360° ENTERPRISE RISK ASSESSMENT

INDUSTRY-LEADING 360-DEGREE CYBERSECURITY RISK ASSESSMENT FROM CRITICALITY ANLAYSIS TO STRATEGIC ROADMAP

Public and private sector entities across diverse markets – utilities, energy, transportation, telecommunications, healthcare, finance, and state and local governments – rely upon Peraton Labs to provide enterprise-level assessments of their security posture and strategic consulting to balance business needs and risks and prioritize cybersecurity investments. Customers trust Peraton Labs' proven 360-degree Enterprise Risk Assessment services to provide a holistic view based on their critical processes and business systems, their threat landscape, and their people, process, technology, and infrastructure. Our Enterprise Risk Assessment is an industry-leading approach for strategic cybersecurity assessment and planning that measures current state, defines desired state, and presents a roadmap to help leadership close the gap to a more secure business.

Peraton | LABS

1. EXECUTIVE SUMMARY

Peraton Labs' 360° Enterprise Risk Assessment helps public and private sector organizations across diverse markets – utilities, energy, telecommunications, healthcare, finance, transportation, and state and local governments – determine their cybersecurity posture, prioritize their cybersecurity risks, and implement an informed, risk-based cybersecurity program to support their mission.

Enterprise cybersecurity exists to mitigate and manage business risks resulting from adversarial exploitation of a business's people, processes, and technology. Like all business risks, the threats, possible consequences, and likelihood of occurrence need to be weighed against the cost of the migration plan. Peraton Labs' 360° Enterprise Risk Assessment helps businesses determine their cybersecurity posture, prioritize their cybersecurity risks, and implement an informed, risk-based cybersecurity program to support their mission.

For decades, large enterprise and critical infrastructure operators have trusted Peraton Labs to provide in-depth security and risk assessments to identify and help manage their cybersecurity business risks. Peraton Labs proven "360-degree" Enterprise Risk Assessment Services provide a formal, enterprise-wide, security evaluation to prioritize cybersecurity needs and build, operate, and refine an effective end-to-end security management program based on a risk-quantified approach. Using a systematic process to identify, assess, and manage cybersecurity risk, the Peraton Labs 360° Enterprise Risk Assessment identifies and prioritizes risk scenarios and potential for loss, profiles the current state of cybersecurity, defines the desired state, and constructs a gap profile to identify where to invest the available cybersecurity budget.

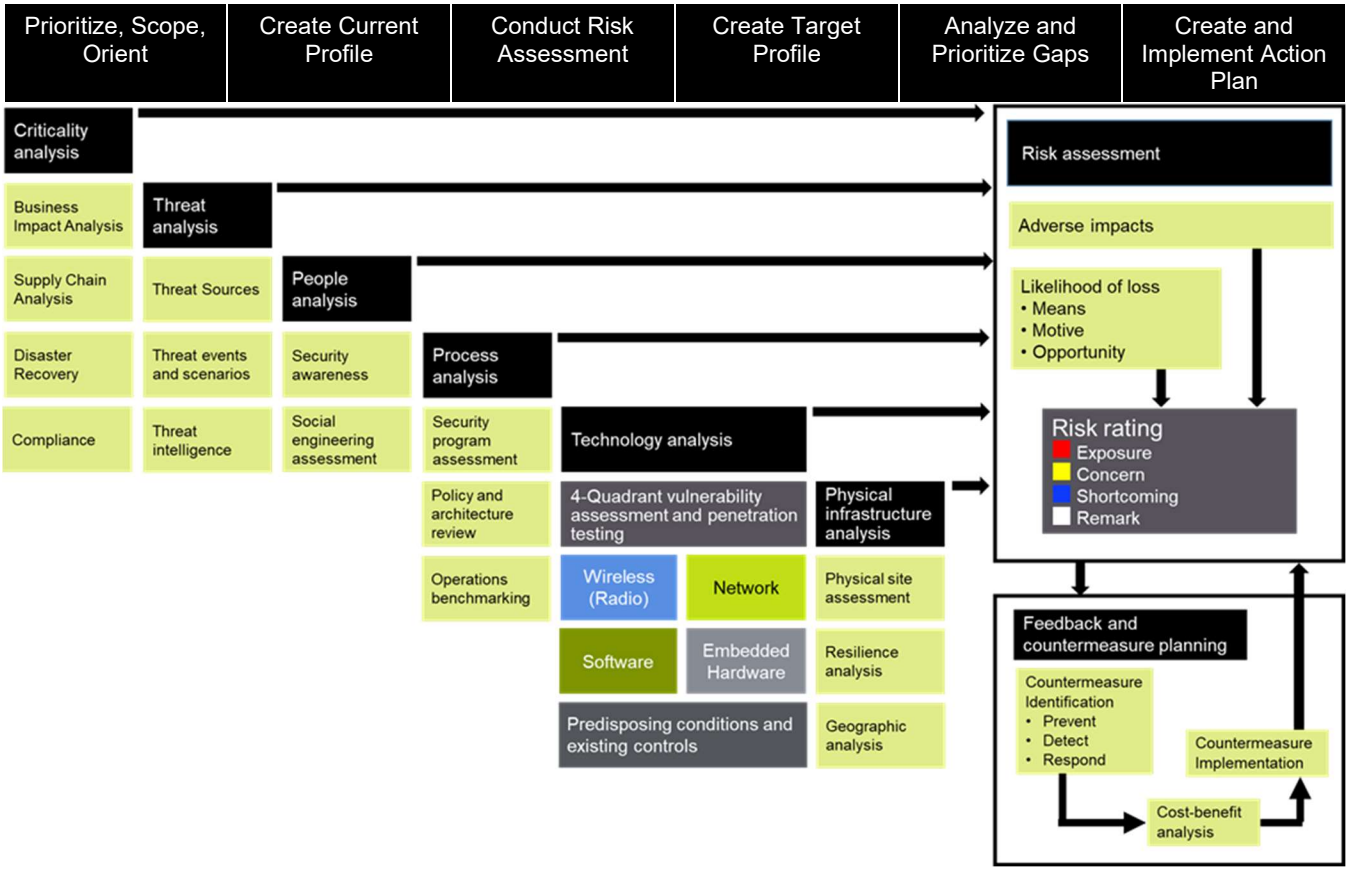


Figure 1: Peraton Labs 360° enterprise risk and security assessment methodology

Peraton Labs uses the NIST Cybersecurity Framework (CSF) as a foundation for its 360° Enterprise Risk Assessment to formally:

1. Prioritize, scope, and orient the risk assessment
2. Describe an organization's current cybersecurity posture
3. Formulate a desired, future target cybersecurity posture based on a risk-quantified approach
4. Identify gaps and prioritize improvements for critical functions
5. Communicate the entity's cybersecurity risk profile, decision process, and plan of action to stakeholders
6. Provide a means to assess progress toward achieving the desired target state

The CSF is widely applicable across many business sectors and helps users manage their cybersecurity needs as part of their organization's business risk management processes. The Peraton Labs 360° Enterprise Risk Assessment structures these activities into five major analyses:

- Criticality Analysis
- Threat Analysis
- People, Process, and Technology Analysis
- Physical Infrastructure Assessment
- Overall Risk Assessment

Our approach seeks to identify critical business functions and systems, define the threats to these systems, assess the current state of cybersecurity controls and processes employed in daily operations, and identify vulnerabilities that could be exploited by adversaries. The results of each analysis feed an overall risk assessment with defined risk ratings that enable enterprises to understand their current cybersecurity posture and implement an informed, risk-based cybersecurity program that supports their mission to reach their desired target posture.

2. CRITICALITY ANALYSIS

Peraton Labs performs a criticality analysis to identify and prioritize the most important business assets, systems, and processes needed for continuity of operations and protection of key business assets. Loss of these systems and assets due to any reason, including cyberattack, undermine business continuity. Systems identified by the criticality analysis are used to focus the remaining efforts of the risk assessment.

Business impact analysis

Business impact analysis focuses on business processes and their supporting applications, networks, personnel, resources, critical relationships to internal and external organizations, and interdependencies. Corruption or disablement of these resources or business process can lead to degradation or mission failure. We identify and group mission systems, including customer care systems, customer engagement portals, ICS/SCADA systems, asset management and location systems, document management systems, workforce management systems, configuration management systems, IT administrative systems, and employee systems. We identify important data flows for information exchange, decompose interdependences into their constituent functions, and assign criticality levels. We map the system architecture of mission-critical functions and identify the infrastructure components that implement those functions. We work with you to assign criticality levels to each component in proportion to the consequence of their failure on the system's ability to perform its mission. Where applicable, we apply Department of Defense (DOD) Trusted Systems and Network techniques and relevant commercial standards. We work collaboratively with managers and executives across the organization in a structured approach to ensure proper balance, drill down to the components that support the top three to five critical business processes, and identify recovery time and recovery point objectives, risk impacts, tolerances, constraints, and trade-offs.

Supply chain analysis

As product supply chains become increasingly global and complex, the threats they pose become more serious and harder to track – especially as they extend to off-shore services, systems, and software, each with their own supply chain. Supply chain concerns apply equally to services provided by contractors, vendors, hosted, and cloud services. A growing attack vector is to target companies by infiltrating their services' supply chain. Your security policies and practices need to flowed through your supply chain to prevent attacks over the weakest link. Our supply chain analysis assesses use of procedural, physical, technical, and contractual controls to safeguard supply chain integrity. We help identify cybersecurity risks inherent in procured products and services, IT infrastructure access, and data sharing arrangements.

Disaster recovery

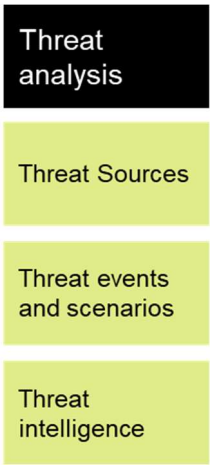
We help customers fortify their emergency management program to organize and manage their resources and responsibilities for dealing with all aspects of emergencies such as preparedness, response, Continuity of Operations (COOP), incident mitigation, and recovery. The aim is to reduce the harmful effects of all hazards, including physical and cyber disasters. We help customers focus on preparing people, processes, technology, and physical infrastructure to be available as needed after a negative event occurs. Our recommendations seek to reduce our customer's vulnerability to disaster, mitigate the impacts of a disaster, or respond more efficiently in an emergency. Our services are flexible and customizable and can include COOP planning to ensure that organizations are able to continue performance of essential functions under a broad range of circumstances. They can also include disaster recovery planning for specific organizations, processes, or functionality.

Compliance

Regulatory compliance encompasses organizational efforts to ensure awareness of and compliance with laws and regulations relevant to their business sector. Our services help determine and interpret the growing number of relevant requirements your business faces, develop cost-effective response plans, and estimate costs for non-compliance in fines, penalties, and litigation. We also assess the negative business impacts of non-compliance such as loss of customers, investor concerns, and impacts of exposing assets to cyberattacks.

3. THREAT ANALYSIS

Peraton Labs conducts a formal threat analysis to develop an adversary model and identify threat scenarios to the customer's industry, company, and critical assets. The threat analysis considers threat sources with different capabilities and motive-driven, threat scenarios. A list of high-risk scenarios is developed, which later guide the prioritization of security control improvements as well as the technical vulnerability assessment and penetration testing.



Threat sources

The threat analysis identifies motivated adversaries called threat sources applicable to customer's business operation. We leverage a broad range of threat actors using industry, government, and intelligence sources, such as:

- National Electric Sector Cybersecurity Organization Resource (NESCOR) https://smartgrid.epri.com/NESCOR.aspx
- Department of Homeland Security (DHS)
- National Cybersecurity and Communications Integration Center (NCCIC) https://www.cisa.gov/publication/connecting-nicc-and-nccic
- Idaho National Laboratory (INL)

- Cloud Security Alliance https://cloudsecurityalliance.org
- North American Electric Reliability Corporation (NERC)
- Critical Infrastructure Protection (CIP) standards
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) https://us-cert.cisa.gov/ics
- Peraton Labs industry domain expertise.

Leveraging a variety of sources helps to get different perspectives into the analysis and reduce any subjectivity inherent in the process. Peraton Labs identifies threat agent types to model nation-states, terrorists, industrial spies, organized crime groups, hacktivists, hackers, and insiders – including those perpetrators with authorized privileges beyond basic user privileges such as employees, contractors, trusted partner staff, and vendors. Our multifaceted threat categories each have their own capabilities, intent, and targeting characteristics which generate independent likelihoods and impacts of a threat event. The results are used to feed into threat event and scenario analysis.

Threat events and scenarios

Peraton Labs identifies threat scenarios or events, which are a sequence of adversary actions that can lead to an undesired outcome (Impact), such as damage to or loss of an asset, disruption of a service, exploitation of information systems, data loss, or harm to people. We consider threat scenarios across the domains of people, process, and technology, including supply chain threats. Peraton Labs applies its domain knowledge, references authoritative sources, and considers the current worldwide threat landscape. Threat scenarios are matched to threat agents known to conduct such activities and each combination is assigned a risk rating.

Peraton Labs evaluates threat scenario risk by considering Means, Motive and Opportunity.

- **Means** – A measure of the skill, knowledge, and resources required to execute the threat scenario/exploit the vulnerability.
- **Motive** – A measure of the highest level of interest among threat agents to inflict damage by successfully executing the threat scenario/exploiting the vulnerability.
- **Opportunity** – A measure of highest occurrence among threat agents for an occasion to successfully execute the threat scenario/exploit the vulnerability.

Existing cybersecurity controls and predisposing conditions are factored into the analysis to adjust risk. The threat analysis allows us to prioritize specific security controls to counteract high risk scenarios in the development of the NIST CSF future state and the gap security profiles.

Threat intelligence

Peraton Labs assesses your threat intelligence efforts to determine if they are achieving the key mission to research and analyze emerging threats, trends, and technical developments. Peraton Labs subsequently applies this information to help your company understand threats and mitigation approaches and to ultimately reduce enterprise risk and incident recovery time. We look at all threat categories applicable to your industry – how you are gathering, assessing, and distributing information – and if the appropriate feedback loops and continuous service improvement processes are working. We look at attacker tactics, techniques, and procedures. We assess the automated detection tools used to aggregate, correlate, and analyze threat data to support defensive actions. The goal is to migrate customers to a predictive cybersecurity posture where better decision-making occurs both during and following incidents, as opposed to being reactive to threat occurrences.

4. PEOPLE, PROCESS, AND TECHNOLOGY ANALYSIS

Peraton Labs evaluates security risk across People, Process, and Technology using three methods:

- **Policy and Architecture Review**: We review security policy and procedure documents and analyze architectural diagrams of critical networks and systems to understand the intended controls, methods of operations, and as-built designs, and to note gaps and deficiencies against best industry practices.
- **Structured Interviews**: We conduct structured interviews with system owners and managers to facilitate a thorough understanding, achieve clarification, and determine the maturity of policy, procedures, and system implementations.
- **Test and Validation**: We conduct social engineering assessments and vulnerability and penetration testing to validate the implementation of security controls and hunt for vulnerabilities using our signature 4-Quadrant™ Vulnerability Assessment methodology.

Peraton Labs applies the NIST CSF and its proven security capability maturity model to assess an organization's cybersecurity posture by security function. Peraton Labs creates a current state cybersecurity profile using the five NIST CSF security functions (Identify, Protect, Detect, Respond, and Recover), rating the presence and level of implementation for each subcategory control based on collected artifacts and observations.

PEOPLE ANALYSIS

People are among a business' most valuable and dynamic assets, making them both critical to business operations and a potential adversarial target. To address risks associated with employee behaviors, Peraton Labs analyzes security awareness and conducts social engineering assessments.

People analysis

Security awareness

Social engineering assessment

Security awareness

The Peraton Labs' security awareness and social engineering security assessment services help companies benchmark and build a culture of security, where employees are knowledgeable of company policies, aware of the ways they are being targeted by attackers, more confident in their decision-making, and empowered to participate in attack identification and prevention. Our approach is based upon four key actions:

- Identify risk,
- Change behavior,
- Reduce exposure, and
- Measure and adapt.

The core components of our approach are policies and procedures, awareness training, and social engineering assessments. We review your policies, procedures, and cyber training, and observe and interview employees as they perform their normal daily activities. We identify out-of-date and deficient policies as well as policies that are not well-practiced by the employee population that result in business risk. We advise on recommendations to improve and change the culture to be more aware of each person's role in protecting company operation and assets.

Social engineering assessment

Social engineering is the clever manipulation of the natural human tendency to trust others in order to elicit data, sensitive business or infrastructure information, or credentials to support an adversarial attack. Industry studies continue to show that social engineering is an effective attack vector. Ransomware attacks tend to follow a model

where the target is first infiltrated using phishing attacks, whereupon malicious actors pivot and move laterally into the critical business systems to deploy ransomware or exfiltrate sensitive data.

Social engineering assessments identify security risks associated with employee and contractor behavior, poorly implemented personnel security policies, and lack of knowledge of procedures, often resulting from insufficient or ineffective security awareness training. Our Social Engineering Assessments use custom scenarios tailored to the client's business operations to help an organization improve its operational security related to:

- Employee Credential Protection,
- Device Security, Session Management, and Portable Media,
- Physical Security and Controlled Access for people and goods,
- Email Security, and
- Information Protection for Company Confidential, Personally Identifiable Information, Protected Critical Infrastructure Information (PCII), and Critical Cyber Assets.

Peraton Labs creates a custom campaign by performing open-source research, working with a client's security organization to understand policies, functions, and roles, and conducting onsite reconnaissance to understand the customer's operation and improve the ruse's appearance of legitimacy and deception. Peraton Labs creates designs, storyboards, selects the acting talent, and implements the ruse to take advantage of the good nature and natural helpfulness of most employees, any vagueness in company policies, and employees, who may be careless, inattentive, or lack of understanding of policy. Typical campaigns include, but are not limited to:

1. Phishing/spear phishing/whaling,
2. Phone-based social engineering,
3. Rogue Wi-Fi network access points,
4. Physical Site (tailgating, "talk your way"), and
5. Exploitable portable media.

See our **Social Engineering Assessment** whitepaper, available at Vulnerability and risk analysis - Peraton Labs, for more information about our approach for protecting against the biggest cyberattack threat vector.

PROCESS ANALYSIS

Processes are as central to a strong cybersecurity posture as they are to business flows and quality assurance. Peraton Labs assesses how your business policies and standards work to secure your business assets, data, and your customers' data.

Security program assessment

Our enterprise-wide security program assessment seeks to evaluate the effectiveness and pervasiveness of your company's business risks and aid you in making informed decisions. We search for artifacts that demonstrate how your company is dutifully implementing those policies and controls in practice and we render an opinion on whether you have sufficient and effective coverage based on our findings, experience, and industry best practices. Peraton Labs applies its proven assessment methodology and maturity model to evaluate your security program objectively and independently. Peraton Labs assesses the adequacy and implementation of security policies and their use in daily operations by analyzing daily practices, critical policies, and procedures, as well as holding in-depth structured interviews with stakeholders and key organizations. We apply our comprehensive security maturity model, which addresses over 30 areas and incorporates principles from multiple standards frameworks, including European Union consumer data regulations and state legislation in the U.S. concerning consumers' rights of the use and protection of their data. We highlight strengths and weaknesses in your security program and present key

findings along with practical recommendations for improvement. This approach has proven effective to identify inconsistencies between what employees should be doing versus what they may be actually doing and why.

Security Policy and Architecture Review

Peraton Labs helps organizations architect and deploy practical, defense-in-depth security strategies. Beginning with business needs and environmental assessments, we help you establish the primary technical and operational security requirements for your organization. Based on these requirements, we formulate a cohesive set of security policies tailored to your organization's unique needs using industry best practices. We help you implement these policies with robust security architectures, such as Zero Trust Architecture (ZTA), and develop more trustworthy systems across the entire system life cycle by employing disciplined cyber resiliency engineering, solution assessment and selection, operational procedures, training, and enforcement programs to effectively ingrain a higher level of security into your day-to-day operations. Our objective position allows us to provide forthright opinions about product selection, program effectiveness, and cost-benefit trade-offs.

Table 1: Function and Category Unique Identifiers (reproduced from NIST CSF, v 1.1, pg. 23).

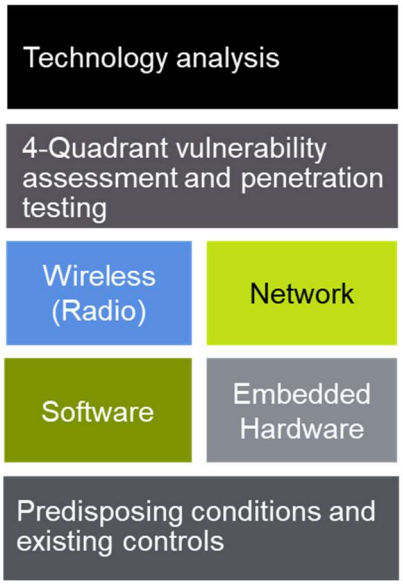
Function Unique Identifier	Function	Category Unique Identifier	Category
Identify	ID	ID.AM	Asset Management
		ID.BE	Business Environment
		ID. GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
Protect	PR	PR.AC	Identity Management, Authentication & Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR. IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
Detect	DE	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE. DP	Detection Processes
Respond	RS	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
Recover	RC	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Current State Cybersecurity Profile / Operations Benchmarking

We apply the NIST CSF and its proven security capability maturity model to assess an organization's cybersecurity posture by security function. We create a current state cybersecurity profile using the five NIST CSF security functions (Identify, Protect, Detect, Respond, and Recover), rating the presence and level of implementation for each subcategory control.

With vast experience in government and enterprise network operations centers, we can also evaluate your effectiveness compared to similar enterprises, as well as the operating procedures they use to detect, respond to, and contain malicious events and network failures. Our cyber intrusion exercise is a unique Peraton Labs security services offering that goes beyond traditional red/blue team exercises. In it, we orchestrate a realistic series of cyber events based on your network that are played out in an interactive table-top environment. The goal is to assess and improve the effectiveness of the network operations center staff by training them to correlate information from a variety of sources in order to diagnose malicious cyber problems; identify a multipart attack from independent, random events; effectively communicate inside and outside the organization; organize a response; and perform in high-stress situations.

TECHNOLOGY ANALYSIS



Businesses depend upon information and operations technology to operate and deliver goods and services. Networking, software, and automation technologies rapidly evolve and pose complex security challenges. Technical vulnerabilities in their architecture, implementation and configuration provide exploit opportunities that result in business risk.

4-Quadrant Vulnerability Assessment and Penetration Testing

Peraton Labs applies its proven 4-Quadrant™ Vulnerability Assessment Methodology to assess technical weaknesses in information technology and operation systems. With over 35 years of experience securing critical infrastructure and authoring industry best practices, Peraton Labs covers four distinct quadrants of the technology vulnerability space. Our 4-Quandrant approach extends traditional information technology (IT) vulnerability assessment and penetration testing for on-premises Web and business applications, servers, and network infrastructure to address hosted operations and cloud infrastructures, wireless systems and embedded devices for IoT, and cyber-physical systems. In a twofold approach, we first validate the existence and operation of design-driven security controls. Informed by a threat analysis of the system architecture, we then discover means to circumvent those security controls to exploit design, implementation, and configuration weaknesses.

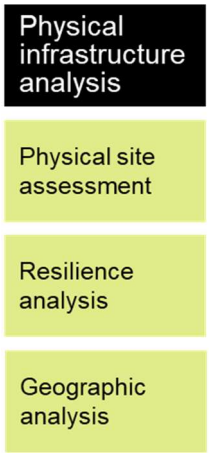
Information and Operations technology identified in the criticality analysis is subject to in-depth vulnerability assessment and penetration testing using Peraton Labs 4-Quadrant Security Assessment Methodology. Our penetration testing seeks to simulate a real-world attack on your networks, systems, and data to evaluate the risk profile of your environment. This includes understanding the level of skill required and time needed for an attacker to exploit each vulnerability and the level of impact to your organization if the attack is successful. Linking together the findings from each of the four quadrants, Peraton Labs develops a holistic and integrated view to expose risks not apparent when looking at a single technology domain.

To assist in selecting methods of migration, Peraton Labs constructs attack trees to visualize how a combination of vulnerabilities from across the quadrants can be linked together to achieve larger exploitation goals. When read left-to-right, the attack trees highlight exploit path dependencies that can be pruned to thwart attacks. When read right-to-left, they show the various ways an adversary can achieve a particular goal. While a single “break” in the attack chain may be sufficient to block an exploit, it is often best to create multiple attack chain “breaks.” See our **4-Quadrant Vulnerability Assessment and Penetration Testing** whitepaper, available at Vulnerability and risk analysis - Peraton Labs, for more information about our technical vulnerability approach.

Predisposing conditions and existing controls

Peraton Labs assesses predisposing conditions, which may be vulnerabilities or factors influencing threat opportunities in either a positive or negative direction. They may include geography and environmental factors, regulatory and compliance, financial, personnel, technology, supply chain, or contractual constraints or opportunities. We factor the predisposing conditions of your business and infrastructure into the risk assessment using the taxonomy structure outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

5. PHYSICAL INFRASTRUCTURE ANALYSIS



Security risks can arise from the physical infrastructure supporting business operations and service delivery, especially for critical infrastructure operators. Physical infrastructure includes power, environmental, and building automation, WAN connectivity, and site physical security. Physical systems are subject to electronic and physical attack. Such infrastructure is controlled by Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems, which are outside of IT operations and present unique risks.

Physical site assessment

Peraton Labs performs physical infrastructure assessment of data centers, administration buildings, factories, equipment yards, and control facilities by deploying a team to observe and inspect a facility from "basement to roof." Site walk-throughs evaluate the structure, its location, vicinity to civil, kinetic, and weather events, physical controls, and practices to maintain and monitor the external facility security perimeter as well as compartments within the facility. Peraton Labs evaluates data, electrical, fuel service, and HVAC systems and their redundancy, backup, and diversity, both entering the building and within building compartments.

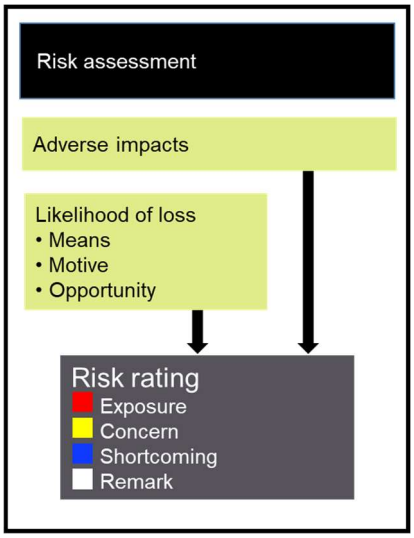
Resilience analysis

This analysis assesses risks due to insufficient redundancy and diversity in the customer's infrastructure that could result in interruption of service and business operations. Peraton Labs analyzes logical and physical diversity of critical site systems, path diversity of cable routes, carriers' diversity for WANs, diversity of commercial power sources, site redundancy, and continuity and disaster recovery plans.

Geographic analysis

A traditional risk component is location hazards due to natural, man-made, and accidental events. As part of site inspections, Peraton Labs evaluates the location and environmental risks of physical plants. We reference historical data for weather, flood, fire, and crime events and assess whether compensating controls are present to mitigate risks. For example, flood prone areas may require elevated fuel storage tanks and back-up generation capability at a higher location instead of the basement. In other cases, natural events such as earthquakes, volcanic activity, tornados, and proximity to industrial sites require special site construction and risk consideration.

6. OVERALL RISK ASSESSMENT



The formal risk analysis is the final and key component of Peraton Labs' 360° Enterprise Risk Assessment. It synthesizes information collected during the analyses of criticality, threats, people/process/technology, and physical infrastructure, and produces several key outputs:

- Customized risk ratings
- Security gap profile
- Feedback and countermeasure planning

Risk management is the process of identifying, assessing, and responding to conditions that could negatively affect a business. To manage risk, organizations need to understand the existence of a threat, the likelihood that a threat scenario will occur, and the resulting impact on the organization's critical functions. With this information, organizations can determine the acceptable level of risk for delivery of services and express their risk tolerance in the form of a cost-effective cybersecurity program.

RISK RATINGS

The formal risk ratings are key components of Peraton Labs 360° Enterprise Risk Assessment. They are based on the information collected during the criticality analysis, threat analysis, and the people/process/technology and physical infrastructure assessments. The Criticality Analysis has identified the essential business functions and associated infrastructure. The Threat Analysis has outlined the threat landscape, threat sources, and attack scenarios, ranking the scenario risk and aligning scenarios to the essential business functions. The evaluation of People, Process and Technology has resulted in a current state cybersecurity profile structured according to the security categories of the NIST CSF. Actual technical weaknesses in the technology infrastructure for essential business systems have been documented by the 4-Quandrant Vulnerability and Penetration Testing.

Peraton Labs evaluates overall risk by evaluating the combination of:

1) Threats
2) Potential for Loss
3) Current State Cybersecurity Posture
4) Infrastructure Vulnerabilities

Potential for loss encompasses the probability (likelihood) that loss will occur, and the magnitude of the potential loss (Impact) under NIST SP 800-30. Peraton Labs relies on its experience working with numerous customer environments to estimate likelihood of occurrence and also factors in infrastructure vulnerabilities and the current state cybersecurity posture. Vulnerabilities in this analysis are weaknesses that threat agents exploit in people, processes, and technology. Peraton Labs develops a custom Impact scale appropriate to the client's business. For critical infrastructure operators, impact categories may include Interruption of Power, Safety Impact, Environmental Damage, Financial Loss, Data or System Breaches, Customer Impact, and Public Image Impact. Peraton Labs links the top-down threat assessment that identified the threat sources and scenarios with the potential for loss, the current state cybersecurity posture, and the discovered vulnerabilities to identify top risks by critical business function.

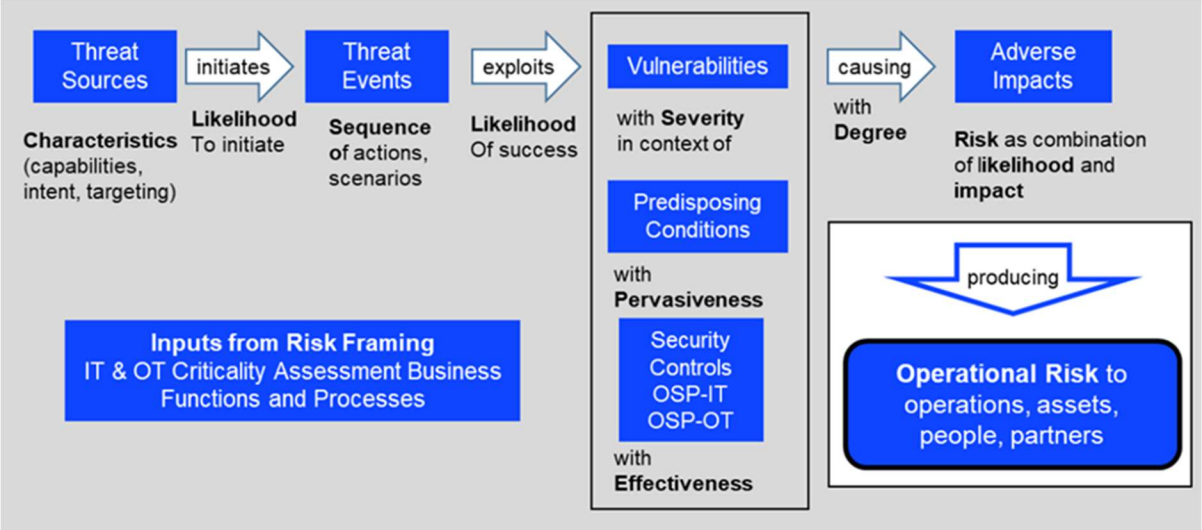


Figure 2: Peraton Labs application of NIST SP 800-30 risk model with key risk factors

Finally, Peraton Labs aligns the top risks to those security functions in the NIST CSF profile that will provide the most benefit for mitigation. We then work with the customer to define the desired future state of its cybersecurity controls and to:

1) Evaluate the courses of action to respond to the risks,
2) Decide on the appropriate courses of action based on the client's risk tolerance,
3) Implement the selected courses of action, and
4) Monitor ongoing risk.

SECURITY GAP PROFILE

A Gap Profile is created to identify areas where investment is needed to reach the desired state. The profile points out where investment is needed, but also where cost savings are possible by reducing a capability. The profile becomes the basis to construct a multi-year remediation program with a Plan of Actions and Milestones (POAM).

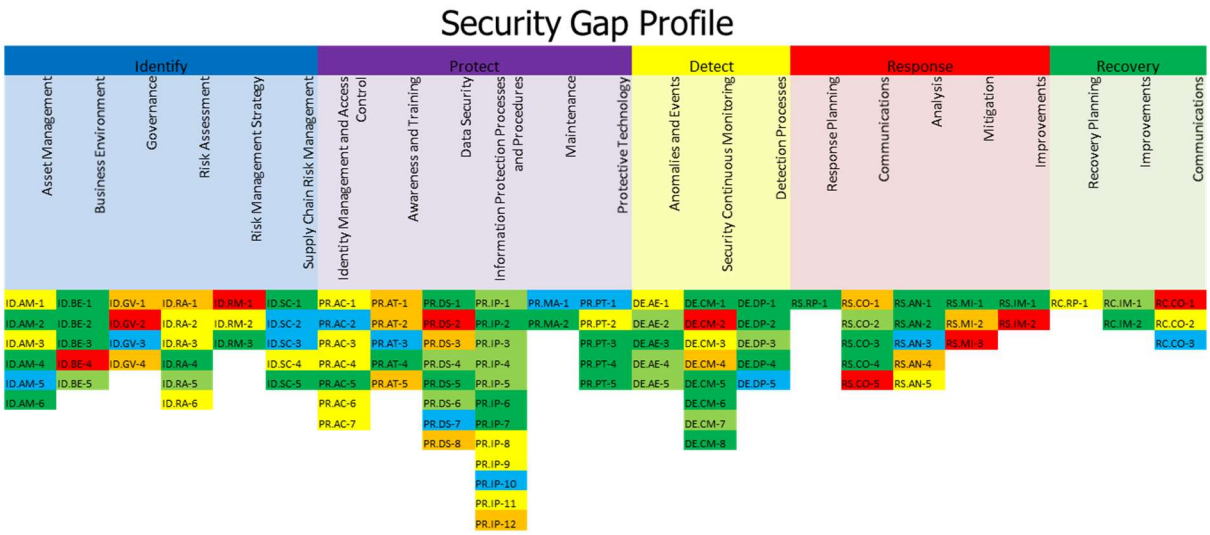


Figure 3: Example Security Gap Profile chart employing the NIST Cybersecurity Framework

At the conclusion of the risk assessment, Peraton Labs provides a risk assessment report and in some cases an Excel-based risk assessment tool summarizing the analysis, operational risks, gaps, and recommendations. In addition to the threat analysis and gap profile, Peraton Labs documents specific findings, interpretation of risk and recommendations. The deliverable report consisting of the following sections:

- Executive Summary;
- Findings Overview;
- Scope and Methodology;
- Test Environment; and
- Detailed Security Findings.

The Executive Summary provides a management level overview of the key findings, an assessment of threat and risk, and top-level recommendations for remediation.

The Findings Overview provides one or more matrices to summarize the findings. Each finding will be listed with a descriptive title, its severity rating, the applicable security domain, the objective observation/measurement, and, as deemed appropriate, the hardware, configuration, and firmware version of the component to which the finding applies.

The Scope and Methodology defines the applications, network infrastructure, systems, and components under assessment, the technical approach used by Peraton Labs to perform the authorized assessment, and the risk assessment methodology to rate the findings.

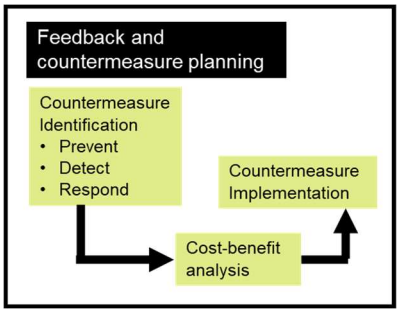
The Test Environment details the configuration of the environment used to conduct the testing, the product model, software version, hardware version, and firmware of the components tested, and the test equipment and tools used by Peraton Labs, as applicable.

The Detailed Security Findings present each finding, which will be assigned one of four severity levels based on Peraton Labs' risk assessment model (unless otherwise agreed). Peraton Labs' four-tier rating system uses these severity ratings:

- An **Exposure** (high risk) is a vulnerability or security weakness with a proven or highly probable method of exploitation.
- A **Concern** (medium risk) is a security weakness that either satisfies known threat objectives or can result in significant damage if successfully exploited, but not both.
- A **Shortcoming** (low risk) is a security weakness that does not satisfy known threat objectives and will not result in significant damage if successfully exploited.
- A **Remark** documents an item worthy of note.

FEEDBACK AND CONTERMEASURE PLANNING

To reduce the likelihood that threat events will result in adverse impacts, Peraton Labs helps customers assess threat intelligence and current countermeasures, and plan future safeguards and countermeasures proportional with the risks appropriate for their business.



Countermeasure identification

Once threats and vulnerabilities are identified and ranked, Peraton Labs helps customers explore alternative tactical and strategic countermeasures to enhance their risk reduction capabilities, achieve the goals of their security program to prevent-detect-respond, and meet their enterprise appetite for risk. We finish with addressing the feedback needed to support your continual service improvement program.

Cost-benefit analysis

We help you develop a realistic cost-benefit model and recommendations that synchronize with your company's business goals and compliance requirements and work with you through the decision-making process. We help you assess which technologies best help you reach your highest priority goals.

Countermeasure implementation

Using our plan, design, build, and operate model, we help customers negotiate the new technology insertion process, including using agile methods to develop of prioritized requirements with stakeholders, issue and assess solicitations, and manage vendor trials through value realization. We help you determine the risks and value of cloud services versus native capabilities, and when and how to engage third-party providers.

7. SUMMARY

Peraton Labs has successfully supported diverse customers with high-value cybersecurity consulting services. We have conducted assessments and improved security for management and business processes, supply chain and staff, hardware and software, as well as critical network infrastructure, services, applications, media, data and information. Some of the markets we serve include:

- Transportation
- Telecommunications
- Electricity, water, wastewater, energy, and other utilities
- Defense and critical infrastructure
- Finance, banking, and insurance
- Federal, state, regional, and municipal government
- Health care and pharmaceuticals
- Entertainment and media

Built on decades of prominent research and cybersecurity experience in public and commercial sectors, Peraton Labs has an unmatched security perspective. We understand an enterprise's end-to-end security needs and can help you develop the optimum plan for your business.

We understand the importance to your business of customizing the growing number of cybersecurity standards, regulations, and legislative advisories, which are emerging as the use of data grows exponentially and threat agents proliferate. We know that one size does not fit all and can help you tailor solutions to meet your unique needs. Our assessment methodology is intrinsically modular and adapts in scope based on customer needs and budgetary constraints. We bring to bear leading-edge knowledge, deep expertise, and best practices across multiple industries to help improve your security posture and keep your networks secure in these increasingly challenging times. We know what works well and what does not work well in different environments to help you get it right the first time. We appreciate the value of data to all your business processes, the data related attack surfaces they present, and the increased focus on data security by regulators. We treat data as its own domain equal to people, processes, technology, and physical infrastructure to help you comply with regulations and maintain your customers' confidence.

For more information on our security consulting services, contact: info@peratonlabs.com or visit Information assurance and compliance - Peraton Labs and Vulnerability and risk analysis - Peraton Labs.