the harmful effects of removing one or more controls. Removing controls could result in an increased risk score that could move the risk beyond the organization's risk tolerance. Similarly, the process allows the risk team to demonstrate the positive effects of introducing new or increased controls or mitigations. The System Safety and Reliablity Engineer is responsible for monitoring changes to the planned budget and alerting management and the risk team to the impact, if any.

Process 6: Risk Monitoring

Once the organization has completed the first five processes of risk management, it must monitor progress. The Risk Monitoring process includes review of all aspects of risk management and supports BVES's efforts at continuous improvement of its framework.

Scheduled or periodic monitoring and review of risk events ensures that risk owners understand the residual risk appropriately and evaluate the effectiveness of controls. New risks can appear while other risks may no longer exist (i.e., discontinued operations). Changes in business conditions may also change the risk frequency or velocity. The dynamic nature of risks requires the risk team to develop measures for monitoring risks and identifying such changes.

Key Risk Indicators / Key Performance Indicators

Key Risk Indicators (KRIs) are one method to monitor risks. They are leading indicators (i.e., predictive) and linked to the triggers of a risk. KRIs can also be helpful in the risk evaluation process by providing quantitative measures for a risk.

Established KRI thresholds can help identify when triggers of a risk reach a level that requires immediate response to mitigate potential consequences. KRIs can also help monitor and review the effectiveness of implemented mitigations. This monitoring promotes the effectiveness and efficiency of the implemented activities in both design and operations.

Key Performance Indicators (KPIs) are also be developed, monitored, and reported as a means of measuring effectiveness of BVES's overall Risk Management Program.

Periodic Review of Risks

BVES's Risk Management Framework calls for the organization to review and refresh their organization's risk register on a periodic basis. This periodic review keeps the risk register current and also allows the company to discuss the occurrence of any risk events, related consequences, and any emerging risks. Additionally, the review should be designed to periodically identify or re-evaluate threats and characterize sources of risks. The System Safety and Reliability Engineer will facilitate these reviews semi-annually or more frequently if needed. Typically, these reviews are best conducted in a brainstorming meeting with the risk team.

As part of this semi-annual review, the risk team should develop/re-evaluate risk measures to mitigate identified risks; quantify or re-quantify risks (consequences and likelihood/probability of occurrence); and quantify or re-quantify risk mitigation impact (risk reduction). Based on the

evaluations, the risk team should select and implement risk mitigations and allocate resources as applicable using the risk informed investment process identified earlier in this manual.

In addition to the proposed activities above, for each authorized mitigation measure, BVES will annually evaluate the risk reduction achieved against that predicted and use that information to help assess the effectiveness of the mitigation measure as well as to improve the risk-based decision-making process for future GRC applications.

Re-adjust scores?

During discussion there may be a consideration of whether risk scores need adjustment. For instance, is there any new information (e.g., new data) that would affect the scoring done earlier? If so, the risk team may re-engage and may return to the Risk Evaluation and Scoring process.

Consideration of New Risks

In addition, new risk events may be considered. For instance, has a peer utility BVES is aware of recently experienced a risk event that likely will affect BVES in the near future? If so, the risk team can analyze those risk events during the risk analysis process. This should be included in the semi-annual risk register review discussed above.

Appendix A: Risk Management Lexicon

Table 1 – BVES Risk Management Lexicon as recommended by the CAPUC RLWG

Term	Definition
Risk	The potential for the occurrence of an event that would be desirable to avoid, often expressed in terms of a combination of various outcomes of an adverse event and their associated probabilities. Different stakeholders may have varied perspectives on risk.
Inherent Risk	The level of risk that exists without risk controls or mitigations.
Event	An occurrence or change of a particular set of circumstances that may have potentially adverse consequences and may require action to address.
Frequency	Number of events generally defined per unit of time. (Frequency is often incorrectly treated as synonymous with probability or likelihood).
Probability	The relative possibility that an event will occur, probability is quantified as a number between 0% and 100% (where 0% indicates impossibility and 100% indicates certainty). The higher the probability of an event, the more certain we are that the event will occur. (Often informally referred to as likelihood or chance).
Impact (or Consequence)	The effect or outcome of an event affecting objectives, which may be expressed, by terms including, although not limited to health, safety, reliability, economic and/or environmental damage.
Mitigation	Measure or activity proposed or in process designed to reduce the impact/consequences and/or likelihood/probability of an event.
Outcome	The final resolution or end result
Risk Driver	Factor(s) that could cause one or more risks to occur (Risk driver may also be commonly referred to as “threat”).
Risk Response Plan	Collection of mitigations
Control	Currently established measure that is modifying risk
Alternative Analysis	Evaluation of different alternatives available to mitigate risk
Residual Risk	Risk remaining after current controls.
Planned or Forecasted Residual Risk	Risk remaining after implementation of proposed mitigations.
Risk Score	Numerical representation of qualitative and/or quantitative risk assessment that is typically used to relatively rank risks and may change over time.
Risk Tolerance	Maximum amount of residual risk that an entity or its stakeholders are willing to accept after application of risk control or mitigation. Risk tolerance can be influenced by legal or regulatory requirements.

Appendix B: Risk Scoring Methodology