

SOUTHERN CALIFORNIA GAS COMPANY

Risk Assessment and Mitigation Phase

2025 Report

Chapter: SCG-Risk-8

Number: SCG-R08-CWP

Cybersecurity Capital Workpapers

SOUTHERN CALIFORNIA GAS COMPANY

May 15, 2025



2025 Risk Assessment & Mitigation Phase

INDEX OF RISK CHAPTER

Risk Chapter 2CR08: SCG-RISK-8 CYBERSECURITY

DOCUMENT	PAGE
Summary of Risk Chapter	1
Mitigations: Incurred Costs & Units	2
Supplemental Workpaper	3
<i>Appendix A: Forecast Methodology</i>	17
<i>Appendix B: Unit Measure</i>	18

Summary of Risk Chapter: 2CR08 - SCG-Risk-8 Cybersecurity

In 2024 \$ (000s) Incurred Costs												
	Adjusted Recorded					Adjusted Forecast						
	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
Control/Mitigation	30,702	17,892	23,247	26,121	26,320	44,091	51,023	31,252	51,744	47,275	41,973	40,112
Alternative Mitigation	0	0	0	0	0	86,678	97,901	63,004	102,540	94,213	81,021	78,409
Units	See detailed pages for Units as the unit measure can vary for each mitigation.											

Note: Totals may include rounding differences.

Risk Chapter: **SCG-Risk-8 Cybersecurity**
Risk ID: **2CR08**

In 2024 \$ (000s) Incurred Costs

Mitigation		Unit Measure	Adjusted Recorded					Adjusted Forecast						
ID	Name		2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
A801	Alternative Portfolio 1	Users Prote	0	0	0	0	0	42,586	41,828	31,252	50,347	43,186	39,048	38,297
A802	Alternative Portfolio 2	Users Prote	0	0	0	0	0	44,092	56,073	31,752	52,193	51,027	41,973	40,112
C801	Perimeter Defenses	Users Prote	20,070	2,507	13,421	18,270	1,991	13,881	21,920	14,245	29,251	15,719	6,435	7,020
C802	Internal Defenses	Users Prote	10,632	11,812	7,101	6,014	11,879	18,949	19,215	6,607	17,894	17,013	24,525	25,221
C803	Sensitive Data Protection	Users Prote	0	696	401	6	2,998	0	3,000	2,400	0	5,400	4,320	0
C804	Operational Technology (OT	Users Prote	0	2,876	2,325	1,830	338	3,489	5,371	6,438	3,151	3,151	4,754	5,873
C805	IT Infrastructure Modernizati	Users Prote	0	0	0	0	9,113	7,772	1,517	1,562	1,448	5,992	1,939	1,998

Units

Mitigation		Unit Measure	Adjusted Recorded					Adjusted Forecast						
ID	Name		2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
A801	Alternative Portfolio 1	Users Prote	0	0	0	0	0	25,000	25,000	25,000	25,000	25,000	25,000	25,000
A802	Alternative Portfolio 2	Users Prote	0	0	0	0	0	25,000	25,000	25,000	25,000	25,000	25,000	25,000
C801	Perimeter Defenses	Users Prote	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000
C802	Internal Defenses	Users Prote	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000
C803	Sensitive Data Protection	Users Prote	0	25,000	25,000	25,000	25,000	0	25,000	25,000	0	25,000	25,000	0
C804	Operational Technology (OT	Users Prote	0	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000
C805	IT Infrastructure Modernizati	Users Prote	0	0	0	0	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000

Note: Totals may include rounding differences.

Supplemental Workpapers

Southern California Gas Company

2025 RAMP

Capital Workpapers

2CR08A801 - SCG-Risk-8 Cybersecurity Alternative Portfolio 1							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2025	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	90,000	510,000	600,000
2025	Enhancements to the technologies, platforms, and services that provides backup of critical and sensitive data, and used in the event of a potential ransomware recovery scenario.	2CR08C802	Internal Defenses	High	1,155,000	6,545,000	7,700,000
2025	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C805	IT Infrastructure Modernization	High	1,165,698	6,605,622	7,771,319
2025	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	988,735	5,602,833	6,591,568
2025	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	523,465	2,966,302	3,489,767
2025	Network security hardware, software, connectivity, visibility of traffic and other critical security controls to ensure traffic entering and exiting our networks are safe.	2CR08C801	Perimeter Defenses	High	1,093,509	6,196,554	7,290,063
2025	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	174,513	988,906	1,163,418
2025	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	340,708	1,930,676	2,271,384
2025	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	856,248	4,852,074	5,708,322
2025 Total					6,387,876	36,197,966	42,585,842
2026	A capability that enables secure connections into our most sensitive operational technologies from remote or offsite locations, often needed by key personnel who use systems to manage electric and gas operations.	2CR08C804	OT Cybersecurity	High	75,000	425,000	500,000
2026	Enhancements to the data recovery platforms, tools and services, ensuring the company is protected from serious threats posed by ransomware.	2CR08C802	Internal Defenses	High	300,000	1,700,000	2,000,000
2026	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C801	Perimeter Defenses	High	1,200,669	6,803,790	8,004,459
2026	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	675,000	3,825,000	4,500,000
2026	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	525,000	2,975,000	3,500,000
2026	Our primary platform that enables threat and vulnerability scanning on a key business technology platform that maintains enterprise-wide financials, work management, field operations, customer data and operations among others.	2CR08C802	Internal Defenses	High	1,018,512	5,771,571	6,790,083
2026	Our primary technology for authentication and connectivity for contractors, required to safely authenticate and connect to our OT network.	2CR08C801	Perimeter Defenses	High	225,000	1,275,000	1,500,000
2026	Platform that enables workflows, cataloguing, tracking and assignment of ownership for operational technology ("OT") vulnerabilities and their associated remediation and/or risk management activities.	2CR08C804	OT Cybersecurity	High	205,643	1,165,312	1,370,955
2026	Platforms and services to enhance our data protection capabilities through classification and labeling of data.	2CR08C803	Sensitive Data Protection	High	450,000	2,550,000	3,000,000
2026	Replacement of obsolete, end of life/end of service hardware that runs firewalls, protecting the company from threats and malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	227,534	1,289,357	1,516,890
2026	The primary platform that protects our web applications (e.g., customer login portal) from malicious traffic and attacks.	2CR08C801	Perimeter Defenses	High	483,171	2,737,971	3,221,142
2026	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	513,749	2,911,244	3,424,993
2026	Upgrade capabilities on a security platform that enables collection of data that can be analyzed to respond to threats.	2CR08C802	Internal Defenses	High	375,000	2,125,000	2,500,000
2026 Total					6,274,278	35,554,244	41,828,522
2027	An upgrade to the company's data loss protection ("DLP") capability, which ensures we mitigate the risk of losing sensitive information either unknowingly or by purposeful attempt from a threat actor.	2CR08C803	Sensitive Data Protection	High	360,000	2,040,000	2,400,000
2027	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	234,360	1,328,037	1,562,397
2027	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C801	Perimeter Defenses	High	1,236,689	7,007,904	8,244,593
2027	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	825,000	4,675,001	5,500,001
2027	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	525,000	2,975,000	3,500,000
2027	Security analytics and threat intelligence platform enhancement.	2CR08C801	Perimeter Defenses	High	75,000	425,000	500,000
2027	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	256,875	1,455,622	1,712,497
2027	Upgrade for our Public Key Infrastructure capabilities, protection from post-quantum cryptographic decryption.	2CR08C802	Internal Defenses	High	734,244	4,160,715	4,894,959

Southern California Gas Company

2025 RAMP

Capital Workpapers

2CR08A801 - SCG-Risk-8 Cybersecurity Alternative Portfolio 1							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2027	Upgrade to the devices (sensors) used to monitor network traffic within operational technology ("OT") environments. This capability ensures we can monitor and log potentially malicious behavior and traffic from OT assets.	2CR08C804	OT Cybersecurity	High	440,682	2,497,199	2,937,881
2027 Total					4,687,849	26,564,479	31,252,328
2028	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	83,430	472,770	556,200
2028	A key security product enabling protection of endpoints (e.g., employee laptops) from risk of a breach or sharing of sensitive information. This capability enforces security policies to keep the company and users safe.	2CR08C801	Perimeter Defenses	High	135,000	765,000	900,000
2028	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	217,251	1,231,091	1,448,342
2028	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	675,000	3,825,000	4,500,000
2028	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2028	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2028	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	161,773	916,716	1,078,489
2028	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	398,628	2,258,891	2,657,519
2028	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	1,155,935	6,550,300	7,706,235
2028	Enterprise licenses for firewall hardware used across the enterprise to protect from malicious traffic and threats.	2CR08C801	Perimeter Defenses	High	-	22,500,000	22,500,000
2028 Total					4,177,018	46,169,767	50,346,785
2029	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	223,769	1,268,023	1,491,792
2029	Investment in a capability that allows the company to identify which specific web connections can or cannot be accessed, typically from within a highly-sensitive environment such as operational technology.	2CR08C802	Internal Defenses	High	351,000	1,989,000	2,340,000
2029	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	270,000	1,530,000	1,800,000
2029	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2029	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2029	Our primary platform that enables threat and vulnerability scanning on a key business technology platform that maintains enterprise-wide financials, work management, field operations, customer data and operations among others.	2CR08C802	Internal Defenses	High	1,191,660	6,752,737	7,944,397
2029	Our primary technology for authentication and connectivity for contractors, required to safely authenticate and connect to our network.	2CR08C801	Perimeter Defenses	High	208,575	1,181,925	1,390,500
2029	Platforms and services to enhance our data protection capabilities through classification and labeling of data.	2CR08C803	Sensitive Data Protection	High	810,000	4,590,000	5,400,000
2029	The primary platform that protects our web applications (e.g., customer login portal) from malicious traffic and attacks.	2CR08C801	Perimeter Defenses	High	447,900	2,538,099	2,985,999
2029	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	300,543	1,703,078	2,003,621
2029	Tool that enables our threat intelligence capability to identify the threat landscape, take action on threats, and prevent and mitigate attacks.	2CR08C801	Perimeter Defenses	High	210,600	1,193,400	1,404,000
2029	Upgrade capabilities on a security platform that enables collection of data that can be analyzed to respond to threats.	2CR08C802	Internal Defenses	High	438,750	2,486,250	2,925,000
2029	Enhancement, replacement or upgrades to advanced threat protection tools, software, capabilities	2CR08C805	IT Infrastructure Modernization	High	675,000	3,825,000	4,500,000
2029 Total					6,477,796	36,707,513	43,185,309
2030	An upgrade to the company's data loss protection ("DLP") capability, which ensures we mitigate the risk of losing sensitive information either unknowingly or by purposeful attempt from a threat actor.	2CR08C803	Sensitive Data Protection	High	648,000	3,672,000	4,320,000
2030	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	290,900	1,648,431	1,939,330
2030	Enhancements to the data recovery platforms, tools and services, ensuring the company is protected from serious threats posed by ransomware.	2CR08C802	Internal Defenses	High	945,000	5,355,000	6,300,000
2030	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2030	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08A801 - SCG-Risk-8 Cybersecurity Alternative Portfolio 1							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2030	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	877,500	4,972,500	5,850,000
2030	Platform that enables workflows, cataloguing, tracking and assignment of ownership for operational technology ("OT") vulnerabilities and their associated remediation and/or risk management activities.	2CR08C804	OT Cybersecurity	High	240,603	1,363,414	1,604,017
2030	Security analytics and threat intelligence platform enhancement.	2CR08C801	Perimeter Defenses	High	87,750	497,250	585,000
2030	Investments in protection of AI related technologies used to serve the business.	2CR08C802	Internal Defenses	High	1,417,500	8,032,500	9,450,000
2030 Total					5,857,252	33,191,095	39,048,347
2031	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	85,933	486,953	572,886
2031	A key security product enabling protection of endpoints (e.g., employee laptops) from risk of a breach or sharing of sensitive information. This capability enforces security policies to keep the company and users safe.	2CR08C801	Perimeter Defenses	High	175,500	994,500	1,170,000
2031	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	299,626	1,697,883	1,997,509
2031	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	877,500	4,972,500	5,850,000
2031	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2031	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2031	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	526,500	2,983,500	3,510,000
2031	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	518,216	2,936,559	3,454,775
2031	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	1,502,716	8,515,390	10,018,106
2031	Upgrade to the devices (sensors) used to monitor network traffic within operational technology ("OT") environments. This capability ensures we can monitor and log potentially malicious behavior and traffic from OT assets.	2CR08C804	OT Cybersecurity	High	408,512	2,314,904	2,723,416
2031 Total					5,744,504	32,552,188	38,296,692
Grand Total					39,606,574	246,937,252	286,543,826

Mitigation Level Units: 25k Users Protected

Southern California Gas Company

2025 RAMP

Capital Workpapers

2CR08A802 - SCG-Risk-8 Cybersecurity Alternative Portfolio 2							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2025	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	90,000	510,000	600,000
2025	Enhancements to the technologies, platforms, and services that provides backup of critical and sensitive data, and used in the event of a potential ransomware recovery scenario.	2CR08C802	Internal Defenses	High	1,155,000	6,545,000	7,700,000
2025	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C805	IT Infrastructure Modernization	High	1,165,698	6,605,622	7,771,319
2025	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	988,735	5,602,833	6,591,568
2025	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	523,465	2,966,302	3,489,767
2025	Network security hardware, software, connectivity, visibility of traffic and other critical security controls to ensure traffic entering and exiting our networks are safe.	2CR08C801	Perimeter Defenses	High	1,093,509	6,196,554	7,290,063
2025	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	174,513	988,906	1,163,418
2025	Platform that enables automated checks and remediation of common Indicators of Compromise ("IOCs"), which indicate a system or platform may be vulnerable to a breach.	2CR08C802	Internal Defenses	Medium	225,904	1,280,120	1,506,024
2025	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	340,708	1,930,676	2,271,384
2025	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	856,248	4,852,074	5,708,322
2025 Total					6,613,780	37,478,086	44,091,866
2026	A capability that enables secure connections into our most sensitive operational technologies from remote or offsite locations, often needed by key personnel who use systems to manage electric and gas operations.	2CR08C804	OT Cybersecurity	High	75,000	425,000	500,000
2026	An attack surface management ("ASM") platform that provides broad, enterprise-scale visibility to key threat, vulnerability, analytics, and security insights in a single console.	2CR08C802	Internal Defenses	Low	525,000	2,975,000	3,500,000
2026	An automation capability that creates conditions for how we manage inbound and outbound traffic between our network and public internet, enabling cost-reduction of manual work.	2CR08C801	Perimeter Defenses	Medium	524,101	2,969,905	3,494,006
2026	An upgrade to the company's Security Information and Event Management ("SIEM") capability, enabling critical insights and action for our security operations and incident response teams.	2CR08C802	Internal Defenses	Medium	375,000	2,125,000	2,500,000
2026	Enhancements to the data recovery platforms, tools and services, ensuring the company is protected from serious threats posed by ransomware.	2CR08C802	Internal Defenses	High	300,000	1,700,000	2,000,000
2026	Investment in a capability that allows the company to identify which specific web connections can or cannot be accessed, typically from within a highly-sensitive environment such as operational technology.	2CR08C802	Internal Defenses	Medium	300,000	1,700,000	2,000,000
2026	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C801	Perimeter Defenses	High	1,200,669	6,803,790	8,004,459
2026	Investment in our Security Orchestration and Automated Response ("SOAR"), enables taking information from security alerts and triggering pre-defined actions to mitigate threats quickly and efficiently.	2CR08C802	Internal Defenses	Low	150,000	850,000	1,000,000
2026	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	675,000	3,825,000	4,500,000
2026	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	525,000	2,975,000	3,500,000
2026	Our primary platform that enables threat and vulnerability scanning on a key business technology platform that maintains enterprise-wide financials, work management, field operations, customer data and operations among others.	2CR08C802	Internal Defenses	High	1,018,512	5,771,571	6,790,083
2026	Our primary technology for authentication and connectivity for contractors, required to safely authenticate and connect to our OT network.	2CR08C801	Perimeter Defenses	High	225,000	1,275,000	1,500,000
2026	Platform that enables automation of penetration testing, an activity that seeks to target, identify and exploit potential attack methods used by malicious threat actors. This investment ensures we can expand through automation vs relying solely on manual human-led penetration testing.	2CR08C801	Perimeter Defenses	Low	82,500	467,500	550,000
2026	Platform that enables workflows, cataloguing, tracking and assignment of ownership for operational technology ("OT") vulnerabilities and their associated remediation and/or risk management activities.	2CR08C804	OT Cybersecurity	High	205,643	1,165,312	1,370,955
2026	Platforms and services to enhance our data protection capabilities through classification and labeling of data.	2CR08C803	Sensitive Data Protection	High	450,000	2,550,000	3,000,000
2026	Replacement of obsolete, end of life/end of service hardware that runs firewalls, protecting the company from threats and malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	227,534	1,289,357	1,516,890
2026	The primary platform that protects our web applications (e.g., customer login portal) from malicious traffic and attacks.	2CR08C801	Perimeter Defenses	High	483,171	2,737,971	3,221,142

Southern California Gas Company

2025 RAMP

Capital Workpapers

2CR08A802 - SCG-Risk-8 Cybersecurity Alternative Portfolio 2							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2026	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	513,749	2,911,244	3,424,993
2026	Tool that enables our threat intelligence capability to identify the threat landscape, take action on threats, and prevent and mitigate attacks.	2CR08C801	Perimeter Defenses	Medium	180,000	1,020,000	1,200,000
2026	Upgrade capabilities on a security platform that enables collection of data that can be analyzed to respond to threats.	2CR08C802	Internal Defenses	High	375,000	2,125,000	2,500,000
2026 Total					8,410,879	47,661,649	56,072,528
2027	An upgrade to the company's data loss protection ("DLP") capability, which ensures we mitigate the risk of losing sensitive information either unknowingly or by purposeful attempt from a threat actor.	2CR08C803	Sensitive Data Protection	High	360,000	2,040,000	2,400,000
2027	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	234,360	1,328,037	1,562,397
2027	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C801	Perimeter Defenses	High	1,236,689	7,007,904	8,244,593
2027	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	825,000	4,675,001	5,500,001
2027	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	525,000	2,975,000	3,500,000
2027	Security analytics and threat intelligence platform enhancement.	2CR08C801	Perimeter Defenses	High	75,000	425,000	500,000
2027	Security orchestration across various platforms and tools, enabling our security operations teams to quickly assess potential threats and take action on them.	2CR08C802	Internal Defenses	Low	75,000	425,001	500,001
2027	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	256,875	1,455,622	1,712,497
2027	Upgrade for our Public Key Infrastructure capabilities, protection from post-quantum cryptographic decryption.	2CR08C802	Internal Defenses	High	734,244	4,160,715	4,894,959
2027	Upgrade to the devices (sensors) used to monitor network traffic within operational technology ("OT") environments. This capability ensures we can monitor and log potentially malicious behavior and traffic from OT assets.	2CR08C804	OT Cybersecurity	High	440,682	2,497,199	2,937,881
2027 Total					4,762,849	26,989,480	31,752,329
2028	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	83,430	472,770	556,200
2028	A key security product enabling protection of endpoints (e.g., employee laptops) from risk of a breach or sharing of sensitive information. This capability enforces security policies to keep the company and users safe.	2CR08C801	Perimeter Defenses	High	135,000	765,000	900,000
2028	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	217,251	1,231,091	1,448,342
2028	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	675,000	3,825,000	4,500,000
2028	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2028	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2028	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	161,773	916,716	1,078,489
2028	Platform that enables automated checks and remediation of common Indicators of Compromise ("IOCs"), which indicate a system or platform may be vulnerable to a breach.	2CR08C802	Internal Defenses	Medium	209,413	1,186,671	1,396,084
2028	Security orchestration across various platforms and tools, enabling our security operations teams to quickly assess potential threats and take action on them.	2CR08C802	Internal Defenses	Low	67,500	382,500	450,000
2028	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	398,628	2,258,891	2,657,519
2028	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	1,155,935	6,550,300	7,706,235
2028	Enterprise licenses for firewall hardware used across the enterprise to protect from malicious traffic and threats.	2CR08C801	Perimeter Defenses	High	-	22,500,000	22,500,000
2028 Total					4,453,930	47,738,939	52,192,869
2029	An attack surface management ("ASM") platform that provides broad, enterprise-scale visibility to key threat, vulnerability, analytics, and security insights in a single console.	2CR08C802	Internal Defenses	Low	486,675	2,757,825	3,244,500
2029	An automation capability that creates conditions for how we manage inbound and outbound traffic between our network and public internet, enabling cost-reduction of manual work.	2CR08C801	Perimeter Defenses	Medium	613,198	3,474,789	4,087,987
2029	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	223,769	1,268,023	1,491,792
2029	Investment in a capability that allows the company to identify which specific web connections can or cannot be accessed, typically from within a highly-sensitive environment such as operational technology.	2CR08C802	Internal Defenses	High	351,000	1,989,000	2,340,000

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08A802 - SCG-Risk-8 Cybersecurity Alternative Portfolio 2							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2029	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	270,000	1,530,000	1,800,000
2029	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2029	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2029	Our primary platform that enables threat and vulnerability scanning on a key business technology platform that maintains enterprise-wide financials, work management, field operations, customer data and operations among others.	2CR08C802	Internal Defenses	High	1,191,660	6,752,737	7,944,397
2029	Our primary technology for authentication and connectivity for contractors, required to safely authenticate and connect to our network.	2CR08C801	Perimeter Defenses	High	208,575	1,181,925	1,390,500
2029	Platform that enables automation of penetration testing, an activity that seeks to target, identify and exploit potential attack methods used by malicious threat actors. This investment ensures we can expand through automation vs relying solely on manual human-led penetration testing.	2CR08C801	Perimeter Defenses	Low	76,478	433,373	509,850
2029	Platforms and services to enhance our data protection capabilities through classification and labeling of data.	2CR08C803	Sensitive Data Protection	High	810,000	4,590,000	5,400,000
2029	The primary platform that protects our web applications (e.g., customer login portal) from malicious traffic and attacks.	2CR08C801	Perimeter Defenses	High	447,900	2,538,099	2,985,999
2029	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	300,543	1,703,078	2,003,621
2029	Tool that enables our threat intelligence capability to identify the threat landscape, take action on threats, and prevent and mitigate attacks.	2CR08C801	Perimeter Defenses	High	210,600	1,193,400	1,404,000
2029	Upgrade capabilities on a security platform that enables collection of data that can be analyzed to respond to threats.	2CR08C802	Internal Defenses	High	438,750	2,486,250	2,925,000
2029	Enhancement, replacement or upgrades to advanced threat protection tools, software, capabilities	2CR08C805	IT Infrastructure Modernization	High	675,000	3,825,000	4,500,000
2029 Total					7,654,147	43,373,499	51,027,646
2030	An upgrade to the company's data loss protection ("DLP") capability, which ensures we mitigate the risk of losing sensitive information either unknowingly or by purposeful attempt from a threat actor.	2CR08C803	Sensitive Data Protection	High	648,000	3,672,000	4,320,000
2030	An upgrade to the company's Security Information and Event Management ("SIEM") capability, enabling critical insights and action for our security operations and incident response teams.	2CR08C802	Internal Defenses	Medium	438,750	2,486,250	2,925,000
2030	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	290,900	1,648,431	1,939,330
2030	Enhancements to the data recovery platforms, tools and services, ensuring the company is protected from serious threats posed by ransomware.	2CR08C802	Internal Defenses	High	945,000	5,355,000	6,300,000
2030	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2030	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2030	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	877,500	4,972,500	5,850,000
2030	Platform that enables workflows, cataloging, tracking and assignment of ownership for operational technology ("OT") vulnerabilities and their associated remediation and/or risk management activities.	2CR08C804	OT Cybersecurity	High	240,603	1,363,414	1,604,017
2030	Security analytics and threat intelligence platform enhancement.	2CR08C801	Perimeter Defenses	High	87,750	497,250	585,000
2030	Investments in protection of AI related technologies used to serve the business.	2CR08C802	Internal Defenses	High	1,417,500	8,032,500	9,450,000
2030 Total					6,296,002	35,677,345	41,973,347
2031	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	85,933	486,953	572,886
2031	A key security product enabling protection of endpoints (e.g., employee laptops) from risk of a breach or sharing of sensitive information. This capability enforces security policies to keep the company and users safe.	2CR08C801	Perimeter Defenses	High	175,500	994,500	1,170,000
2031	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	299,626	1,697,883	1,997,509
2031	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	877,500	4,972,500	5,850,000
2031	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2031	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2031	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	526,500	2,983,500	3,510,000

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08A802 - SCG-Risk-8 Cybersecurity Alternative Portfolio 2							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2031	Platform that enables automated checks and remediation of common Indicators of Compromise ("IOCs"), which indicate a system or platform may be vulnerable to a breach.	2CR08C802	Internal Defenses	Medium	272,236	1,542,673	1,814,909
2031	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	518,216	2,936,559	3,454,775
2031	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	1,502,716	8,515,390	10,018,106
2031	Upgrade to the devices (sensors) used to monitor network traffic within operational technology ("OT") environments. This capability ensures we can monitor and log potentially malicious behavior and traffic from OT assets.	2CR08C804	OT Cybersecurity	High	408,512	2,314,904	2,723,416
2031 Total					6,016,740	34,094,861	40,111,601
Grand Total					44,208,328	273,013,859	317,222,187

Mitigation Level Units: 25k Users Protected

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08C801 - SCG-Risk-8 Cybersecurity Perimeter Defenses							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2025	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	988,735	5,602,833	6,591,568
2025	Network security hardware, software, connectivity, visibility of traffic and other critical security controls to ensure traffic entering and exiting our networks are safe.	2CR08C801	Perimeter Defenses	High	1,093,509	6,196,554	7,290,063
2025 Total					2,082,245	11,799,387	13,881,631
2026	An automation capability that creates conditions for how we manage inbound and outbound traffic between our network and public internet, enabling cost-reduction of manual work.	2CR08C801	Perimeter Defenses	Medium	524,101	2,969,905	3,494,006
2026	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C801	Perimeter Defenses	High	1,200,669	6,803,790	8,004,459
2026	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	675,000	3,825,000	4,500,000
2026	Our primary technology for authentication and connectivity for contractors, required to safely authenticate and connect to our OT network.	2CR08C801	Perimeter Defenses	High	225,000	1,275,000	1,500,000
2026	The primary platform that protects our web applications (e.g., customer login portal) from malicious traffic and attacks.	2CR08C801	Perimeter Defenses	High	483,171	2,737,971	3,221,142
2026	Tool that enables our threat intelligence capability to identify the threat landscape, take action on threats, and prevent and mitigate attacks.	2CR08C801	Perimeter Defenses	Medium	180,000	1,020,000	1,200,000
2026 Total					3,287,941	18,631,666	21,919,607
2027	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C801	Perimeter Defenses	High	1,236,689	7,007,904	8,244,593
2027	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	825,000	4,675,001	5,500,001
2027	Security analytics and threat intelligence platform enhancement.	2CR08C801	Perimeter Defenses	High	75,000	425,000	500,000
2027 Total					2,136,689	12,107,905	14,244,594
2028	A key security product enabling protection of endpoints (e.g., employee laptops) from risk of a breach or sharing of sensitive information. This capability enforces security policies to keep the company and users safe.	2CR08C801	Perimeter Defenses	High	135,000	765,000	900,000
2028	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2028	Enterprise licenses for firewall hardware used across the enterprise to protect from malicious traffic and threats.	2CR08C801	Perimeter Defenses	High	-	22,500,000	22,500,000
2028 Total					1,012,500	28,237,500	29,250,000
2029	An automation capability that creates conditions for how we manage inbound and outbound traffic between our network and public internet, enabling cost-reduction of manual work.	2CR08C801	Perimeter Defenses	Medium	613,198	3,474,789	4,087,987
2029	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2029	Our primary technology for authentication and connectivity for contractors, required to safely authenticate and connect to our network.	2CR08C801	Perimeter Defenses	High	208,575	1,181,925	1,390,500
2029	The primary platform that protects our web applications (e.g., customer login portal) from malicious traffic and attacks.	2CR08C801	Perimeter Defenses	High	447,900	2,538,099	2,985,999
2029	Tool that enables our threat intelligence capability to identify the threat landscape, take action on threats, and prevent and mitigate attacks.	2CR08C801	Perimeter Defenses	High	210,600	1,193,400	1,404,000
2029 Total					2,357,773	13,360,713	15,718,486
2030	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2030	Security analytics and threat intelligence platform enhancement.	2CR08C801	Perimeter Defenses	High	87,750	497,250	585,000
2030 Total					965,250	5,469,750	6,435,000
2031	A key security product enabling protection of endpoints (e.g., employee laptops) from risk of a breach or sharing of sensitive information. This capability enforces security policies to keep the company and users safe.	2CR08C801	Perimeter Defenses	High	175,500	994,500	1,170,000
2031	Investments in security technologies, platforms and services that enable security guardrails for our cloud applications and services.	2CR08C801	Perimeter Defenses	High	877,500	4,972,500	5,850,000
2031 Total					1,053,000	5,967,000	7,020,000
Grand Total					12,895,398	95,573,920	108,469,318

Mitigation Level Units: 25k Users Protected

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08C802 - SCG-Risk-8 Cybersecurity Internal Defenses							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2025	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	90,000	510,000	600,000
2025	Enhancements to the technologies, platforms, and services that provides backup of critical and sensitive data, and used in the event of a potential ransomware recovery scenario.	2CR08C802	Internal Defenses	High	1,155,000	6,545,000	7,700,000
2025	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	174,513	988,906	1,163,418
2025	Platform that enables automated checks and remediation of common Indicators of Compromise ("IOCs"), which indicate a system or platform may be vulnerable to a breach.	2CR08C802	Internal Defenses	Medium	225,904	1,280,120	1,506,024
2025	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	340,708	1,930,676	2,271,384
2025	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	856,248	4,852,074	5,708,322
2025 Total					2,842,372	16,106,776	18,949,148
2026	An upgrade to the company's Security Information and Event Management ("SIEM") capability, enabling critical insights and action for our security operations and incident response teams.	2CR08C802	Internal Defenses	Medium	375,000	2,125,000	2,500,000
2026	Enhancements to the data recovery platforms, tools and services, ensuring the company is protected from serious threats posed by ransomware.	2CR08C802	Internal Defenses	High	300,000	1,700,000	2,000,000
2026	Investment in a capability that allows the company to identify which specific web connections can or cannot be accessed, typically from within a highly-sensitive environment such as operational technology.	2CR08C802	Internal Defenses	Medium	300,000	1,700,000	2,000,000
2026	Our primary platform that enables threat and vulnerability scanning on a key business technology platform that maintains enterprise-wide financials, work management, field operations, customer data and operations among others.	2CR08C802	Internal Defenses	High	1,018,512	5,771,571	6,790,083
2026	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	513,749	2,911,244	3,424,993
2026	Upgrade capabilities on a security platform that enables collection of data that can be analyzed to respond to threats.	2CR08C802	Internal Defenses	High	375,000	2,125,000	2,500,000
2026 Total					2,882,261	16,332,815	19,215,076
2027	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	256,875	1,455,622	1,712,497
2027	Upgrade for our Public Key Infrastructure capabilities, protection from post-quantum cryptographic decryption.	2CR08C802	Internal Defenses	High	734,244	4,160,715	4,894,959
2027 Total					991,118	5,616,338	6,607,456
2028	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	83,430	472,770	556,200
2028	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	675,000	3,825,000	4,500,000
2028	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	161,773	916,716	1,078,489
2028	Platform that enables automated checks and remediation of common Indicators of Compromise ("IOCs"), which indicate a system or platform may be vulnerable to a breach.	2CR08C802	Internal Defenses	Medium	209,413	1,186,671	1,396,084
2028	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	398,628	2,258,891	2,657,519
2028	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	1,155,935	6,550,300	7,706,235
2028 Total					2,684,179	15,210,348	17,894,527
2029	Investment in a capability that allows the company to identify which specific web connections can or cannot be accessed, typically from within a highly-sensitive environment such as operational technology.	2CR08C802	Internal Defenses	High	351,000	1,989,000	2,340,000
2029	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	270,000	1,530,000	1,800,000
2029	Our primary platform that enables threat and vulnerability scanning on a key business technology platform that maintains enterprise-wide financials, work management, field operations, customer data and operations among others.	2CR08C802	Internal Defenses	High	1,191,660	6,752,737	7,944,397
2029	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	300,543	1,703,078	2,003,621
2029	Upgrade capabilities on a security platform that enables collection of data that can be analyzed to respond to threats.	2CR08C802	Internal Defenses	High	438,750	2,486,250	2,925,000
2029 Total					2,551,953	14,461,065	17,013,018
2030	An upgrade to the company's Security Information and Event Management ("SIEM") capability, enabling critical insights and action for our security operations and incident response teams.	2CR08C802	Internal Defenses	Medium	438,750	2,486,250	2,925,000
2030	Enhancements to the data recovery platforms, tools and services, ensuring the company is protected from serious threats posed by ransomware.	2CR08C802	Internal Defenses	High	945,000	5,355,000	6,300,000

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08C802 - SCG-Risk-8 Cybersecurity Internal Defenses							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2030	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	877,500	4,972,500	5,850,000
2030	Investments in protection of AI related technologies used to serve the business.	2CR08C802	Internal Defenses	High	1,417,500	8,032,500	9,450,000
2030 Total					3,678,750	20,846,250	24,525,000
2031	A key component of our vulnerability management program, this platform enables visibility across the enterprise to identify vulnerabilities on our systems and infrastructure.	2CR08C802	Internal Defenses	High	85,933	486,953	572,886
2031	Investment in ensuring cryptography enhancements to protect against post-quantum computing.	2CR08C802	Internal Defenses	High	877,500	4,972,500	5,850,000
2031	Our primary method of verifying digital identities for safe and secure connections that protect sensitive information.	2CR08C802	Internal Defenses	High	526,500	2,983,500	3,510,000
2031	Platform that enables automated checks and remediation of common Indicators of Compromise ("IOCs"), which indicate a system or platform may be vulnerable to a breach.	2CR08C802	Internal Defenses	Medium	272,236	1,542,673	1,814,909
2031	The primary tool that protects the company from malicious email traffic, spam, and potential phishing and ransomware attacks.	2CR08C802	Internal Defenses	High	518,216	2,936,559	3,454,775
2031	The technologies, platforms and services that enable our companies to confirm (authenticate) who should be accessing our network and applications.	2CR08C802	Internal Defenses	High	1,502,716	8,515,390	10,018,106
2031 Total					3,783,101	21,437,575	25,220,676
Grand Total					19,413,735	110,011,166	129,424,902

Mitigation Level Units: 25k Users Protected

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08C803 - SCG-Risk-8 Cybersecurity Sensitive Data Protection							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2026	Platforms and services to enhance our data protection capabilities through classification and labeling of data.	2CR08C803	Sensitive Data Protection	High	450,000	2,550,000	3,000,000
2026 Total					450,000	2,550,000	3,000,000
2027	An upgrade to the company's data loss protection ("DLP") capability, which ensures we mitigate the risk of losing sensitive information either unknowingly or by purposeful attempt from a threat actor.	2CR08C803	Sensitive Data Protection	High	360,000	2,040,000	2,400,000
2027 Total					360,000	2,040,000	2,400,000
2029	Platforms and services to enhance our data protection capabilities through classification and labeling of data.	2CR08C803	Sensitive Data Protection	High	810,000	4,590,000	5,400,000
2029 Total					810,000	4,590,000	5,400,000
2030	An upgrade to the company's data loss protection ("DLP") capability, which ensures we mitigate the risk of losing sensitive information either unknowingly or by purposeful attempt from a threat actor.	2CR08C803	Sensitive Data Protection	High	648,000	3,672,000	4,320,000
2030 Total					648,000	3,672,000	4,320,000
Grand Total					2,268,000	12,852,000	15,120,000

Mitigation Level Units: 25k Users Protected

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08C804 - SCG-Risk-8 Cybersecurity Operational Technology (OT) Cyberse							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2025	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	523,465	2,966,302	3,489,767
2025 Total					523,465	2,966,302	3,489,767
2026	A capability that enables secure connections into our most sensitive operational technologies from remote or offsite locations, often needed by key personnel who use systems to manage electric and gas operations.	2CR08C804	OT Cybersecurity	High	75,000	425,000	500,000
2026	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	525,000	2,975,000	3,500,000
2026	Platform that enables workflows, cataloguing, tracking and assignment of ownership for operational technology ("OT") vulnerabilities and their associated remediation and/or risk management activities.	2CR08C804	OT Cybersecurity	High	205,643	1,165,312	1,370,955
2026 Total					805,643	4,565,312	5,370,955
2027	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	525,000	2,975,000	3,500,000
2027	Upgrade to the devices (sensors) used to monitor network traffic within operational technology ("OT") environments. This capability ensures we can monitor and log potentially malicious behavior and traffic from OT assets.	2CR08C804	OT Cybersecurity	High	440,682	2,497,199	2,937,881
2027 Total					965,682	5,472,199	6,437,881
2028	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2028 Total					472,500	2,677,500	3,150,000
2029	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2029 Total					472,500	2,677,500	3,150,000
2030	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2030	Platform that enables workflows, cataloguing, tracking and assignment of ownership for operational technology ("OT") vulnerabilities and their associated remediation and/or risk management activities.	2CR08C804	OT Cybersecurity	High	240,603	1,363,414	1,604,017
2030 Total					713,103	4,040,914	4,754,017
2031	Investments in security technologies, platforms and services that enable security controls, visibility of threats and vulnerabilities within our operational technology ("OT") environments.	2CR08C804	OT Cybersecurity	High	472,500	2,677,500	3,150,000
2031	Upgrade to the devices (sensors) used to monitor network traffic within operational technology ("OT") environments. This capability ensures we can monitor and log potentially malicious behavior and traffic from OT assets.	2CR08C804	OT Cybersecurity	High	408,512	2,314,904	2,723,416
2031 Total					881,012	4,992,404	5,873,416
Grand Total					4,833,905	27,392,131	32,226,036

Mitigation Level Units: 25k Users Protected

Southern California Gas Company
2025 RAMP
Capital Workpapers

2CR08C805 - SCG-Risk-8 Cybersecurity IT Infrastructure Modernization							
Forecast Year	Description (Public)	RAMP Workpaper Group	Mitigation	Portfolio Impact	Labor	Non-Labor	Total
2025	Investment in our enterprise licenses for our firewalls which function as our primary perimeter defense capability.	2CR08C805	IT Infrastructure Modernization	High	1,165,698	6,605,622	7,771,319
2025 Total					1,165,698	6,605,622	7,771,319
2026	Replacement of obsolete, end of life/end of service hardware that runs firewalls, protecting the company from threats and malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	227,534	1,289,357	1,516,890
2026 Total					227,534	1,289,357	1,516,890
2027	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	234,360	1,328,037	1,562,397
2027 Total					234,360	1,328,037	1,562,397
2028	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	217,251	1,231,091	1,448,342
2028 Total					217,251	1,231,091	1,448,342
2029	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	223,769	1,268,023	1,491,792
2029	Enhancement, replacement or upgrades to advanced threat protection tools, software, capabilities	2CR08C805	IT Infrastructure Modernization	High	675,000	3,825,000	4,500,000
2029 Total					898,769	5,093,023	5,991,792
2030	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	290,900	1,648,431	1,939,330
2030 Total					290,900	1,648,431	1,939,330
2031	Enhancement, replacement or upgrades to our core firewall infrastructure hardware. This hardware enables our primary line of defense against malicious traffic.	2CR08C805	IT Infrastructure Modernization	High	299,626	1,697,883	1,997,509
2031 Total					299,626	1,697,883	1,997,509
Grand Total					3,334,137	18,893,443	22,227,579

Mitigation Level Units: 25k Users Protected

Appendix A: Forecast Methodology

Mitigation ID	Mitigation Name	Labor	Non-Labor	NSE	Units
A801	Alternative Portfolio 1	Zero-Based	Zero-Based	Zero-Based	Zero-Based
A802	Alternative Portfolio 2	Zero-Based	Zero-Based	Zero-Based	Zero-Based
C801	Perimeter Defenses	Zero-Based	Zero-Based	Zero-Based	Zero-Based
C802	Internal Defenses	Zero-Based	Zero-Based	Zero-Based	Zero-Based
C803	Sensitive Data Protection	Zero-Based	Zero-Based	Zero-Based	Zero-Based
C804	Operational Technology (OT) Cybersecurity	Zero-Based	Zero-Based	Zero-Based	Zero-Based
C805	IT Infrastructure Modernization	Zero-Based	Zero-Based	Zero-Based	Zero-Based

Risk Chapter: **SCG-Risk-8 Cybersecurity**
Risk ID: **2CR08**

Appendix B: Unit Measure

Mitigation ID	Mitigation Name	Unit Measure
A801	Alternative Portfolio 1	Users Protected
A802	Alternative Portfolio 2	Users Protected
C801	Perimeter Defenses	Users Protected
C802	Internal Defenses	Users Protected
C803	Sensitive Data Protection	Users Protected
C804	Operational Technology (OT) Cybersecurity	Users Protected
C805	IT Infrastructure Modernization	Users Protected