CALIAN
Confidence. Engineered.

Calian Cybersecurity Program

Stay ahead and secure your organization with a comprehensive annual security plan.

A robust cybersecurity program is essential for safeguarding sensitive data, maintaining customer trust, and ensuring business continuity. By implementing a comprehensive cybersecurity strategy, your organization not only protects itself from potential threats but also demonstrates your commitment to security to clients, partners, and stakeholders.

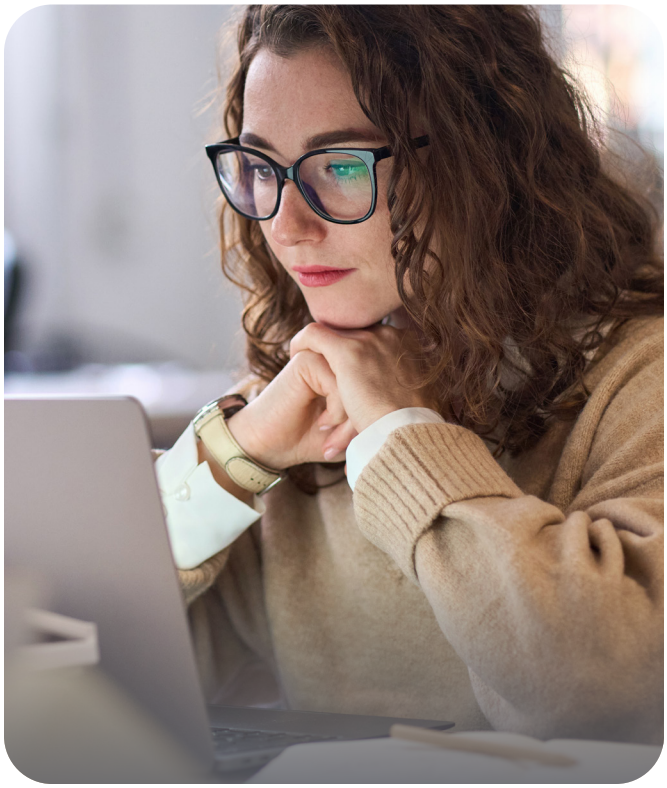
Being prepared is crucial for a strong cybersecurity strategy. This means having the right tools and technologies, and making sure all employees know their roles in keeping the organization secure. Regular training helps everyone understand their part in protecting the organization.

Preparedness also includes having clear incident response plans that can be quickly activated during a cyber incident. Regular practice exercises ensure your team is ready to respond efficiently, minimizing downtime and reducing the impact of breaches.

Pentesting and vulnerability management are key parts of cybersecurity. They help organizations understand their attack surface and reduce it. Regular pentesting finds weaknesses before they can be exploited, while vulnerability management addresses these weaknesses systematically. By being prepared and proactive, organizations can protect their assets and maintain trust with clients and partners.

Why Calian Cybersecurity Program?

- Tailored to your organization's unique needs and team availability.
- Annual critical security activities pre-planned and covered for your organization.
- Flexible payment through monthly or annual plans.
- Planned and delivered by cybersecurity consultants with deep industry expertise.



Our Cybersecurity Plans

Core Defence

Foundation: Establish a strong cybersecurity and incident readiness foundation.

Critical Defence

Enhanced capabilities: Proactively mitigate vulnerabilities and enhance your security posture.

Advanced Defence

Holistic strategy: Comprehensive security planning and strategy for robust protection

Customized Defence

Build your own cybersecurity program with guidance from our expert consultants. Choose from our predefined plans or create a bespoke solution tailored to your requirements

Customized Defence Build your own cybersecurity program	**Core Defence** Cybersecurity program and incident readiness foundation	**Critical Defence** Enhance capabilities and proactively mitigate vulnerabilities	**Advanced Defence** Holistic security planning and strategy
Enterprise Risk Assessment	✓	✓	✓
Incident Response Plan	✓	✓	✓
Incident Response Playbook	✓	✓	✓
Tabletop Exercise	✓	✓	✓
Technical Vulnerability Assessment (Pentest, Ransomware Simulation)		✓	✓
Business Continuity and Disaster Recovery Planning		✓	✓
Vendor Security Review			✓
Vulnerability Management			✓
Cybersecurity Policy Framework Review			✓
Cybersecurity Awareness Training			✓

Program Services Overview

Enterprise Risk Assessment

Calian's enterprise risk assessment is a strategic process used to identify, evaluate and prioritize the potential cybersecurity risks that could hinder an organization's operations, objectives or values. It involves a comprehensive evaluation of internal and external factors, providing a holistic view of potential threats and risks. By identifying risks early, organizations can proactively develop mitigation strategies, ensuring long-term sustainability and resilience.

This process helps in making informed decisions, allocating resources effectively, and maintaining compliance with relevant standards and regulations.

Outcomes:

- **Identification of gaps in cybersecurity controls:** Using a cybersecurity framework, Calian reviews the current state of controls in your organization and compiles these lists as vulnerabilities.
- **Risk evaluation:** An assessment of the likelihood and potential impact of identified risks. Compensating controls are also considered when assigning risk ratings.
- **Mitigation strategies:** Development of risk treatment plans to mitigate or eliminate identified risks, enhancing the organization's security posture.
- **Compliance assurance:** Ensuring the organization meets relevant industry standards, regulations and legal requirements.
- **Remediation priority:** Prioritizing risk remediation plans based on resource capabilities, impact and likelihood of risks.

Incident Response Plan

An incident response (IR) plan is a guide that an organization follows during their response to a cybersecurity incident. It is a strategic document that contains a high-level overview of the entire incident response process. It covers:

- **Preparation:** Establishing and training an incident response team and setting up necessary tools and resources.
- **Detection and analysis:** Identifying and analyzing potential security incidents to determine their scope and impact.
- **Containment:** Implementing measures to limit the spread and impact of the incident.
- **Eradication:** Removing the cause of the incident and ensuring that affected systems are clean.
- **Recovery:** Restoring and validating system functionality to normal operations.
- **Post-incident activities:** Conducting a thorough review to understand the incident, improve future responses and update the plan as needed.

Incident Response Playbook

Calian's incident response (IR) playbooks are comprehensive guides that outline step-by-step instructions on what an organization should do when responding to a specific cybersecurity incident. They serve as a blueprint for security teams to follow, ensuring a coordinated and effective response. Calian IR playbooks are industry aligned and based primarily on the NIST SP800-61 r2 (Computer Security Incident Handling Guide) and NIST SP800-184 (Guide for Cybersecurity Event Recovery), and take into consideration alignment with NIST Cybersecurity Framework, ISO 27001, PIPEDA, and PHIPA. This model is extensible, supporting cyber breaches in sizes from 10s to 1,000,000s of records, and fits with any industry.

Some examples of the threats that IR playbooks can be designed for include:

- Ransomware
- Data exfiltration and data breach
- Malware infections
- Denial of services including DDoS
- Phishing attacks
- Supply chain attacks
- Data loss/leakage
- Insider threats and attacks

Tabletop Exercise

Calian provides two types of tabletop exercises.

- **Senior leadership team IR tabletop:** This tabletop exercise focuses on the activities related to the executive leaders and provides awareness of their roles and responsibilities and key decisions that they will need to make during an incident.
- **IT/technical team incident response tabletop:** This tabletop focuses on the IT/IS and technical teams. It provides awareness of their roles, responsibilities and their activities during the incident response.

Benefits:

- **Improved preparedness:** Ensures all team members understand their roles and responsibilities during an incident.
- **Enhanced communication:** Tests and improves internal and external communication protocols.
- **Identifies gaps:** Reveals weaknesses in the incident response plan and areas for improvement.
- **Builds confidence:** Provides a safe environment for practicing responses to incidents without real-world pressure.
- **Realistic training:** Delivers scenarios based on existing operational plans, ensuring practical and relevant responses.
- **Collaborative thinking:** Encourages teamwork and improves both technical and soft skills necessary for resolution.
- **Security awareness:** Enhances security awareness for executives, senior managers and operational staff.

Technical Vulnerability Assessment (Pentest, Ransomware Simulation)

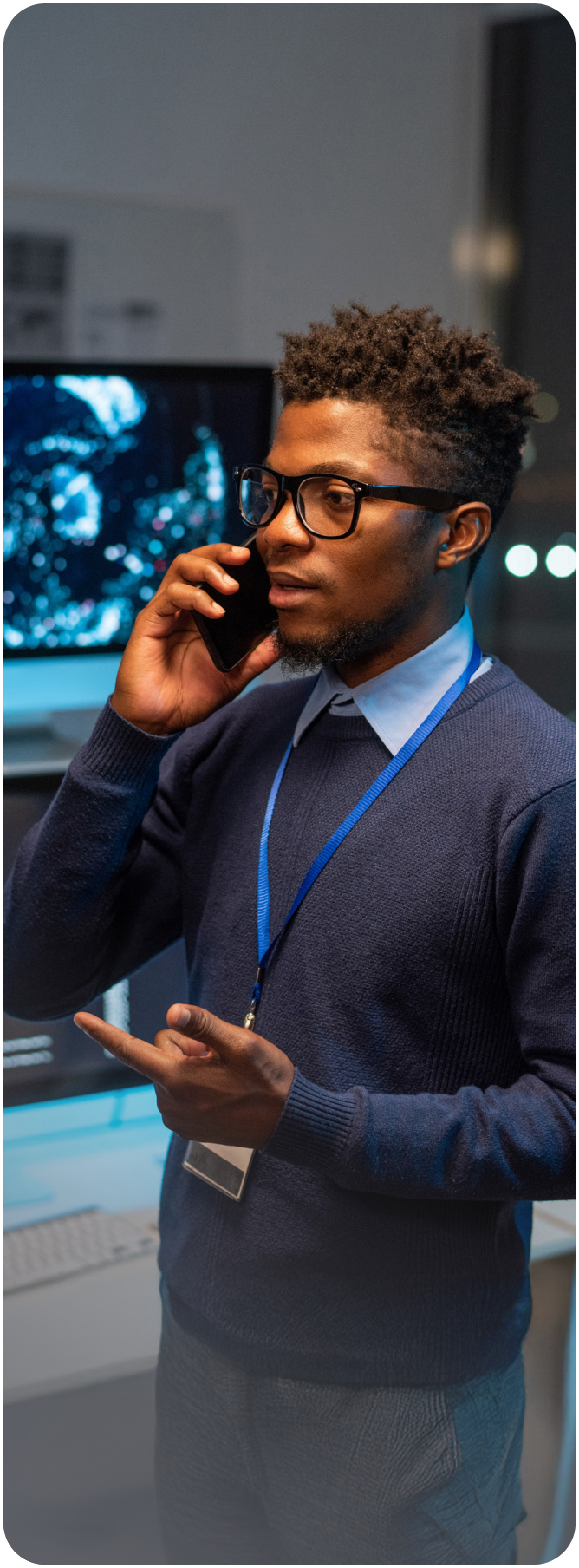
This is a simulated attack conducted by an ethical hacker to identify vulnerabilities in an organization's network environment.

Outcomes:

- A comprehensive overview of the perimeter/assets from an offensive security perspective, indicating all vulnerabilities that can be exploited for malicious intent.
- The insights gained from the pentest enable better decision-making regarding security investments and resource allocation.

By proactively identifying and addressing vulnerabilities, the organization reduces the risk of successful cyberattacks.

- **Identify vulnerabilities:** Detect weaknesses in the network infrastructure, such as misconfigurations, outdated software and unpatched systems.
- **Assess security posture:** Evaluate the effectiveness of existing security measures and identify areas for improvement.
- **Simulate real-world attacks:** Mimic the tactics, techniques and procedures used by malicious actors to understand how an actual attack might unfold.
- **Enhance incident response:** Test the organization's ability to detect, respond to, and recover from security incidents.
- **Ensure compliance:** Verify that the organization meets regulatory and industry standards for cybersecurity.
- **Prioritize remediation:** Provide actionable insights and recommendations to prioritize and address identified vulnerabilities.



Business Continuity and Disaster Recovery Planning

In BCDR, we assist organizations in preparing for and responding to disruptions by developing comprehensive plans that ensure critical business functions can continue during and after a disaster. This involves:

- Conducting a comprehensive assessment to identify critical systems and business operations.
- Performing business impact analyses.
- Creating detailed business continuity and disaster recovery plans.
- Outlining effective backup and recovery solutions.

We also provide crisis management and communication strategies. Our team ensures readiness by regularly testing and updating. Clients benefit from minimized operation downtime, reduced financial and reputation losses during a crisis, and enhanced resilience against cyberattacks, natural disasters and other disruptions.

Vendor Security Review

Our vendor security review service ensures that third-party vendors meet our clients' security standards and do not introduce unnecessary risks to their operations. We perform thorough security assessments, evaluate vendor cybersecurity policies and practices, and deliver detailed risk scoring and reporting. Our team also provides actionable recommendations to mitigate identified risks.

Clients can expect a significant reduction in the risk of data breaches or other security incidents caused by third-party vendors. This service offers assurance that all vendors comply with regulatory requirements, a clear understanding of their security strengths and weaknesses, and improved confidence in the security and integrity of your supply chain.

Vulnerability Management

Calian's vulnerability management service offers comprehensive resources and a detailed process for identifying, evaluating, treating, and reporting on security vulnerabilities in systems and their software. While we advise customers on selecting the right tools, this service focuses on retrieving data, analyzing it, and presenting it to the organization.

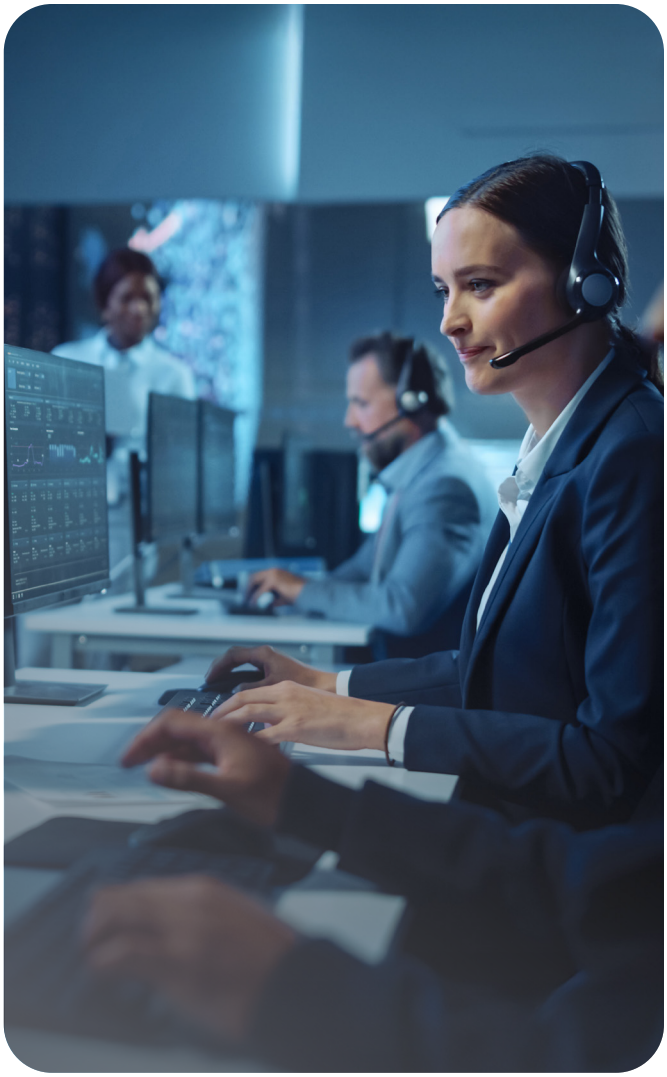
When implemented alongside other security measures, this service is crucial for organizations to prioritize potential threats and minimize their attack surface.

Objectives:

- **Minimize risk exposure:** Reduce the overall risk to the organization by identifying and addressing vulnerabilities before they can be exploited.
- **Ensure compliance:** Meet regulatory and industry standards by maintaining up-to-date security measures and documentation.
- **Improve incident response:** Enhance the ability to respond quickly and effectively to security incidents by having a clear understanding of potential vulnerabilities.
- **Maintain system availability:** Ensure that systems remain operational and minimize downtime by promptly addressing vulnerabilities.
- **Prevent breaches:** Decrease the likelihood of successful cyberattacks by continuously monitoring and remediating vulnerabilities.

Outcomes:

- **Threat landscape:** Reduce attack surface and mitigate risk.
- **Improved security posture:** A higher level of protection against sophisticated attacks.
- **Visibility:** Enhanced visibility and reporting of vulnerabilities that exist in the environment.
- **Response:** Rapidly responding to threats.
- **Compliance:** Maintaining compliance requirements.



Cybersecurity Policy Framework Review

In the cybersecurity policy framework review service, we review and enhance our clients' cybersecurity policies to ensure they are robust, up-to-date and aligned with industry best practices. This includes assessing existing cybersecurity policies, identifying gaps and areas for improvement, and developing new policies and procedures. We ensure alignment with regulatory requirements and standards such as NIST and ISO and provide training and awareness programs for employees.

Clients can expect enhanced organizational security, stronger compliance with regulatory and industry standards, and clear, effective cybersecurity policies tailored to their needs. By increasing employee awareness and engagement, this service ensures a proactive security culture across the organization.

Cybersecurity Awareness Training

Calian's learning management system, BeCyberSecure, is an online platform with modules that cover all present and emerging information security threats. Each lesson topic contains interactive content slides with videos and quizzes built in.

Objectives:

- **Increase awareness:** Educate employees about the various types of cyber threats, such as phishing, malware and social engineering, and how to recognize them.
- **Promote best practices:** Teach employees best practices for maintaining cybersecurity, including strong password management, safe browsing habits and secure handling of sensitive information.
- **Reduce human error:** Minimize the risk of security breaches caused by human error by ensuring employees understand the importance of following security protocols.
- **Enhance incident response:** Improve employees' ability to respond effectively to potential security incidents, such as recognizing and reporting suspicious activities.
- **Foster a security culture:** Create a culture of security within the organization where employees are vigilant and proactive about cybersecurity.

Outcomes:

- **Enhanced security posture:** Employees become more adept at identifying and mitigating cyber threats, reducing the overall risk of security breaches.
- **Reduced incidents:** With better awareness, the number of security incidents caused by human error, such as falling for phishing scams, decreases.
- **Improved compliance:** Training helps ensure that employees follow regulatory and compliance requirements, protecting the organization from legal and financial penalties.
- **Increased employee confidence:** Employees feel more confident in their ability to handle sensitive information and respond to potential security threats.

Benefits of Calian Cybersecurity Program

- **Improved preparedness:** Ensure all team members understand their roles during an incident.
- **Enhanced communication:** Test and improve communication protocols.
- **Identifies gaps:** Reveal weaknesses in incident response plans.
- **Builds confidence:** Practice responses in a safe environment.
- **Realistic training:** Deliver practical and relevant training scenarios.
- **Collaborative thinking:** Encourage teamwork and improve skills.
- **Security awareness:** Enhance awareness for executives and staff.

Contact Us Today

to activate your organization's Cybersecurity Program!

calian.com/**itcs**
For more information, contact: itcs@calian.com

calian.com | info@calian.com | 1.877.225.4264 |

Contract Service: Cybersecurity Program

Duration: Annual Contract (monthly or annual payment options)
Service Level: Sr Cybersecurity Consultants