2025 Risk Assessment Mitigation Phase

(Chapter SCG-Risk-8/SDG&E-Risk-8)
Cybersecurity

May 15, 2025

TABLE OF CONTENTS

I. INTRODUCTION

The purpose of this chapter is to present Southern California Gas Company (SoCalGas) and San Diego Gas & Electric Company's (SDG&E) (collectively, the Companies) risk control and mitigation plan for the Cybersecurity Risk.[1] This chapter contains information and analysis for this risk that meet the requirements of the California Public Utilities Commission's (Commission or CPUC) Risk-Based Decision-Making Framework (RDF),[2] including the requirements adopted in Decision (D.) 22-12-027 (Phase 2 Decision) and D.24-05-064 (Phase 3 Decision). Although the Cybersecurity Risk does not meet the minimum requirements for mandatory inclusion under the RDF, this risk is included in the 2025 RAMP Report because of its significant reliability consequences. This risk chapter describes the basis for selection of Cybersecurity Risk, the controls and/or mitigations put forth to reduce the likelihood or consequence of this risk, a discussion of alternative mitigations considered but not selected, and a graphic to show historical progress. This chapter presents cost and unit forecasts for the risk mitigating activities, but it does not request funding. Any funding requests for this risk will be made through the Company's Test Year (TY) 2028 General Rate Case (GRC) application. Finally, this chapter describes the methods applied to estimate the risk's monetized, pre-mitigated risk, the estimated risk-reduction benefits of each included control and mitigation, and the calculation of Cost-Benefit Ratios (CBRs) for each control and mitigation consistent with the method and process prescribed in the RDF.

A. Risk Definition and Overview

1. Risk Definition

For the purposes of this RAMP Report, SoCalGas's and SDG&E's Cybersecurity Risk refers to the risk of a major cybersecurity incident, which results in disruptions to electric or gas operations (Supervisory Control And Data Acquisition (SCADA) system, supply, transmission, distribution) and/or damage or disruption to Company operations (*e.g.*, human resources, payroll, billing, customer services), reputation, or disclosure of sensitive customer or Company data.

[1] This risk chapter is identical for SoCalGas and SDG&E because the Cybersecurity Risk is managed centrally for the Companies.

[2] As discussed in Volume 1, Chapter RAMP-1, the RDF Framework broadly refers to the recent modifications to the Commission's Rate Case Plan adopted in Rulemaking (R.) 13-11-006, Safety Model Assessment Proceeding A.15-05-002 et al. (cons.), and R.20-07-013 (the Risk OIR), including D.24-05-064, Appendix A.

Certain controls and mitigations presented in this chapter are subject to compliance mandates beyond RDF requirements, such as those from North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards and the Transportation Security Administration's (TSA) Security Directive (SD). A list of compliance requirements applicable to Cybersecurity is provided in Attachment A. Certain mitigation programs have value beyond the estimated risk reduction calculated under the RDF, such as protecting customers, and promoting public trust in the community.

2. Risk Overview

Cybersecurity is critical to the safe and reliable delivery of electric and gas service to customers, including critical infrastructure providers in Southern California (*e.g.*, financial services, telecommunication providers, other utilities). The Companies' service territories include millions of people, one of the nation's busiest ports, some of the country's largest cities, critical military bases, numerous defense contractors and small businesses.

Cybersecurity is a unique risk, as compared to other risks driven by operations and asset management, because it deals with intelligent adversaries that are attempting to achieve their objectives by gaining access to Company systems or information through artifice or other improper means. In addition, gaining information about the Companies' security controls and mitigation plans could be useful to an adversary—not only to directly harm the Companies and their stakeholders, including customers, but also to undermine broader national security and economic stability by exploiting vulnerabilities in critical infrastructure. Cybersecurity threats have continued to increase and have become more complex and impactful year over year. For these reasons, publishing the Companies' Cybersecurity-related controls, intelligence, strategies, and tactics in the public record could aid those adversaries, the bad actors that are attempting to disrupt the Companies' systems and society at large. Sensitive details associated with the content of this chapter are available upon Commission request for discussion in person.

The criticality of Cybersecurity is evidenced by the breadth of adversaries the Companies face. These adversaries include diverse types of threat actors with varying intent to cause harm; they are not just criminal entities or hackers looking to make a political statement or achieve financial gain. They also include advanced adversaries, often aligned to nation-states, that are targeting critical infrastructure for economic exploit, espionage, or covert action in preparation for some overt act (*e.g.*, disrupting energy supply). The Companies current and planned investment in Cybersecurity are prudent and reasonable to address this existing and growing threat.

Adversaries continue to use an evolving and increasingly more sophisticated set of tools and strategies to conduct attacks on the energy sector. Their suite of capabilities includes advanced malware, complex phishing attacks, identification of non-public vulnerabilities, and ransomware, among others. The Companies' strategy to counter rapidly evolving Cybersecurity threats must be flexible and enable adaption over time. Later in this narrative the discussion delves deeper into these threats and provides recent examples. Accordingly, timely and accurate Cybersecurity Threat Intelligence (CTI) is key to staying abreast of this ever-changing threat landscape. SoCalGas and SDG&E rely on federal, state, and local government partnerships for intelligence feeds along with peer utility industry relationships and private (subscription) based services for Industrial Control Systems (ICS) CTI. The Companies also obtain CTI from a variety of entities and sources, including Information Sharing and Analysis Centers (ISACs), the Federal Bureau of Investigations (FBI), Federal Energy Regulatory Commission (FERC), Department of Energy (DOE), Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA), Transportation Security Administration (TSA) and other U.S. intelligence community agencies. Information from threat intelligence sources in the utility industry continues to reveal adversaries that are employing advanced tradecraft in their attempts to access the nation's utility systems.

The next section examines the evolving threat landscape, with a focus on vulnerabilities in the Energy sector, which include the gas, bulk power grid, and renewable energy sectors and outlines specific risks to the Companies.

B. Threat Landscape

The cybersecurity threat landscape includes sophisticated adversaries like state-sponsored groups Volt Typhoon and Salt Typhoon (linked to Chinese intelligence) and Fancy Bear (APT28) from Russia, targeting Operational Technology (OT) and ICS environments and critical infrastructure. Cybercriminal organizations, such as the Z-Pentest hacker group, are increasingly attacking OT environments, including water treatment plants, and ransomware syndicates are exploiting these critical systems for higher payouts. Insider threats from employees or contractors with legitimate access also pose significant risks through credential exposure or social engineering schemes.

C. Tactics, Techniques, and Procedures

Tactics, Techniques, and Procedures (TTPs) refer to the specific methods and strategies used by cyber threat actors to achieve their objectives. TTPs include:

- **Remote Access Exploitation**: Attackers use brute-force attacks on Virtual Private Networks (VPNs) and exploit improperly configured remote access capabilities to access critical OT environments.
- **Vishing and Impersonation:** Spoofed calls to executives, impersonating IT staff or vendors, collect sensitive information using advanced voice phishing tactics.
- **Trojanized Software[3] and Watering-Hole Attacks:[4]** Malware in trusted software or websites targets specific organizations, similar to APT28 Fancy Bear campaigns.
- **Reconnaissance and Social Engineering:** Detailed mapping of organizational structures and employee behaviors using spear-phishing, spoofed phone numbers, and tailored watering-hole attacks.
- **Persistent and Adaptive Campaigns:** Persistent adversaries refine methods, focusing on credential theft, bypassing Multi-Factor Authentication (MFA), and data exfiltration.
- **HMI Manipulation:** Targeting programmable logic controllers (PLCs) with human-machine interfaces (HMIs) instead of exploiting zero-day vulnerabilities.
- **Disinformation Campaigns:** Groups like the Cyber Army of Russia (CAR) use disinformation alongside operational attacks, exaggerating control over critical infrastructure to spread propaganda.

D. Key Cyber Threat Vectors

Cybersecurity threat vectors, or attack vectors, are methods or mechanisms cybercriminals use to gain illegal, unauthorized access to computer systems and networks. Common threat vectors include:

[3] "Trojanized software" refers to legitimate software that has been maliciously altered to include a Trojan horse. A Trojan horse is a type of malware that disguises itself as a benign application but performs harmful activities once installed, such as stealing data or providing unauthorized access to the attacker.

[4] A "watering-hole attack" involves compromising a specific website or group of websites that are frequently visited by the target victims. The attacker infects these sites with malware, which then infects the visitors' systems. The goal is to target a particular group or organization by exploiting their common online habits.

- **Ransomware and Targeted ICS Attacks**: Ransomware gangs prioritize OT environments to disrupt energy delivery systems, leveraging their critical nature to demand higher ransoms.
- **Denial-of-Service (DoS) Attacks**: Persistent DoS attacks degrade ICS and OT system communications, often serving as a precursor to more severe attacks.
- **Third-Party Equipment and Supply Chain Risks**: Vulnerabilities in foreign-manufactured transformers and other components, flagged for embedded backdoors, present ongoing risks.

E. Specific Risks to the Companies

Threats specific to the energy industry include:

- **Vulnerabilities in Renewable Energy Systems**: The FBI has warned of increased cyber threats to renewable energy infrastructure as the sector expands. Adversaries target wind and solar farms, exploiting less mature security controls compared to traditional power grids.
- **Remote Access and Internet-Facing Devices**: Increasing reliance on remote access solutions introduces risks such as credential theft, brute-force attacks, and vishing schemes targeting remote workers and administrators.
- **Vendor and Supply Chain Exploitation**: Attackers compromise third-party vendors to infiltrate utility systems. Vulnerabilities in equipment sourced from foreign manufacturers exacerbate these risks.
- **Reconnaissance and Targeted Social Engineering**: Threat actors conduct sophisticated reconnaissance and launch tailored spear-phishing campaigns against high-level executives, leveraging spoofed communication channels and impersonation tactics.

F. Examples of Attacks Targeting Victims in the United States

1. OT Attacks on Utility Infrastructure

Title: *APT28 Infiltrates Texas Water Utility*

- **Link:** https://apnews.com/article/texas-muleshoe-water-systems-cyberattacks-russia-5f388bf0d581fc8eb94b1190a7f29c3a
- **Summary: July 2020:** APT28 infiltrated a Texas water utility’s OT systems through misconfigured remote access points. The attackers manipulated HMIs, disrupting operations and causing a water system to overflow. This incident exposed significant vulnerabilities in OT segmentation and inadequate access

control measures, highlighting the need for improved cybersecurity protocols in critical infrastructure.

***Title**: Colonial Pipeline hack explained: Everything you need to know*

- **Link**: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
- **Summary: May 2021**: The Colonial Pipeline, a major U.S. fuel pipeline supplying nearly 45% of the East Coast's fuel, was forced to shut down after a ransomware attack by the group DarkSide. The attackers exploited a compromised VPN password, leading to widespread fuel shortages and emergency declarations across multiple states. The incident marked one of the most significant cyberattacks on U.S. critical infrastructure and highlighted the urgent need for stronger cybersecurity in the energy sector.

***Title:** CAR Sabotages Texas Water Utilities*

- **Link:** https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/
- **Summary: April 2024:** CAR, potentially linked to APT44 Sandworm, released videos showing their ability to manipulate HMIs for water utility control systems in Abernathy and Muleshoe, Texas. This attack underscored the risks posed by poor access controls and unsecured OT interfaces, emphasizing the need for enhanced security measures to protect critical water infrastructure.

***Title:** CAR Targets Indiana Wastewater Plant*

- **Link:** https://www.cnn.com/2024/04/22/politics/russia-linked-hacking-group-targets-indiana-water-plant/index.html
- **Summary: April 2024:** CAR claimed responsibility for sabotaging the Tipton West Wastewater Treatment Plant in Indiana. The group demonstrated their capability to remotely access and manipulate critical infrastructure, raising concerns about the security of wastewater treatment facilities and the potential for significant environmental and public health impacts.

***Title:** Z-Pentest Disrupts Arkansas Water Treatment*

- **Link:** https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-arkansas-city-water-treatment-plant-prompting-federal-investigation/
- **Summary: September 2024:** The Z-Pentest hacker group forced hydraulic systems into manual control at a water treatment facility in Arkansas City, disrupting operations. This attack highlighted the growing sophistication of

cybercriminals targeting OT systems and the urgent need for robust cybersecurity defenses to protect essential services.

2. Attacks on IT

Title: *Volt Typhoon Targets Texas Power Grid*

- **Link:** https://www.mysanantonio.com/news/local/article/power-grid-attack-18551459.php
- **Summary: Summer 2023:** Chinese hackers, part of the Volt Typhoon campaign, attempted to access Texas power grid infrastructure, targeting the Public Utility Commission (PUC) of Texas and the Electric Reliability Council of Texas (ERCOT). Although no successful breaches were found, the attack highlighted vulnerabilities in the power grid and the need for enhanced cybersecurity measures to protect critical infrastructure.

Title: *Halliburton Cyberattack*

- **Link:** https://www.cybersecuritydive.com/news/halliburton-cyberattack/725065/
- **Summary: August 2024:** Halliburton, a leading energy services provider, experienced a cyberattack that led to the proactive shutdown of certain systems. The company notified law enforcement and confirmed that energy services were not impacted. This incident underscored the importance of cybersecurity in the energy sector and the need for rapid response protocols.

Title: *ENGlobal Ransomware Attack*

- **Link:** https://therecord.media/energy-industry-contractor-ransomware-disruption
- **Summary: November 2024:** ENGlobal, an energy sector vendor, faced a ransomware attack that involved illegal access and encryption of data files. The company restricted access to its IT systems to contain and remediate the attack. This incident marked the third disruptive cyberattack on Texas-based energy sector providers since August 2024, highlighting the persistent threat of ransomware.

Title: *BHI Energy Ransomware Attack*

- **Link:** https://www.bleepingcomputer.com/news/security/us-energy-firm-shares-how-akira-ransomware-hacked-its-systems/
- **Summary: May 2023:** BHI Energy, part of Westinghouse Electric Company, was attacked by the Akira ransomware gang. The attackers stole 690GB of data, including the company’s Windows Active Directory database.

Title: *Lazarus Group Exploits VMWare Horizon*

- **Link:** https://www.bleepingcomputer.com/news/security/north-korean-lazarus-hackers-take-aim-at-us-energy-providers/

- **Summary: September 2022:** The North Korean APT group Lazarus exploited VMWare Horizon servers to infiltrate energy providers in the US, Canada, and Japan. They used custom malware for data theft and system control, highlighting the sophisticated and versatile attack strategies employed by Lazarus and the significant threats posed to critical infrastructure.

G. Examples of Attacks Targeting Victims Globally

1. OT Attacks on Utility Infrastructure

Title: *Dragonfly Infiltrates US and European Energy Firms*

- **Link:** https://www.bleepingcomputer.com/news/security/sabotage-warning-issued-on-hackers-hiding-deep-inside-energy-sector /

- **Summary: September 2017:** The Dragonfly group infiltrated several U.S. and European energy firms, positioning themselves to potentially sabotage critical infrastructure. They used common computer management tools and mundane malware, shifting focus from learning about energy facilities to gaining access to operational systems. This attack raised concerns about the group's ability to control key SCADA equipment and other operational systems.

2. Attacks on IT

Title: *EDP Ransomware Attack*

- **Link:** https://www.bleepingcomputer.com/news/security/edp-energy-giant-confirms-ragnar-locker-ransomware-attack/

- **Summary: April 2020:** The Portuguese energy giant EDP was attacked by the Ragnar Locker ransomware group, leading to unauthorized access and data theft. The attackers demanded a ransom of over $10 million. EDP implemented enhanced security measures and involved law enforcement authorities to investigate the breach and prevent future incidents.

Title: Enel Group Ransomware Attack

- **Link:** https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/

- **Summary: October 2020:** Enel Group, a multinational energy company, was hit by the Netwalker ransomware group, demanding $14 million. The attackers threatened to leak stolen data to pressure Enel into paying the ransom. This incident highlighted the persistent threat of ransomware to large corporations and the significant financial and operational risks involved.

Title: *Shell Data Breach*

- **Link:** https://www.bleepingcomputer.com/news/security/energy-giant-shell-discloses-data-breach-after-accellion-hack/
- **Summary: March 2021:** Shell disclosed a data breach after attackers compromised its secure file-sharing system, affecting personal data and information from Shell companies and stakeholders. The Clop ransomware gang and FIN11 were identified as the groups behind the attack, exploiting a zero-day vulnerability in the Accellion File Transfer Appliance (FTA).

Title*: Suncor Energy's Petro-Canada Subsidiary Breach*

- **Link:** https://www.cybersecuritydive.com/news/suncor-hackers-breached-petro-canada-customer-data/685365/
- **Summary: June 2023:** Suncor Energy confirmed a cybersecurity breach affecting its Petro-Canada subsidiary. Hackers accessed basic information of Petro-Points members, disrupting credit and debit card purchases and car wash services.

Title*: Schneider Electric Ransomware Attack*

- **Link:** https://www.bleepingcomputer.com/news/security/energy-giant-schneider-electric-hit-by-cactus-ransomware-attack/
- **Summary: January 2024:** Schneider Electric was hit by the Cactus ransomware gang, disrupting its Resource Advisor cloud platform and stealing sensitive data. The attack highlighted the significant threat posed by ransomware to critical infrastructure and the importance of robust cybersecurity measures.

Title: *Schneider Electric Developer Platform Breach*

- **Link:** https://www.bleepingcomputer.com/news/security/schneider-electric-confirms-dev-platform-breach-after-hacker-steals-data/
- **Summary: November 2024:** Schneider Electric confirmed a breach of its developer platform by the Hellcat ransomware gang, leading to the theft of 40GB of data. The attackers used exposed credentials to access the server and demanded $125,000 to prevent the data from being leaked.

Title: *X_Trader Supply Chain Attack*

- **Link:** https://www.bleepingcomputer.com/news/security/critical-infrastructure-also-hit-by-supply-chain-attack-behind-3cx-breach/
- **Summary: April 2023:** North Korean-backed threat group used a trojanized installer for X_Trader software to deploy malware, impacting critical infrastructure organizations in the U.S. and Europe. The attack highlighted the risks associated with supply chain vulnerabilities and the need for robust cybersecurity measures.

Title: *Clop Ransomware Attack on Siemens Energy*

- **Link:** https://www.bleepingcomputer.com/news/security/siemens-energy-confirms-data-breach-after-moveit-data-theft-attack/
- **Summary: June 2023:** Siemens Energy confirmed a data breach from Clop ransomware attacks exploiting a MOVEit Transfer vulnerability. While data was stolen, no critical information was compromised, and business operations remained unaffected. This incident is part of a broader wave of Clop attacks affecting numerous organizations.

Title: *Darkside Ransomware Attack on Brazilian Utilities*

- **Link:** https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/
- **Summary: February 2021:** Eletrobras and Copel, major Brazilian utilities, suffered ransomware attacks by Darkside. The attacks led to data theft and temporary suspension of some operations, highlighting the significant threat ransomware poses to critical infrastructure and the importance of robust cybersecurity measures.

H. Risk Scope

SoCalGas and SDG&E's Cybersecurity Risk analysis considers the scope noted in Table 1 below.

Table 1
Cybersecurity Risk Scope

	Cybersecurity Risk
In-Scope:	The scope of this risk includes gas and electric control systems, all company data and information systems, operational technology systems, and related processes.

I. Data Sources Used to Quantify Risk Estimates[5]

SoCalGas and SDG&E utilized internal data sources to determine a Cybersecurity Risk Pre-Mitigation Risk Value and calculate risk reduction estimates for mitigation activities (which enables estimation of Post Mitigation Monetized Risk Values and Cost Benefit Ratios). Where internal data is deemed insufficient, supplemental industry or national data is used, as appropriate and adjusted to account for risk characteristics associated with the Companies' specific operating locations and service territories. For example, certain types of incident events have not occurred within the SoCalGas and SDG&E service territories. Expanding the quantitative data sources to include industry data where such incidents have been recorded is appropriate to establish a baseline of risk and risk addressed by mitigative activities. Attachment B provides additional information regarding these data resources.

II. RISK ASSESSMENT

In accordance with Commission guidance, this section provides a qualitative description of the Cybersecurity Risk, including a risk Bow Tie, which delineates potential Drivers/Triggers and Potential Consequences, followed by a description of the Tranches determined for this risk.

A. Risk Selection

The Cybersecurity Risk was included as a risk in SoCalGas's and SDG&E's 2021 RAMP and was also included in the Companies' 2022, 2023, and 2024 Enterprise Risk Registries (ERR).[6] SoCalGas's and SDG&E's ERR evaluation and selection process is summarized in Chapter RAMP-2, Enterprise Risk Management Framework and in Chapter RAMP-3 Risk Quantification Framework.

SoCalGas and SDG&E selected this risk in accordance with the RDF Row 9.[7] Specifically SoCalGas and SDG&E assessed the top risks from the Companies' 2024 ERRs based on the Consequence of a Risk Event (CoRE) Safety attribute. The Cybersecurity Risk was among the risks presented in SoCalGas's and SDG&E's list of Preliminary 2025 RAMP Risks

[5] Copies and/or links to these data resources are provided in the workpapers served with this Report on May 15, 2025.

[6] In the 2021 RAMP Report this risk was called "(Chapter SCG/SDG&E-Risk-6) Cybersecurity." The risk definition and elements are unchanged.

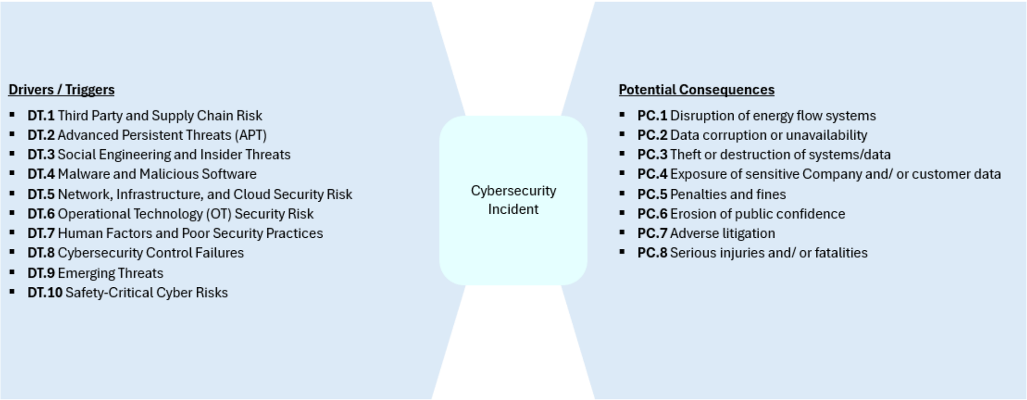
[7] D.24-05-064, RDF Row 9 states that risks to be included in the RAMP Report, at minimum, are those identified in the Company's ERR comprising "the top 40% of ERR risks with a Safety Risk Value greater than zero dollars."

on December 17, 2024 at a Pre-Filing Workshop. Cybersecurity was selected electively, as it did not qualify based on the Safety risk attribute alone. At the pre-filing workshop, no party expressed opposition to inclusion of this risk in SoCalGas's or SDG&E's 2025 RAMP Reports.

B. Risk Bow Tie

In accordance with Commission requirements, this section describes the risk Bow Tie, possible Drivers, Potential Consequences, and a mapping of the elements in the Bow Tie to the mitigation(s) that addresses it.[8] As illustrated in the risk Bow Tie shown below in Figure 1, the Risk Event (center of the Bow Tie) is a Cybersecurity event, the left side of the Bow Tie illustrates Drivers/Triggers that could lead to a Cybersecurity event, and the right side shows the Potential Consequences of a Cybersecurity event. SoCalGas and SDG&E applied this framework to identify and summarize the information provided in Figure 1. A mapping of each mitigation to the addressed elements of the risk Bow Tie is provided in Attachment C.

Figure 1
Cybersecurity Risk: Risk Bow Tie



Drivers / Triggers

- **DT.1** Third Party and Supply Chain Risk
- **DT.2** Advanced Persistent Threats (APT)
- **DT.3** Social Engineering and Insider Threats
- **DT.4** Malware and Malicious Software
- **DT.5** Network, Infrastructure, and Cloud Security Risk
- **DT.6** Operational Technology (OT) Security Risk
- **DT.7** Human Factors and Poor Security Practices
- **DT.8** Cybersecurity Control Failures
- **DT.9** Emerging Threats
- **DT.10** Safety-Critical Cyber Risks

Cybersecurity Incident

Potential Consequences

- **PC.1** Disruption of energy flow systems
- **PC.2** Data corruption or unavailability
- **PC.3** Theft or destruction of systems/data
- **PC.4** Exposure of sensitive Company and/ or customer data
- **PC.5** Penalties and fines
- **PC.6** Erosion of public confidence
- **PC.7** Adverse litigation
- **PC.8** Serious injuries and/ or fatalities

C. Potential Risk Event Drivers/Triggers[9]

When performing a risk assessment for the Cybersecurity Risk, SoCalGas and SDG&E identify potential leading indicators, referred to as Drivers or Triggers, that reflect current and/or forecasted conditions and may include both external actions as well as characteristics inherent to

[8] D.24-05-064, RDF Row 15.

[9] An indication that a risk could occur. It does not reflect actual or threatened conditions.

the asset.[10] These Bow Tie Drivers/Triggers inform the Likelihood of a Risk Event (LoRE) component of the risk value. These include:

- **DT.1: Third Party and Supply Chain Risk**: Risks introduced through external partners, vendors, and supply chains are common and can have widespread impacts.
- **DT.2: Advanced Persistent Threats (APT)**: Highly sophisticated and targeted attacks that can cause significant damage over a prolonged period.
- **DT.3: Social Engineering and Insider Threats**: Human factors often present the greatest risk, as they can bypass technical controls through manipulation or exploitation.
- **DT.4: Malware and Malicious Software**: Widespread and varied, malware can cause extensive damage, from data breaches to operational disruptions.
- **DT.5: Network, Infrastructure, and Cloud Security Risk**: Compromises in these areas can lead to widespread access and control issues, affecting multiple systems and data.
- **DT.6: Operational Technology (OT) Security Risk**: Risks in OT environments can lead to significant operational disruptions, especially in critical infrastructure sectors.
- **DT.7: Human Factors and Poor Security Practices**: Inadequate security behaviors, policies, and mistakes by employees that can lead to security breaches.
- **DT.8: Cybersecurity Control Failures**: Failures or malfunctions in security controls, such as IDS/IPS, firewalls, and other security tools, that can lead to missed alerts and undetected intrusions.
- **DT.9: Emerging Threats**: New and evolving threats can be unpredictable and may not be fully understood or mitigated by existing defenses.
- **DT.10: Safety-Critical Cyber Risks**: Inadequate cybersecurity measures in safety-critical systems and processes, such as job site safety plans and job safety analysis, which can lead to vulnerabilities that compromise both safety and security.

D. Potential Consequences of Risk Event (CoRE)

Potential Consequences are listed to the right side of the risk Bow Tie. SoCalGas and SDG&E identify the Potential Consequences of this risk by analyzing internal data sources where available, industry data, and subject matter expertise (SME).[11] These Bow Tie Consequences inform the CoRE component of the risk value. If one or more of the Drivers listed

[10] D.24-05-064, RDF Row 10-11.

[11] D.24-05-064, RDF Rows 10-11.

above were to result in an incident, the Potential Consequences, in a plausible worst-case scenario, could include:

- PC.1 - Disruption of energy flow systems
- PC.2 - Data corruption or unavailability
- PC.3 - Theft or destruction of systems/data
- PC.4 - Exposure of sensitive Company and/ or customer data
- PC.5 - Penalties and fines
- PC.6 - Erosion of public confidence
- PC.7 - Adverse litigation
- PC.8 - Serious injuries and/ or fatalities

While this risk chapter primarily addresses internal threats to the companies and their customers, a large-scale disruption in the Companies' ability to deliver energy could also pose significant societal impacts, particularly to public health and safety, including:

- Economic disruption
- Infrastructure and transportation system failures, including critical facilities such as hospitals or water treatment plants
- Heightened vulnerability of at-risk populations

These Potential Consequences were used by SoCalGas and SDG&E in the scoring of the Cybersecurity Risk during the development of their 2024 ERRs.

E. Evolution of Its Drivers and Consequences

As specified in the Phase 3 Decision,[12] the following changes to the previous ERR and/or the 2021 RAMP include:

1. Changes to Drivers/Triggers of the Risk Bow Tie

- **DT.1: Third Party and Supply Chain Risk**: Risks introduced through external partners, vendors, and supply chains are common and can have widespread impacts.
- *This driver was not included in the 2021 RAMP. Given the heightened activity from this threat vector, third party and supply chain risk was included as an event Driver/Trigger.*
- **DT.2: Advanced Persistent Threats (APTs)**: Highly sophisticated and targeted attacks that can cause significant damage over a prolonged period.

[12] D.24-05-064, RDF Row 8.

- *This driver was not included in the 2021 RAMP. APTs has been added as a Driver/Trigger for a cybersecurity incident because of their highly sophisticated and targeted nature. APTs are capable of causing significant damage over extended periods, making them particularly dangerous.*
- **DT.3: Social Engineering and Insider Threats**: Human factors often present the greatest risk, as they can bypass technical controls through manipulation or exploitation.
- *This driver was not included in the 2021 RAMP. Although Social Engineering and Insider Threats encompass various other Drivers and Triggers, such as human error, malicious software, access failures, and cyber control failures, it was added as a Driver/Trigger because human factors often present the greatest risk to security. Phishing and other social engineering attacks are among the most common and effective attack techniques.*
- **DT.4: Malware and Malicious Software**: Widespread and varied, malware can cause extensive damage, from data breaches to operational disruptions.
- *Two Drivers from the 2021 RAMP were merged to form this driver: (Manipulated data or integrity failure)* Any unintended changes to data as the result of a storage, retrieval or processing operation, including malicious intent, unexpected hardware failure, and human error.

  and
- *(Malicious software intrusion)* Any malicious program or code that is harmful to systems. For example, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations.
- **DT.5: Network, Infrastructure, and Cloud Security Risk**: Compromises in these areas can lead to widespread access and control issues, affecting multiple systems and data.
- *Two Drivers from the 2021 RAMP were merged to form this driver:* (*Infrastructure or availability failure*) An unplanned, severe, extensive and/or large-scale system outage caused by a cybersecurity- related event or incident.

  and
- *RAMP 2021 (Equipment loss or theft)* A type of data breach where there is a loss of a laptop, mobile device, or storage device such as backup tapes, hard drives, and flash drives whether by accidental loss or through malicious intent.
- **DT.6: Operational Technology (OT) Security Risk**: Risks in OT environments can lead to significant operational disruptions, especially in critical infrastructure sectors.
- *This driver was changed from the 2021 RAMP, which had: (Operational system failure)* A system failure occurring due to a cybersecurity event/incident, causing the system to freeze, reboot, function counter to its design or stop functioning.

- **DT.7: Human Factors and Poor Security Practices**: Inadequate security behaviors, policies, and mistakes by employees that can lead to security breaches.
- *Two Drivers from the 2021 RAMP were merged to form this driver: (Access control or confidentiality failure)* Inability to effectively perform identification, authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors.
- *RAMP 2021 (Human error (e.g., clicking on a phishing email)* An accidental cybersecurity event/incident conducted by a human.
- **DT.8: Cybersecurity Control Failures**: Failures or malfunctions in security controls, such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), firewalls, and other security tools, that can lead to missed alerts and undetected intrusions.
- *This driver was changed from the 2021 RAMP, which had: (Cybersecurity control failure)* A general failure of a cybersecurity control(s). *E.g.*, a vulnerability scanner ceases functioning, allowing an exploitable vulnerability to go unnoticed in the environment.
- **DT.9: Emerging Threats**: New and evolving threats can be unpredictable and may not be fully understood or mitigated by existing defenses.
- *This driver was not included in the 2021 RAMP. Emerging Threats was added as a Driver/Trigger for a cybersecurity incident because these threats are new, evolving, and often unpredictable. Examples of emerging threats include use of AI and quantum computing.*
- **DT.10: Safety-Critical Cyber Risks**: Inadequate cybersecurity measures in safety-critical systems and processes, such as job site safety plans and job safety analysis, which can lead to vulnerabilities that compromise both safety and security.
- *This driver was not included in the 2021 RAMP. Safety-Critical Cyber Risks was added as a new Driver/Trigger for a Cybersecurity Risk because inadequate cybersecurity in safety-critical systems can lead to vulnerabilities that compromise both safety and security, potentially causing accidents, data breaches, and operational disruptions.*

2. Changes to Potential Consequences of the Risk Bow Tie

- There were no changes to Potential Consequences.

F. Summary of Tranches

To determine groups of assets or systems with similar risk profiles, or Tranches, and in accordance with Row 14 of the RDF, SoCalGas and SDG&E applied the Homogeneous Tranching Methodology (HTM) as outlined in Chapter RAMP - 3: Risk Quantification Framework. As a result, the following classes, LoRE-CoRE pairs, and resulting number of Tranches were determined:

Table 2
Cybersecurity Risk Tranche Identification

Class	Number of LoRE-CoRE Pairs	Number of Resulting Tranches
Tier 1	1	1
Tier 2	1	1
Tier 3	1	1
Tier 4	1	1
TOTAL	**4**	**4**

Attachment D illustrates the derivation of the Tranches, as shown in Table 2 above, in accordance with the HTM. The classes were identified by SoCalGas and SDG&E as logical groups of assets and systems based on the Companies' operations. These classes also align risk treatments with asset risk profiles reflective of SoCalGas's and SDG&E's operations. More detailed Tranche information, including risk quantification by LoRE-CoRE pair, Tranche names, and mitigation associations (*i.e.*, cost mapping and risk reduction) to Tranches, is provided in workpapers.

III. PRE-MITIGATION RISK VALUE

In accordance with the RDF Row 19, Table 3 below provides the pre-mitigation risk values for Cybersecurity Risk. Further details, including pre-mitigation risk values by Tranche, are provided in workpapers. Explanations of the risk quantification methodology and other higher-level assumptions are provided in Chapter RAMP-3 Risk Quantification Framework.

Table 3
Cybersecurity Risk Monetized Risk Values
(Direct, in 2024 $ millions)

Company	LoRE	CoRE [Risk-Adjusted Attribute Values]			Total CoRE	Total Risk [LoRE x Total CoRE]
		Safety	Reliability	Financial		
SoCalGas	0.59	$0.003	$215.70	$4.73	$220.44	$129.02
SDG&E	0.51	$0.69	$3,466.54	$8.14	$3,475.37	$1,775.20
SoCalGas and SDG&E[13]	1.10	$0.32	$1,730.65	$6.32	$1,737.29	$1,904.22

A. Risk Value Methodology

SoCalGas's and SDG&E's risk modeling for the Cybersecurity Risk follows RDF guidance[14] for implementing a Cost Benefit Approach, as described below:

- **Cost Benefit Approach Principle 1 – Attribute Hierarchy (RDF Row 2):** Cybersecurity Risk is quantified in a combined attribute hierarchy as shown in Table 3 above, such that Safety, Reliability, and Financial are presented based on available, observable, and measurable data.
- **Cost Benefit Approach Principle 2 – Measured Observations (RDF Row 3):** The Cybersecurity Risk used observable and measurable data in the estimation of CoRE values. SoCalGas and SDG&E utilized a combination of internal and external data to estimate the consequence in terms of natural units (*e.g.*, fatalities, serious injuries, meters out, and customer minutes interrupted [CMI]) that occur as the result of a risk event.
- **Cost Benefit Approach Principle 3 – Comparison (RDF Row 4):** Cybersecurity Risk utilized proxy data from various sources including, but not limited to, Business Continuity Institute, IBISWorld, NetDiligence Cyber Claims Study, IBM Cost of a Data Breach (2024), Department of Energy, and National Institute of Health, to estimate the financial impacts, safety, and reliability impacts of cybersecurity incidents. Reference materials are further detailed in Attachment B.
- **Cost Benefit Approach Principle 4 - Risk Assessment (RDF Row 5):** Data sources used for Cybersecurity Risk – as described in the preceding paragraphs – were sufficient to model probability distributions for use in estimating risk values.
- **Cost Benefit Approach Principle 5 – Monetized Levels of Attributes (RDF Row 6):** In accordance with D.22-12-027 and D.24-05-064, RDF Row 6,

[13] SoCalGas and SDG&E individual Company risk values are provided for informational purposes only. All mitigation benefits and the resulting cost-benefit ratios are assessed using the Companies' combined risk scores. *See* Cybersecurity workpapers for more information.

[14] D.24-05-064, RDF Rows 2-7.

SoCalGas and SDG&E used a California-adjusted Department of Transportation monetized equivalent to calculate the Safety CoRE attribute at a monetized equivalent of $16.2 million per fatality, $4.1 million per serious injury, and $49 thousand for minor injury;[15] the Electric Reliability CoRE attribute is valued at a monetized equivalent of $3.76 per CMI; Gas Reliability is valued at a monetized equivalent of $3,868 per gas meter outage; and the Financial CoRE attribute is valued at $1 per dollar.[16]

- **Cost Benefit Approach Principle 6 – Adjusted Attribute Level (RDF Row 7):**

Table 4
Cybersecurity Risk Scaled vs Unscaled Value by CoRE Attribute
(Direct, in 2024 $ millions)

SoCalGas	**Safety**	**Reliability**	**Financial**	**Total**
Unscaled Risk Value	$0.002	$18.84	$2.29	$21.13
Scaled Risk Value	$0.002	$126.25	$2.77	$129.02
SDG&E	**Safety**	**Reliability**	**Financial**	**Total**
Unscaled Risk Value	$0.34	$139.09	$2.80	$142.23
Scaled Risk Value	$0.35	$1,770.69	$4.16	$1,775.20
SoCalGas and SDG&E	**Safety**	**Reliability**	**Financial**	**Total**
Unscaled Risk Value	$0.34	$157.93	$5.09	$163.36
Scaled Risk Value	$0.35	$1,896.94	$6.93	$1,904.22

Table 4 depicts the results of applying the risk scaling methodology described in Chapter RAMP-3 to the CoRE attributes for the Cybersecurity Risk. For the Cybersecurity Risk it is driven by the Reliability and Financial attributes due to the increase in the risk of Cybersecurity. Further information regarding the risk scaling function, including the risk scaling factor and the loss threshold at which the risk scaling factor begins to apply, is provided in Chapter-RAMP-3.

Further information regarding SoCalGas's and SDG&E's quantitative risk analyses, including raw data, calculations, and technical references are provided in workpapers.

IV. 2024-2031 CONTROL & MITIGATION PLAN

This section identifies and describes the controls and mitigations comprising the portfolio of mitigations for Cybersecurity Risk and reflects changes expected to occur from the last year of recorded costs at the time of filing this RAMP Report (2024) through the 2028 GRC cycle (2031). For clarity, a current activity that is included in the plan may be referred to as either a

[15] *See* D.22-12-027 at 35 ("We adopt Staff's recommendation to require a dollar valuation of the Safety Attribute in the Cost-Benefit Approach in the RDF using the DOT VSL as the standard value.").

[16] *See* Chapter RAMP-3: Risk Quantification Framework, Section II.

control and/or a mitigation. Table 5 below shows which control activities are in place in 2024 and which are expected to be on-going, completed, or new during the 2025-2031 periods. Because the TY 2024 GRC proceeding established rates through 2027,[17] information through 2027 is calculated as part of the baseline risk, in accordance with D.21-11-009.[18] For the TY 2028 GRC, SoCalGas and SDG&E calculated CBRs beginning with TY 2028 and for each Post-Test Year (PTY) (2029, 2030, and 2031).[19]

Table 5
Cybersecurity Risk 2024-2031 Control and Mitigation Plan Summary

ID	Control/Mitigation Description	2024 Control	2025-2031 Plan
C801	Perimeter Defenses	X	Ongoing
C802	Internal Defenses	X	Ongoing
C803	Sensitive Data Protection	X	Ongoing
C804	Operational Technology (OT) Cybersecurity	X	Ongoing
C805	IT Infrastructure Modernization	X	Ongoing

***Bold** indicates this control/mitigation includes mandated programs/activities.*

A. Control Programs

In accordance with Commission guidance, this section "[d]escribe[s] the controls or mitigations currently in place"[20] (*i.e.* activities in this section were in place as of December 31, 2024). Controls that will continue as part of the risk mitigation plan are identified in Table 5 above. The controls for Cybersecurity are evaluated at the program level due to the availability of data, the rapidly changing threats, and applicable counter measures. As mentioned in the Risk Overview section above, sharing specific details of the individual risk mitigation activity can provide adversaries crucial information that could aid their ability to disrupt Company systems. Therefore, the level of granularity for quantifying Cost-Benefit Ratios is currently at the operational program level (*i.e.*, Perimeter Defenses, Internal Defenses, Sensitive Data Protection, OT Cybersecurity, and IT Infrastructure Modernization), rather than each individual risk mitigation activity for the Cybersecurity Risk.

[17] *See* D.24-12-074.

[18] *See* D.21-11-009 at 136, Conclusion of Law 7 (providing a definition for "baselines" and "baseline risk").

[19] In the TY 2028 GRC, the last year of recorded costs, or base year, will be 2025. SoCalGas and SDG&E will forecast information for 2026 through 2031, in accordance with the Rate Case Plan.

[20] D.18-12-014 at 33.

- **C801: Perimeter Defenses**

The Perimeter Defenses program includes activities that the Companies take to protect the external access points of their internal information technology systems. Perimeter Defenses are designed to prevent attacks, protect the integrity of, and detect unauthorized access to the Companies' internal information technology systems. The information technology environment includes the entire business technology system, including email, information storage, billing and customer records among others. The operational technology environment also uses Perimeter Defenses to protect operational technology assets.

A robust set of controls at the perimeter of corporate systems contributes to the Companies' *defense-in-depth* strategy. The purpose of the defense-in-depth strategy is to manage risk with diverse defenses so that if one layer of defense turns out to be inadequate, the additional layers of defense will prevent and detect further impacts and/or a potential breach.

Perimeter Defenses are an important component of defense-in-depth but can only reduce the probability of an adversary having unauthorized access to internal systems and data (*i.e.*, the LoRE). This control includes enhancements to firewalls and other intrusion protection measures to maintain the risk at the current manageable level and keep up with the increasing potential threats to the Companies' perimeter.

Perimeter Defenses reduce the frequency or probability of successful attacks. As a security strategy, it accomplishes this by limiting access to authorized users, reducing the likelihood that malicious code will enter the information technology environment, and delaying or frustrating potential attackers. This strategy also helps the Companies to understand the number of pathways into or out of the perimeter while simultaneously monitoring the perimeter in real time.

Accordingly, the Perimeter Defenses control addresses several Drivers/Triggers outlined above in Figure 1 including: DT.1: Third Party and Supply Chain Risk; DT.2: Advanced Persistent Threats (APT); DT.3: Social Engineering and Insider Threats; DT.4: Malware and Malicious Software; DT.5: Network, Infrastructure, and Cloud Security Risk; DT.6: Operational Technology (OT) Security Risk; DT.7: Human Factors and Poor Security Practices; DT.8: Cybersecurity Control Failures; DT.9: Emerging Threats; DT.10: Safety-Critical Cyber Risks; PC.1: Disruption of energy flow systems; PC.3: Theft or destruction of systems/data; PC.4:

Exposure of sensitive Company and/ or customer data; PC.5: Penalties and fines; PC.6: Erosion of public confidence; PC.8 Serious injuries and/ or fatalities.

Perimeter Defenses projects included within this control include:

- Network security and firewall infrastructure upgrades;
- Web Application Firewall Protection;
- Distributed Denial of Service Protection;
- Cloud application and infrastructure security;
- Endpoint monitoring and protection; and
- Perimeter Defense mechanisms.

- **C802: Internal Defenses**

Internal Defense program activities are designed to detect and prevent unauthorized users, those misusing authorized credentials, and malicious software (*i.e.*, malware) from propagating inside of the perimeter, moving within the IT system or into the OT system. Enhancements to the Companies' IT and OT systems' Access Management system reduces the risk to internal assets, systems, and the likelihood and impact of a Cybersecurity incident.

As another layer of *defense-in-depth*, the activities within this category include investments that directly reduce the risk to internal assets and information. The controls in this category are designed to detect unauthorized users from moving laterally or vertically within the IT system or into the OT system, in turn improving the ability to identify and respond to threats more quickly. The enhancements to the IT and OT systems' Access Management system allow the Companies to keep the current risk level steady.

Based on the foregoing, Internal Defenses address several Drivers/Triggers and Potential Consequences including: DT.2: Advanced Persistent Threats (APT); DT.3: Social Engineering and Insider Threats; DT.4: Malware and Malicious Software; DT.5: Network, Infrastructure, and Cloud Security Risk; DT.6: Operational Technology (OT) Security Risk; DT.7: Human Factors and Poor Security Practices; DT.8: Cybersecurity Control Failures; DT.9: Emerging Threats; DT.10: Safety-Critical Cyber Risks; PC.1: Disruption of energy flow systems; PC.2: Data corruption or unavailability; PC.3: Theft or destruction of systems/data; PC.4: Exposure of sensitive Company and/ or customer data; PC.5: Penalties and fines; PC.6: Erosion of public confidence; PC.7: Adverse litigation; PC.8: Serious injuries and/ or fatalities.

Internal Defenses projects presented in this control include:

- Endpoint Security Monitoring;
- Threat and Vulnerability Management;
- Third Party External Privileged Access Management;
- Data Loss Prevention (DLP);
- Identity & Access Management Enhancements;
- Cloud Access Security;
- Attack Surface Management; and
- Security Conformance Monitoring and Automation.

- **C803: Sensitive Data Protection**

Sensitive Data Protection is a core component of the Companies' *defense-in-depth* strategy for Cybersecurity Risk. The Sensitive Data Protection projects outlined below enhance technology to reduce the risk of unauthorized access. The Sensitive Data Protection control helps reduce the risk of unauthorized access to the Companies' information by understanding where sensitive data is stored, how it is transmitted, and how it is used. This helps to further protect customer and Company information. The activities for this control help the Companies continue to prudently manage sensitive data.

Sensitive Data Protection addresses several Drivers/Triggers and Potential Consequences including: DT.1: Third Party and Supply Chain Risk; DT.2: Advanced Persistent Threats (APT); DT.3: Social Engineering and Insider Threats; DT.4: Malware and Malicious Software; DT.7: Human Factors and Poor Security Practices; DT.8: Cybersecurity Control Failures; DT.9: Emerging Threats; PC.2: Data corruption or unavailability; PC.3: Theft or destruction of systems/data; PC.4: Exposure of sensitive Company and/ or customer data; PC.5: Penalties and fines; PC.6: Erosion of public confidence; PC.7: Adverse litigation.

The Companies' current control activities target sensitive data within information technology systems, including laptops and other mobile computing devices.

Sensitive Data Protection controls are designed to include:

- Identity Access Management Enhancements;
- Data Loss Prevention & Enhancements;
- Forensics Infrastructure Enhancements;
- Mobile Device Security; and

- Data Crawler Technology.

- **C804: Operational Technology (OT) Cybersecurity**

The OT Cybersecurity program focuses on securing the electric and gas control systems for the Companies. OT environments enable critical business functions, including safe and reliable energy delivery to customers throughout the service territory. OT Cybersecurity requires a specialized approach to balance operational needs with Cybersecurity Risk. Improving asset management helps identify unauthorized systems, which could potentially be a source of an attack. Anomaly detection, endpoint detection, and security event monitoring improve visibility into the OT environment, which allows for faster response and remediation. Enhanced secure access technologies help reduce the risk of unauthorized access. These risk mitigation activities strengthen the Companies' capabilities by securing the foundation of OT security. Additionally, these enhancements are necessary to maintain a secure OT system and mitigate the increasing potential threat to that critical system.

This specialized OT Cybersecurity addresses several Drivers/Triggers and Potential Consequences including: DT.1: Third Party and Supply Chain Risk; DT.2: Advanced Persistent Threats (APT); DT.3: Social Engineering and Insider Threats; DT.4: Malware and Malicious Software; DT.5: Network, Infrastructure, and Cloud Security Risk; DT.6: Operational Technology (OT) Security Risk; DT.7: Human Factors and Poor Security Practices; DT.8: Cybersecurity Control Failures; DT.9: Emerging Threats; DT.10: Safety-Critical Cyber Risks; PC.1: Disruption of energy flow systems; PC.2: Data corruption or unavailability; PC.3: Theft or destruction of systems/data; PC.5: Penalties and fines; PC.6: Erosion of public confidence; PC.8: Serious injuries and/ or fatalities.

The Companies' Cybersecurity program prioritizes OT controls, including: the management of its existing technology assets, improving threat intelligence and vulnerability management, and securing the communication infrastructure. The Companies are focused on maintaining a secure operational environment to support safe, reliable gas and electric systems and service.

The Companies' OT Cybersecurity projects presented in this control include:

- OT network security enhancements;
- OT asset management;
- OT sensor deployment and monitoring;

- OT vulnerability management; and
- OT security platform enhancements.
- **C805**: **IT Infrastructure Modernization**

One of the fundamental practices that supports a strong Cybersecurity program is the refresh of technology, both hardware and software, at regular intervals, to minimize risks posed by obsolete technologies that lead to security risks. This is frequently referred to as "Foundational Technology Systems Lifecycle Management."

Technology lifecycles are short and require frequent upgrades to meet modern security standards and capabilities. In addition to technology obsolescence, this approach also addresses security obsolescence. Security obsolescence refers to cybersecurity tools and processes that are no longer effective or potentially could create new vulnerabilities.

Vulnerabilities inherent in legacy technology can provide a foothold for entry or movement within the Companies' environment. Failure to invest in modern technologies could degrade the value of modern investments due to compatibility restrictions. Replacing legacy technology is a necessary method of managing Cybersecurity Risk.

In addition, there are fundamental control activities required to support and effectively manage the Cybersecurity capabilities listed in the previous sections. These fundamental activities referenced in the Operations & Maintenance (O&M) forecast (*see* Section E below) support the capital investments.

This chapter is intended to address the Company's core cybersecurity investments; it does not encompass every capital or expense item that may mitigate cybersecurity risk (for example, certain electric-operations sensor or OT upgrade projects are accounted for under their respective risk domains). Because many cyber-related expenditures overlap with other functions, the RAMP values attributed to this section are comparatively lower. Nevertheless, each investment described herein directly contributes to the reduction of enterprise risk, rather than serving solely as an infrastructural prerequisite.

The following controls are representative, but not exhaustive, of the core measures through which the Company reduces cybersecurity risk:

- Security Policy Framework
- Risk Management and Assessment
- Cybersecurity Awareness and Training

- Security Assessment and Vulnerability Management
- Asset Management
- Protective Technologies (Network, User, Application)
- System Authentication Services (*e.g.*, public key infrastructure (PKI))
- Security Operations Center (SOC), which:
    - Continuously monitors security-related events across systems and applications;
    - Detects anomalies and escalates confirmed security incidents;
    - Investigates and responds to incidents; and
    - Conducts regular exercises and drills to validate incident-response capabilities.

IT Infrastructure Modernization addresses several Drivers/Triggers and Potential Consequences outlined above in Figure 1 including: DT.2: Advanced Persistent Threats (APT); DT.3: Social Engineering and Insider Threats; DT.4: Malware and Malicious Software; DT.5: Network, Infrastructure, and Cloud Security Risk; DT.9: Emerging Threats; PC.2: Data corruption or unavailability; PC.4: Exposure of sensitive Company and/ or customer data; PC.6: Erosion of public confidence; PC.8: Serious injuries and/ or fatalities.

The projects presented in this control include:

- Technology refreshes, including, but not limited to:
    - Infrastructure;
    - Operating systems;
    - Middleware; and
    - Applications.
- System maintenance to confirm continued secure configurations, patching, upgrading, among others.
- Use of effective architecture and other mechanisms to confirm high availability and service continuity for critical systems.

B. Changes from 2024 Controls

SoCalGas and SDG&E plan to continue each of the existing controls discussed above, and reflected in Table 5, through the 2025-2031 period. The identified Drivers, Consequences, and controls categories do not change significantly,[21] however, as discussed above, the specific mitigation projects within the controls must continually change and evolve as existing threats evolve and become more sophisticated and as new Cybersecurity threats emerge.

C. Mitigation Programs

SoCalGas and SDG&E do not currently foresee implementing new mitigations not described above during the 2025-2031 period. As noted above in the Risk Overview section, gaining information about the Companies' control and mitigation plan for Cybersecurity Risk could be useful to an adversary therefore it is presented at a summary level. That is, the mitigations represent broad categories of controls rather than individual projects to avoid disclosing information to adversaries. The broad control categories are intended to capture emerging Cybersecurity threats, and the projects within the existing controls continually change and evolve in response to new and changing threats.

D. Climate Change Adaptation

In assessing Cybersecurity Risk, controls and/or mitigations that address climate adaptation planning were determined to be inapplicable (from the perspective of climate exposure, asset sensitivity, and asset adaptive capacity). A list of climate-relevant controls and mitigations is provided in Volume 1, Chapter RAMP-5: Climate Change Adaptation.

E. Foundational Programs

Foundational Programs are "[i]nitiatives that support or enable two or more Mitigation programs or two or more Risks but do not directly reduce the Consequences or reduce the Likelihood of safety Risk Events." [22] For the Cybersecurity Risk there are no activities that meet this definition of a Foundational Program.

[21] In its 2021 RAMP filing, SoCalGas and SDG&E referred to the IT Infrastructure Modernization control as Obsolete IT Infrastructure and Asset Replacement. The controls are substantively the same.

[22] D.24-05-064, Appendix A at A-4.

F. Estimates of Costs, Units, and Cost-Benefit Ratios (CBRs)

The tables in this section provide a quantitative summary of the risk control and mitigation plan for Cybersecurity Risk, including the associated costs,[23] units, and CBRs. Additional information by Tranche is provided in workpapers. The costs shown are estimated using assumptions provided by SMEs and available data. In compliance with the Phase 3 Decision,[24] for each enterprise risk, SoCalGas and SDG&E use actual results and industry data and when that is not available, supplement the data with SME input. Additional details regarding the data and expertise relied upon in developing these estimates is provided in Attachment B.

Table 6
SoCalGas Cybersecurity Risk Control and Mitigation Plan

Recorded and Forecast Costs Summary (Direct, in 2024 $ thousands)							
Control/Mitigation		**Adjusted Recorded**		**Forecast**			
ID	**Name**	**2024 Capital**	**2024 O&M**	**2028 O&M**	**2025-2028 Capital**	**PTY Capital**	**PTY O&M**
C801	Perimeter Defenses	1,991	3,851	4,091	79,297	29,174	12,993
C802	Internal Defenses	11,879	8,625	8,982	62,665	66,759	26,946
C803	Sensitive Data Protection	2,998	0	0	5,400	9,720	0
C804	Operational Technology (OT) Cybersecurity	338	0	0	18,449	13,778	0
C805	IT Infrastructure Modernization	9,113	0	0	12,299	9,929	0
Total		**26,319**	**12,476**	**13,073**	**178,110**	**129,360**	**39,939**

Bold *indicates this control/mitigation includes mandated programs/activities.*

[23] Cybersecurity Risk is centrally managed and includes Shared Services and Shared Assets that are allocated and billed to the entity or entities receiving those services or using the asset. Shared Assets are recorded on the financial records of the Company that receives the most service or use from the asset. In this 2025 RAMP Application costs are presented where they are incurred, before allocations.

[24] D.24-05-064, RDF Row 10.

Table 7
SDG&E Cybersecurity Risk Control and Mitigation Plan

Recorded and Forecast Costs Summary (Direct, in 2024 $ thousands)							
Control/Mitigation		**Adjusted Recorded**		**Forecast**			
ID	**Name**	**2024 Capital**	**2024 O&M**	**2028 O&M**	**2025-2028 Capital**	**PTY Capital**	**PTY O&M**
C801	Perimeter Defenses	0	1,103	1,346	0	0	4,038
C802	Internal Defenses	116	10,284	10,724	2,789	1,458	31,722
C803	Sensitive Data Protection	0	527	526	0	0	1,578
C804	Operational Technology (OT) Cybersecurity	3,897	0	0	14,764	11,100	0
C805	IT Infrastructure Modernization	0	0	0	18,900	0	0
Total		**4,013**	**11,914**	**12,596**	**36,453**	**12,558**	**37,338**

***Bold** indicates this control/mitigation includes mandated programs/activities.*

Table 8
SoCalGas Cybersecurity Risk Control & Mitigation Plan

Recorded and Forecast Units[25] Summary							
Control/Mitigation		**Recorded Units**		**Forecast Units**			
ID	**Name**	**2024 Capital**	**2024 O&M**	**2028 O&M**	**2025-2028 Capital**	**PTY Capital**	**PTY O&M**
C801	Perimeter Defenses	25,000	12	14	100,000	75,000	42
C802	Internal Defenses	25,000	12	15	100,000	75,000	45
C803	Sensitive Data Protection	25,000	0	0	50,000	50,000	0
C804	Operational Technology (OT) Cybersecurity	25,000	0	0	100,000	75,000	0
C805	IT Infrastructure Modernization	25,000	0	0	100,000	75,000	0

***Bold** indicates this control/mitigation includes mandated programs/activities.*

[25] For capital, the unit of measure is Users Protected, for O&M, the unit of measure is Full-Time Equivalents (FTEs).

Table 9
SDG&E Cybersecurity Risk Control & Mitigation Plan

Recorded and Forecast Units[26] Summary							
Control/Mitigation		**Recorded Units**		**Forecast Units**			
ID	**Name**	**2024 Capital**	**2024 O&M**	**2028 O&M**	**2025-2028 Capital**	**PTY Capital**	**PTY O&M**
C801	Perimeter Defenses	0	5	6	0	0	18
C802	Internal Defenses	25,000	29	30	50,000	25,000	90
C803	Sensitive Data Protection	0	3	3	0	0	9
C804	Operational Technology (OT) Cybersecurity	25,000	0	0	100,000	75,000	0
C805	IT Infrastructure Modernization	0	0	0	50,000	0	0

***Bold** indicates this control/mitigation includes mandated programs/activities.*

In Table 10 below, CBRs are presented in summary at the mitigation or control level for the TY 2028 GRC cycle.[27] CBRs are calculated based on scaled, expected values unless otherwise noted, and are calculated for each of the three required discount rates[28] in each year of the GRC cycle and for the Post-Test Years in aggregate (2029-2031). Costs and CBRs for each year of the GRC cycle and the aggregated years are provided in workpapers.

Table 10
Cybersecurity Risk Cost Benefit Ratio Results Summary
2028-2031
(Direct, in 2024 $ millions)

ID	Control/Mitigation Name	Capital (2028 – 2031)	O&M (2028 – 2031)	CBR (Societal)	CBR (Hybrid)	CBR (WACC)
C801	Perimeter Defenses	$58	$22	103.98	97.52	87.83
C802	Internal Defenses	$88	$79	33.71	32.54	29.31
C803	Sensitive Data Protection	$10	$2	236.70	227.09	204.55

[26] For capital, the unit of measure is Users Protected, for O&M, the unit of measure is Full-Time Equivalents (FTEs).

[27] A combined CBR for SoCalGas and SDG&E is presented for each mitigation or control. Cybersecurity Risk is managed centrally for the Companies.

[28] *See* Chapter RAMP-3 Risk Quantification Framework for definitions of discount rates, as ordered in the Phase 3 Decision.

ID	Control/Mitigation Name	Capital (2028 – 2031)	O&M (2028 – 2031)	CBR (Societal)	CBR (Hybrid)	CBR (WACC)
C804	Operational Technology (OT) Cybersecurity	$32	$0	220.11	213.21	192.03
C805	IT Infrastructure Modernization	$21	$0	197.04	182.04	163.97

***Bold** indicates this control/mitigation includes mandated programs/activities.*

Tranche-level CBRs by year and in aggregate for each mitigation are provided in workpapers.

V. ALTERNATIVE MITIGATIONS

Pursuant to D.14-12-025, D.16-08-018, and D.18-12-014[29] SoCalGas and SDG&E considered two alternatives to the Risk Mitigation Plan for Cybersecurity Risk. The risk mitigation plan for the Cybersecurity Risk is defined as the planned portfolio of control programs. Typically, analysis of alternatives occurs when designing the portfolio to obtain the best result or product for the cost. The alternatives analysis considers changes in risk reduction, cost, reasonableness, current conditions, modifications to the plan and constraints, such as budget and resources.

The Companies considered two alternative portfolios of mitigation activities in addition to the planned portfolio control program to address the Companies' Cybersecurity Risk. The alternative portfolios were analyzed in the context of CBRs, as outlined in the tables below.

For the alternative analysis, the Companies analyzed the effectiveness of three portfolios:

1. The risk mitigation plan for the Cybersecurity Risk (the Plan);
2. Alternative Portfolio 1; and
3. Alternative Portfolio 2.

To create these three different portfolios, the Companies first assessed the potential impact of each capital project under consideration, identifying each as high/medium/low impact based on several criteria:

- The project implementation's impact on the maturity of cybersecurity at the Companies;

[29] *See, e.g.,* D.18-12-014 at 33-35.

- The extent to which each project addresses recommendations from Critical Security Controls (CSC) 18,[30] ICS-CERT,[31] and other frameworks;
- The extent to which each project addresses threats to cybersecurity of high impact and likelihood;
- The effectiveness in mitigating a credible attack impacting safety, and;
- The urgency or time horizon for the project's implementation to assess how quickly a project needs to be completed or the specific timeframe within which it should be implemented. Projects with higher urgency or shorter time horizons are prioritized to address immediate cybersecurity threats and vulnerabilities.

After each project was tagged as high/medium/low impact, the following three portfolios were developed: The risk mitigation plan for the Cybersecurity Risk, Alternative Portfolio 1 and Alternative Portfolio 2.

A. The Risk Mitigation Plan for the Cybersecurity Risk

The Companies' risk mitigation plan includes a mix of high impact and medium impact projects. The identified high-impact and medium-impact projects were grouped into the five programs described above, as applicable:

1. Perimeter Defenses;
2. Internal Defenses;
3. Sensitive Data Protection;
4. Operational Technology Cybersecurity; and
5. IT Infrastructure Modernization.

[30] CSC-18: The Customer Information System CSC version 8 includes 18 prioritized measures designed to enhance cybersecurity posture. These controls cover areas such as asset management, software inventory, data protection, secure configurations, account and access management, vulnerability management, audit logging, and penetration testing, available at https://www.cisecurity.org/controls.

[31] ICS-CERT: The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT, available at https://us-cert.cisa.gov/ics to:

- Conduct vulnerability and malware analysis.
- Provide onsite support for incident response and forensic analysis.
- Provide situational awareness in the form of actionable intelligence.
- Coordinate the responsible disclosure of vulnerabilities/mitigations.
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The quantitative analysis conducted by the Companies shows that the Companies' Plan of high- and medium-impact projects is the most cost-effective portfolio for managing the increase in Cybersecurity Risk, as is demonstrated by the CBRs compared to other alternative portfolios.

B. Alternative Portfolio 1

The Companies' Alternative Portfolio 1 consists of high impact projects only. The identified high-impact projects were grouped into the same five programs described above, as applicable. The quantitative analysis conducted by the Companies shows that the Companies' Alternative Portfolio 1, comprising only high-impact projects, is estimated to have a slightly higher CBR than the Plan when considering the CBR of the individual categories. However, this portfolio does not provide enough risk reduction to address the increasing rate of Cybersecurity Risk. The effectiveness of the projects in this alternative portfolio is lower than the projected growth rate of the risk. If Alternative Portfolio 1 is executed, Cybersecurity Risk will increase compared to the Companies' risk mitigation plan.

C. Alternative Portfolio 2

Alternative Portfolio 2 consists of all cybersecurity projects under consideration (*i.e.,* high-impact, medium-impact and low-impact). Whereas the Companies' risk mitigation plan includes high- and medium-impact projects, and Alternative Portfolio 1 includes only high-impact projects, Alternative Portfolio 2 includes all projects that the Companies have currently identified. Alternative Portfolio 2 has the highest cost, with the most risk reduction. Alternative Portfolio 2 has a CBR lower than the Companies' Plan since the additional projects in the portfolio (the low-impact projects not included in the Companies' risk mitigation plan for the Cybersecurity Risk) provide an incremental benefit; however, that incremental benefit is less effective relative to its incremental cost.

D. Costs and Cost Benefit Ratios (CBRs) for Alternative Portfolios

The costs and CBRs for Alternative Portfolio 1 and Alternative Portfolio 2 are presented in the tables that follow.[32]

[32] A combined CBR for SoCalGas and SDG&E is presented for each mitigation or control. Cybersecurity Risk is managed centrally for the Companies.

Table 11
SoCalGas Cybersecurity Risk Alternative Mitigation Plan

Alternative Mitigation Forecasted Costs Summary (Direct, in 2024 $ thousands)					
Alternative Mitigation		Forecasted			
ID	Name	2025-2028 Capital	PTY Capital	2025-2028 O&M	PTY O&M
A801	Alternative Portfolio 1	166,013	120,531	51,745	39,945
A802	Alternative Portfolio 2	184,110	133,112	51,745	39,945

Table 12
SDG&E Cybersecurity Risk Alternative Mitigation Plan

Alternative Mitigation Forecasted Costs Summary (Direct, in 2024 $ thousands)					
Alternative Mitigation		Forecasted			
ID	Name	2025-2028 Capital	PTY Capital	2025-2028 O&M	PTY O&M
A801	Alternative Portfolio 1	36,454	12,558	49,494	37,341
A802	Alternative Portfolio 2	36,454	12,558	49,494	37,341

Table 13
Cybersecurity Risk Alternative Mitigation Cost Benefit Ratio Results Summary
(Direct, in 2024 $ millions)

ID	Alternative Mitigation Name	Capital TY 2028	O&M TY 2028	CBR (Societal)	CBR (Hybrid)	CBR (WACC)
A801	Alternative Portfolio 1					
	C801: Perimeter Defenses	29.3	5.4	105.29	98.69	88.88
	C802: Internal Defenses	17.9	19.7	34.23	33.02	29.74
	C803: Sensitive Data Protection	0.0	0.5	243.34	233.43	210.25
	C804: Operational Technology (OT) Cybersecurity	6.9	0.0	223.51	216.43	194.92
	C805: IT Infrastructure Modernization	11.4	0.0	199.20	183.92	165.65
A802	Alternative Portfolio 2					
	C801: Perimeter Defenses	29.3	5.4	103.28	96.86	87.25
	C802: Internal Defenses	19.7	19.7	33.59	32.41	29.19
	C803: Sensitive Data Protection	0.0	0.5	232.90	223.34	201.18
	C804: Operational Technology (OT) Cybersecurity	6.9	0.0	219.38	212.43	191.33
	C805: IT Infrastructure Modernization	11.5	0.0	195.46	180.63	162.70

VI. HISTORICAL PROGRESS GRAPHIC

As directed by the Commission in the Phase 2 Decision, this section illustrates the accomplishments in safety work and the progress in mitigating safety risks over the two immediately preceding RAMP cycles. The historical progress graphic for SoCalGas's and SDG&E's Cybersecurity Risk mitigation programs and activities aligns with safety goals to illustrate trends in historical progress and identify remaining tasks necessary to continue mitigating risks.

Figure 2 below shows SoCalGas's and SDG&E's cybersecurity rating score by BitSight.[33] Cybersecurity rating services, like BitSight, evaluate an organization's cybersecurity posture by continuously monitoring and assessing various risk factors and provide a security score (or rating) that reflects an organization's overall security performance. Security rating services provide an objective, data-driven view of an organization's cybersecurity program, developing cybersecurity ratings by analyzing networks, assets, and vulnerabilities in real-time. Similar to a credit score, which reflects a business's creditworthiness based on its financial history and ability to repay debts, cybersecurity rating services offer a security score that indicates the organization's ability to manage and mitigate Cybersecurity Risks. The score allows external stakeholders such as investors, financial institutions, and government agencies to gauge how effectively an organization is protecting against potential threats. For example, insurance companies may use these ratings to determine premiums and coverage limits or regulators may utilize these ratings to assess compliance with cybersecurity regulatory obligations. BitSight uses a scale from 250 to 900 to rate organizations based on their security performance.

Recent studies have demonstrated a correlation between a cybersecurity rating and the risk of a cybersecurity incident.[34] BitSight compared its ratings to publicly disclosed data breaches and concluded that companies with a rating of 400 or lower were five times more likely to experience a publicly disclosed data breach than companies with a rating of 700 or higher[35]

[33] *See* Bitsight, available at https://www.bitsight.com/about/our-story.

[34] *See* Bitsight, Bitsight Security Ratings Correlate to Breaches, available at https://help.bitsighttech.com/hc/en-us/articles/360011652613-Bitsight-Security-Ratings-Correlate-to-Breaches#Marsh-McLennan.

[35] *See* Bitsight, Bitsight Security Ratings Correlated to Breaches, Data Sheet, available at https://www.bitsight.com/resources/datasheet-bitsight-security-ratings-correlate-breaches.

and that its ratings are indicative of the risk of data breach. A Marsh McLennan Cyber Risk Analytics Center (Marsh McLennan) study identified a clear correlation between lower security ratings and higher likelihood of cybersecurity incidents.[36] An analysis by Verisk (formerly known as AIR Worldwide) demonstrated that organizations with ratings of 700 or greater had a breach probability of less than 1%, while those with ratings below 500 had a probability of nearly 3%.[37] As shown in Figure 2, for the period 2016 through 2024 SoCalGas and SDG&E's BitSight cybersecurity rating score ranged from 683 to 794.

Figure 2
Cybersecurity Risk Historical Progress Graphic
BitSight Cybersecurity Rating Score

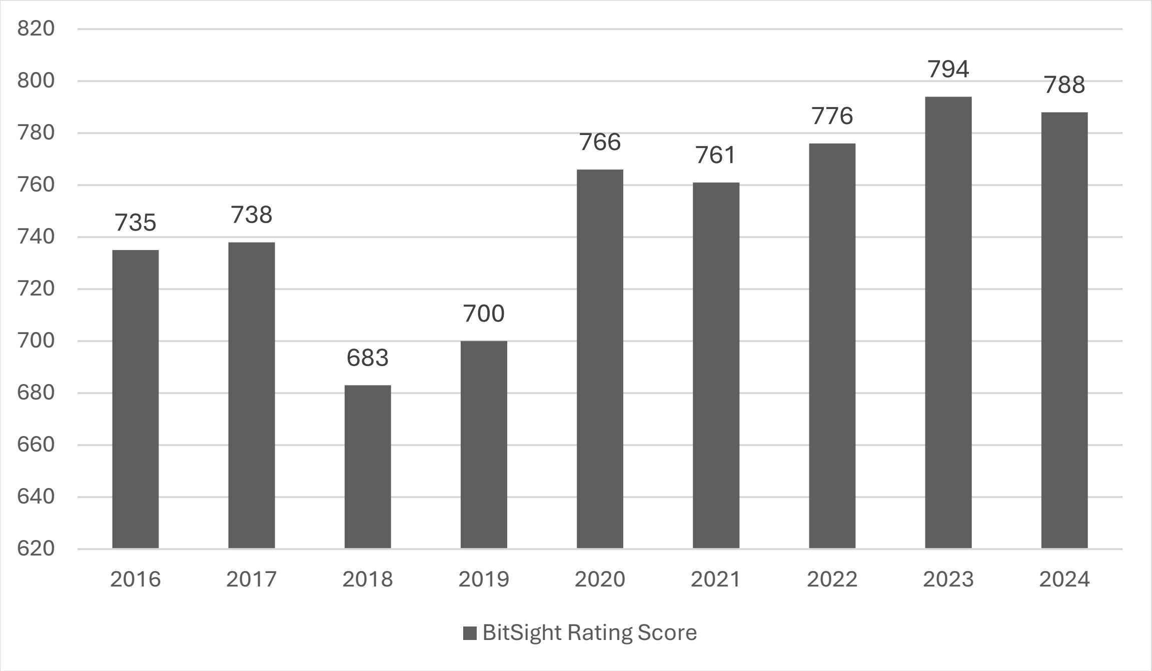
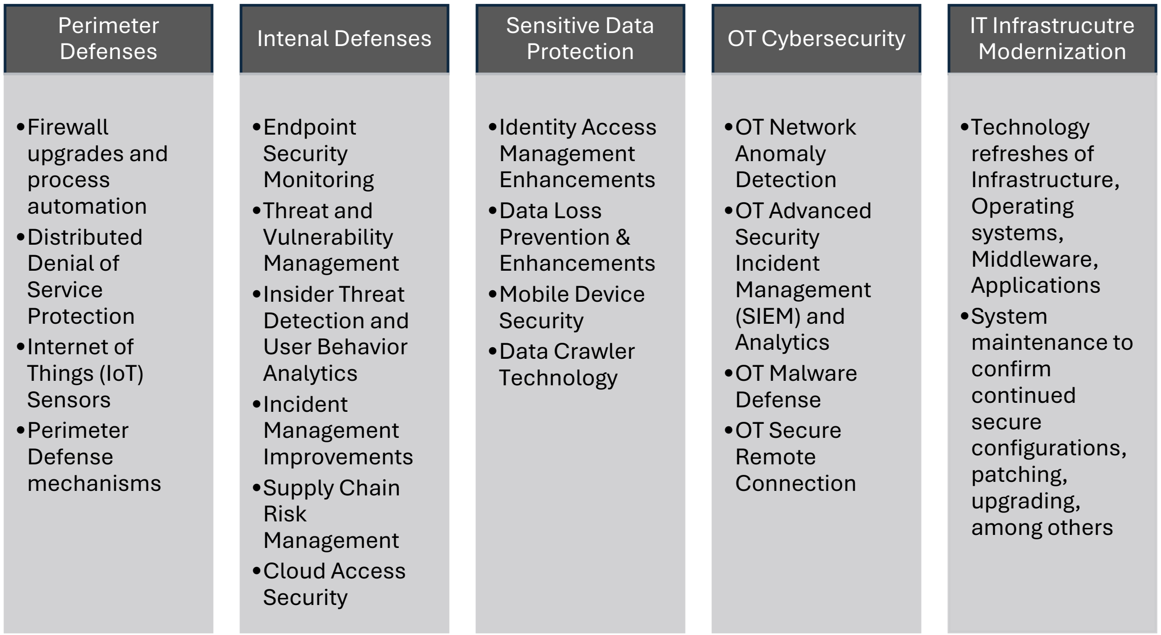


Figure 3 below presents an overview of certain cybersecurity risk mitigation programs and activities implemented during this period.

[36] *See* Bitsight, New Study Finds Significant Correlation Between Bitsight Analytics and Cybersecurity Incidents (October 25, 2022), available at https://www.bitsight.com/blog/new-study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity-incidents.

[37] *See* Bitsight, Bitsight Security Ratings Correlate to Breaches, Verisk: Correlation to Breach, available at https://help.bitsighttech.com/hc/en-us/articles/360011652613-Bitsight-Security-Ratings-Correlate-to-Breaches#Marsh-McLennan.

Figure 3
Cybersecurity Risk Historical Progress Graphic
Cybersecurity Mitigation Programs and Activities



Perimeter Defenses

- Firewall upgrades and process automation
- Distributed Denial of Service Protection
- Internet of Things (IoT) Sensors
- Perimeter Defense mechanisms

Intenal Defenses

- Endpoint Security Monitoring
- Threat and Vulnerability Management
- Insider Threat Detection and User Behavior Analytics
- Incident Management Improvements
- Supply Chain Risk Management
- Cloud Access Security

Sensitive Data Protection

- Identity Access Management Enhancements
- Data Loss Prevention & Enhancements
- Mobile Device Security
- Data Crawler Technology

OT Cybersecurity

- OT Network Anomaly Detection
- OT Advanced Security Incident Management (SIEM) and Analytics
- OT Malware Defense
- OT Secure Remote Connection

IT Infrastrucutre Modernization

- Technology refreshes of Infrastructure, Operating systems, Middleware, Applications
- System maintenance to confirm continued secure configurations, patching, upgrading, among others

Additionally, for the period 2022 through 2024, SoCalGas and SDG&E remediated more than 2.6 million cybersecurity vulnerabilities to mitigate potential security threats. The number of cybersecurity vulnerabilities remediated refers to the total count of security weaknesses or flaws in a system, network, or application that have been identified and successfully fixed. This metric is crucial for understanding how effectively an organization is addressing and mitigating potential security threats. In the realm of threat and vulnerability management, zero-day vulnerabilities represent a significant challenge. These are security flaws that are unknown to the software vendor and can be exploited by attackers before a patch is available. The Citrix Bleed vulnerability is an example, affecting numerous organizations before it was identified and addressed.[38] While the Companies implement robust security measures to mitigate known vulnerabilities, zero-day vulnerabilities create a critical gap between the time they are exploited and the time they are remediated. This gap underscores the importance of proactive monitoring,

[38] The Citrix Bleed vulnerability (CVE-2023-4966) was a critical flaw that allowed unauthenticated, remote attackers to obtain valid session tokens from the device's memory, enabling them to bypass authentication. This vulnerability was actively exploited, leading to significant security risks for affected organizations. *See* ITPRO, What is Citrix Bleed and should you be worried? (October 26, 2023), available at https://www.itpro.com/security/cyber-attacks/what-is-citrix-bleed-and-should-you-be-worried.

rapid response strategies, and continuous improvement in security practices to minimize potential threats. The safety work that remains to be done is addressed in the controls/mitigations detailed above in Section IV. 2024-2031 Control and Mitigation Plan.

ATTACHMENTS

ATTACHMENT A

CONTROLS AND MITIGATIONS WITH REQUIRED COMPLIANCE DRIVERS

The table below indicates some examples of the compliance Drivers that underpin identified controls and mitigations. This is not a complete list.

ID	Control/Mitigation Name	Compliance Driver
C801	Perimeter Defenses	NERC Critical Infrastructure Protection (CIP) Standards, TSA Security Directive (SD)
C802	Internal Defenses	NERC CIP Standards, TSA SD
C803	Sensitive Data Protection	NERC CIP Standards, California Consumer Privacy Act (CCPA), TSA SD
C804	Operational Technology (OT) Cybersecurity	NERC CIP Standards, TSA SD
C805	IT Infrastructure Modernization	NERC CIP Standards, TSA SD

ATTACHMENT B

CYBERSECURITY - REFERENCE MATERIAL FOR QUANTITATIVE ANALYSES

The Phase 3 Decision RDF at Row 10 and Row 29 directs each utility to identify Potential Consequences of a Risk Event using available and appropriate data.[39] Appropriate data may include Company specific data or industry data supplemented by the judgment of subject matter experts. Provided below is a listing of the inputs utilized as part of this assessment and the description of the data.

Risk Data	Source Type	Source Information
Cyber Attack Impact Per Year	External Data	Agency: Business Continuity Institute Link: https://www.thebci.org/news/cyber-attacks-rise-in-volume-as-attackers-revolutionise-their-attack-vectors.html#:~:text=Increase%20in%20volume%20and%20methods,to%20a%20successful%20cyber%2Dattack Description: Expected Likelihood of Cyberattack with Limited Impact Per Year
Data Violations in the Utilities Industry	External Data	Agency: Statista Link: https://www.statista.com/statistics/1318379/us-number-of-private-data-compromises-by-industry/ Description: Industry Due to Cyberattacks in 2023
Reportable Cyberattacks that could have affected Electric System	External Data	Agency: Department of Energy, Report on Electric Emergency and Disturbance Events, 2022 – 2023 (available upon request) Description: Number of reportable electric cyberattacks that could have affected electric system reliability (2022 - 2023)
People Affected by Blackout	External Data	Agency: Department of Energy

[39] D.24-05-064, RDF Row 10 and Row 29.

Risk Data	Source Type	Source Information
		Link: https://www.energy.gov/oe/august-2003-blackout#:~:text=August%2014%20and%2015%2C%202003,50%20million%20customers%20were%20impacted Description: Number of People affected by the August 2003 blackout
Fatalities Attributed to Blackout	External Data	Agency: Reuters Link: https://www.reuters.com/article/business/healthcare-pharmaceuticals/spike-in-deaths-blamed-on-2003-new-york-blackout-idUSTRE80Q07H/ Description: Number of Fatalities occurred during August 2003 blackout
Financial Impact to Public	External Data	Agency: Net Diligence Link: https://netdiligence.com/wp-content/uploads/2023/10/2023-NetDiligence-Cyber-Claims-Study_v1.1.pdf Description: Financial Impact to the public due to a cybersecurity attack.
Cost of Data Breach	External Data	Agency: IBM Link: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec Description: Financial Impact to the public because of the data breach

ATTACHMENT C

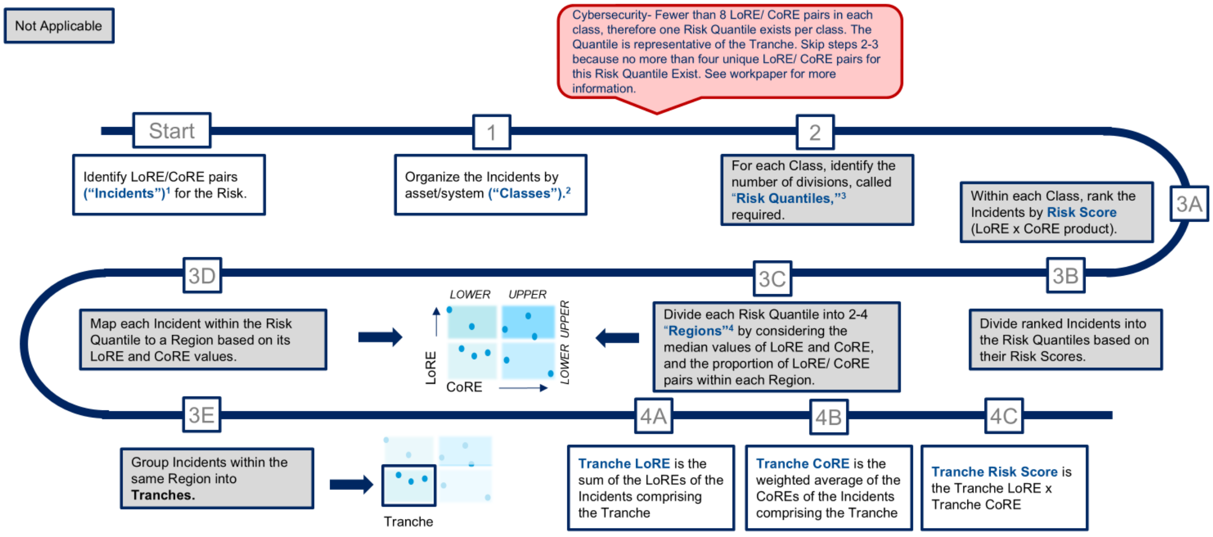
CYBERSECURITY - SUMMARY OF ELEMENTS OF BOW TIE

SUMMARY OF ELEMENTS OF BOW TIE			
ID	**Control/Mitigation Name**	**Drivers Addressed**	**Consequences Addressed**
C801	Perimeter Defenses	DT.1; DT.2; DT.3; DT.4; DT.5; DT.6; DT.7; DT.8; DT.9; DT.10	PC.1; PC.3; PC.4; PC.5; PC.6; PC.8
C802	Internal Defenses	DT.2; DT.3; DT.4; DT.5; DT.6; DT.7; DT.8; DT.9; DT.10	PC.1; PC.2; PC.3; PC.4; PC.5; PC.6; PC.7; PC.8
C803	Sensitive Data Protection	DT.1; DT.2; DT.3; DT.4; DT.7; DT.8; DT.9	PC.2; PC.3; PC.4; PC.5; PC.6; PC.7
C804	Operational Technology (OT) Cybersecurity	DT.1; DT.2; DT.3; DT.4; DT.5; DT.6; DT.7; DT.8; DT.9; DT.10	PC.1; PC.2; PC.3; PC.5; PC.6; PC.8
C805	IT Infrastructure Modernization	DT.2; DT.3; DT.4; DT.5; DT.9	PC.2; PC.4; PC.6; PC.8

ATTACHMENT D:

CYBERSECURITY - APPLICATION OF TRANCHING METHODOLOGY

A sample walkthrough of the Homogeneous Tranching Methodology (HTM) as outlined in Volume 1, Chapter RAMP - 3: Risk



Not Applicable

Cybersecurity- Fewer than 8 LoRE/ CoRE pairs in each class, therefore one Risk Quantile exists per class. The Quantile is representative of the Tranche. Skip steps 2-3 because no more than four unique LoRE/ CoRE pairs for this Risk Quantile Exist. See workpaper for more information.

Start

Identify LoRE/CoRE pairs **("Incidents")**[1] for the Risk.

1

Organize the Incidents by asset/system **("Classes").**[2]

2

For each Class, identify the number of divisions, called **"Risk Quantiles,"**[3] required.

3A

Within each Class, rank the Incidents by **Risk Score** (LoRE x CoRE product).

3B

Divide ranked Incidents into the Risk Quantiles based on their Risk Scores.

3C

Divide each Risk Quantile into 2-4 **"Regions"**[4] by considering the median values of LoRE and CoRE, and the proportion of LoRE/ CoRE pairs within each Region.

3D

Map each Incident within the Risk Quantile to a Region based on its LoRE and CoRE values.

3E

Group Incidents within the same Region into **Tranches.**

4A

Tranche LoRE is the sum of the LoREs of the Incidents comprising the Tranche

4B

Tranche CoRE is the weighted average of the CoREs of the Incidents comprising the Tranche

4C

Tranche Risk Score is the Tranche LoRE x Tranche CoRE

NOTES

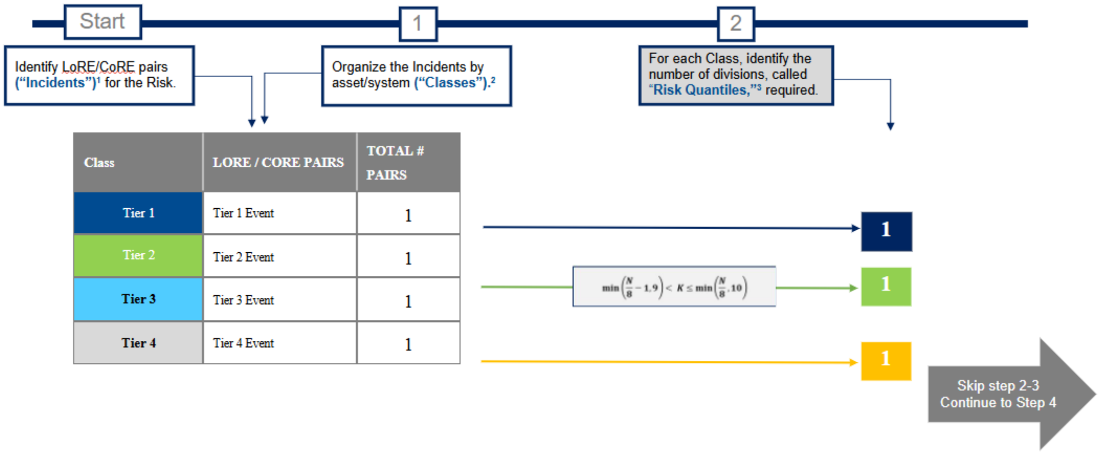
[1] *For example,* ***Incidents (or "Risk Incidents")*** *for Cybersecurity events may include incursions that lead to adverse outcomes*

[2] *For example,* ***Classes (or "Asset Classes")*** *for Cybersecurity include Internal Defense, Perimeter Defense, Sensitive Data Protection, OT Cybersecurity, IT Infrastructure Modernization.*

[3] ***Quantiles*** *are divisions of equal numbers of incidents (quartiles have 4 divisions, quintiles have 5, etc.) The number of incidents dictates the number of quantiles needed.*

[4] *The four* ***Regions*** *are: 1. Lower LoRE-Lower CoRE (LL-LC), 2. Lower LoRE-Upper CoRE (LL-UC), 3. Upper LoRE-Lower CoRE (UL-LC), and 4. Upper LoRE-Upper CoRE (UL-UC).*

Not Applicable



Identify LoRE/CoRE pairs (“Incidents”)[1] for the Risk.

Organize the Incidents by asset/system (“Classes”).[2]

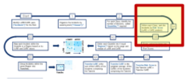
For each Class, identify the number of divisions, called “Risk Quantiles,”[3] required.

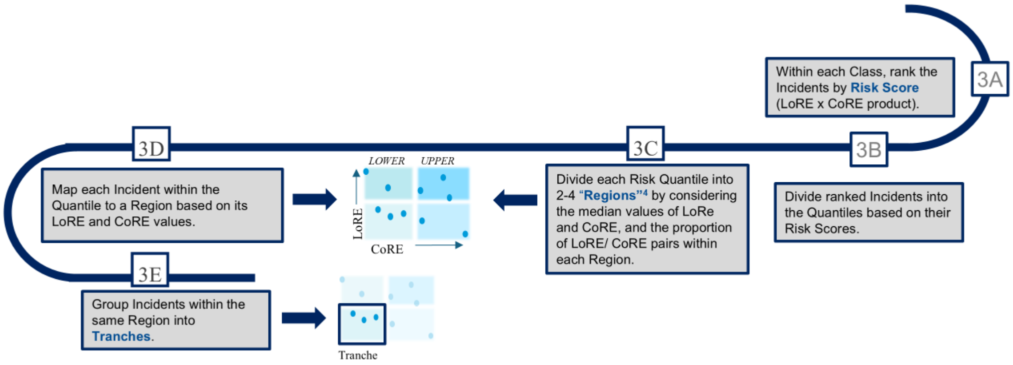
Class	LORE / CORE PAIRS	TOTAL # PAIRS
Tier 1	Tier 1 Event	1
Tier 2	Tier 2 Event	1
Tier 3	Tier 3 Event	1
Tier 4	Tier 4 Event	1

$$\min\left(\frac{N}{8} - 1.9\right) < K \le \min\left(\frac{N}{8}.10\right)$$

Skip step 2-3
Continue to Step 4

Not Applicable





Within each Class, rank the Incidents by Risk Score (LoRE x CoRE product).

Divide ranked Incidents into the Quantiles based on their Risk Scores.

Divide each Risk Quantile into 2-4 “Regions”[4] by considering the median values of LoRe and CoRE, and the proportion of LoRE/ CoRE pairs within each Region.

Map each Incident within the Quantile to a Region based on its LoRE and CoRE values.

Group Incidents within the same Region into Tranches.

4A

Tranche LoRE is the sum of the LoREs of the Incidents comprising the Tranche

4B

Tranche CoRE is the weighted average of the CoREs of the Incidents comprising the Tranche

4C

Tranche Risk Score is the Tranche LoRE x Tranche CoRE

					4A	4B	4C
Class	Risk Quantile	Incident (LoRE/CoRE) Pair	Risk Quantile Region	Tranche	Tranche LoRE	Tranche CoRE	Tranche Risk Score
Tier 1	1	Tier 1 Event	None	Tier 1	0.78	$0.01M	$0.01M
Tier 2	1	Tier 2 Event	None	Tier 2	0.191	$5.29M	$1.01M
Tier 3	1	Tier 3 Event	None	Tier 3	0.085	$892.71M	$75.69M
Tier 4	1	Tier 4 Event	None	Tier 4	0.04	$45,687.82M	$1,827.51M