VIEW POINT

UK CYBER ASSESSMENT FRAMEWORK 4.0: A STRATEGIC APPROACH TO ENHANCED CYBER RESILIENCE

Abstract

The evolution of cyber threats targeting critical infrastructure demands a sophisticated and adaptive approach to security governance. The UK Cyber Assessment Framework (CAF) version 4.0 represents a significant advancement in risk-based cybersecurity regulation, introducing enhanced requirements that reflect the contemporary threat landscape facing Operators of Essential Services (OES). This POV examines the strategic implications of CAF 4.0 and demonstrates how Infosys, in partnership with leading security platforms, delivers comprehensive solutions that enable organizations to achieve and maintain compliance while strengthening operational resilience.

Infosys®
Navigate your next

Introduction: The CAF 4.0 Imperative

The UK Cyber Assessment Framework 4.0 introduces transformative changes that extend beyond traditional compliance requirements. Organizations must now demonstrate sophisticated capabilities in threat intelligence consumption, secure software development lifecycle management, behavioral monitoring, and threat hunting. These enhancements reflect the maturation of both cyber threats and defensive capabilities, requiring operators of essential services to adopt more proactive and intelligence-driven security postures.

Infosys brings deep expertise in operational technology security, regulatory compliance, and digital transformation to help organizations navigate this complex landscape. Our comprehensive approach combines strategic consulting, implementation services, and managed security operations to deliver measurable outcomes aligned with CAF 4.0 requirements.

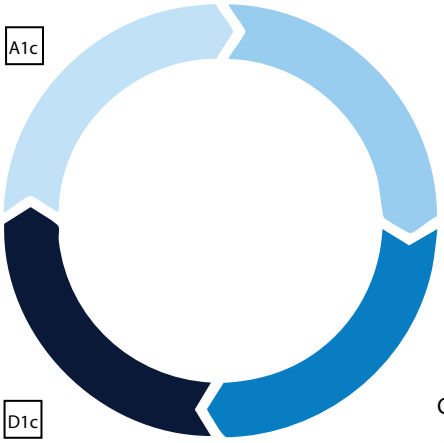
4.0
Framework Version
Latest CAF release with enhanced requirements

20+
Years Experience
Combined expertise in critical infrastructure security

100%
Risk-Based Adaptive approach
to compliance and resilience

A. Managing security risk

- A1. Governance — A1a, A1b, A1c
- A2. Risk Management — A2a, A2b
- A3. Asset Management — A3a
- A4. Supply Chain — A4a



B. Protecting against cyber attack

- B1. Service Protection Policies and Processes — B1a, B1b
- B2. Identity and Access Control — B2a, B2b, B2c, B2d
- B3. Data Security — B3a, B3b, B3c, B3d, B3e
- B4. System Security — B4a, B4b, B4c, B4d
- B5. Resilient Networks and Systems — B5a, B5b, B5c
- B6. Staff Awareness and Training B6z — B6a, B6b

C. Detecting cyber security events

- C1. Security Monitoring — B1a, B1b, B1c, B1d, B1e
- C2. Proactive Security Event Discovery — B2a, B2b

D. Minimising the impact of cyber security incidents

- D1. Response and Recovery Planning — D1a, D1b, D1c
- D2. Lessons Learned — D2a, D2b

Understanding the CAF 4.0 Framework: A Risk-Based Foundation

The UK Cyber Assessment Framework distinguishes itself from other regulatory frameworks through its fundamentally risk-based approach. Unlike prescriptive compliance regimes that mandate specific technical controls, CAF 4.0 recognizes that organizations operate in diverse contexts with varying risk profiles, operational requirements, and threat exposures. This flexibility enables operators of essential services to develop security programs that address both corporate risk management objectives and broader societal protection imperatives.

The framework's evolution reflects a sophisticated understanding of how critical infrastructure organizations must balance operational efficiency, reliability, and security. Competent authorities across different sectors bring industry-specific expertise to their assessments, recognizing that electricity transmission networks face different challenges than oil and gas production facilities or manufacturing operations. This sector-specific approach ensures that compliance requirements remain practical and achievable while driving meaningful security improvements.

Risk-Based Assessment

Organizations are evaluated on their journey toward maturity, not against binary pass/fail criteria. This approach recognizes that security is a continuous improvement process.

Sector-Specific Application

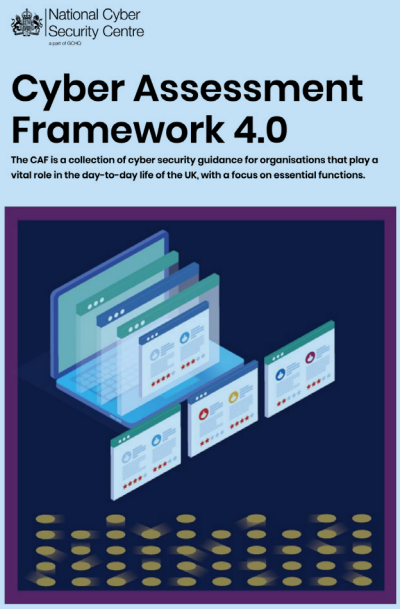
Competent authorities tailor assessments to reflect the unique operational characteristics, threat profiles, and business drivers of different industries.

Outcome-Focused Requirements

The framework specifies what organizations should achieve rather than prescribing exactly how to achieve it, enabling innovation and efficiency.

Infosys leverages this risk-based foundation to help clients develop pragmatic, cost-effective security programs that deliver compliance as a natural consequence of sound risk management. Our consultants work closely with organizations to understand their specific operational context, threat environment, and business objectives, ensuring that security investments deliver maximum value while satisfying regulatory expectations.

The Evolution of Cyber Threats: Why CAF 4.0 Matters Now



The threat landscape facing critical infrastructure has transformed dramatically since the original NIS Directive implementation in 2018. Early concerns centered primarily on sophisticated state-sponsored actors demonstrated by attacks such as TRITON and CrashOverride. While these threats remain significant, the emergence of ransomware as a pervasive threat to operational technology environments has fundamentally altered the risk calculus for operators of essential services.

Criminal groups now possess the capability and motivation to target industrial control systems, seeking financial gain through operational disruption. Simultaneously, hacktivist groups have emerged as proxies for state actors, conducting disruptive attacks that blur traditional threat categorizations. These evolving threats employ increasingly sophisticated techniques, including living-off-the-land tactics that evade traditional signature-based detection methods.

CAF 4.0 addresses this dynamic threat environment by emphasizing continuous threat intelligence consumption, behavioral monitoring, and proactive threat hunting. Organizations can no longer rely solely on perimeter defenses and signature-based detection. They must develop sophisticated capabilities to understand adversary tactics, techniques, and procedures (TTPs), detect anomalous behaviors indicative of compromise, and hunt proactively for threats that may have evaded automated defenses.

Infosys partners with leading threat intelligence providers to deliver comprehensive threat monitoring and hunting services tailored to operational technology environments. Our security operations centers combine advanced analytics, industry-specific threat intelligence, and deep OT expertise to identify and respond to threats before they impact critical operations. This proactive approach aligns perfectly with CAF 4.0's enhanced expectations for threat understanding and behavioral monitoring.

Objective A: Managing Security Risk - Enhanced Governance Requirements

01 **Threat Intelligence Integration**
Organizations must demonstrate continuous consumption of relevant threat intelligence, understanding adversaries targeting their sector and geography

02 **Secure Development Lifecycle**
Enhanced requirements for understanding software composition, including software bills of materials (SBOMs) for both new and legacy systems

03 **Risk Assessment Evolution**
Risk management processes must incorporate emerging threat intelligence and evolving attack techniques into ongoing assessments

04 **Governance Framework**
Robust business frameworks must be established before implementing technical controls, ensuring security aligns with business objectives

Objective A establishes the governance foundation upon which all other security capabilities are built. CAF 4.0 significantly strengthens requirements in this area, recognizing that effective security begins with sound business processes, clear accountability, and comprehensive risk understanding. Organizations must move beyond generic risk assessments to develop sophisticated threat models that incorporate specific intelligence about adversaries targeting their industry, geography, and technology stack.

The enhanced focus on secure software development represents a particularly significant shift. Organizations must now understand not only what software they deploy but also the components, libraries, and frameworks that comprise that software. This requirement addresses the growing threat of supply chain attacks, where adversaries compromise widely-used software components to gain access to multiple targets simultaneously. The SolarWinds attack demonstrated the devastating potential of such compromises, affecting government agencies and critical infrastructure operators worldwide.

Infosys delivers comprehensive governance consulting services that help organizations establish robust frameworks for managing security risk. Our approach begins with a thorough assessment of existing governance structures, identifying gaps relative to CAF 4.0 requirements. We then work collaboratively with clients to design and implement enhanced governance processes, including threat intelligence programs, secure development lifecycle frameworks, and risk assessment methodologies tailored to operational technology environments. Our consultants bring extensive experience across multiple sectors, enabling us to share best practices while respecting the unique characteristics of each client's operational context.

Threat Intelligence: From Reactive to Proactive Security

CAF 4.0's emphasis on threat intelligence consumption represents a fundamental shift from reactive to proactive security postures. Organizations must actively track threat groups targeting their sector, understand the tactics and techniques these adversaries employ, and continuously adapt their defenses based on emerging intelligence. This is not a one-time exercise but an ongoing operational capability that requires dedicated resources, specialized expertise, and integration with broader security operations.

Effective threat intelligence programs must go beyond consuming generic threat feeds. Organizations need intelligence that is specific, actionable, and relevant to their operational environment. This means understanding which threat groups target their industry, what vulnerabilities these groups exploit, what operational impacts they seek to achieve, and what indicators might reveal their presence in the environment.

Collection

Gather intelligence from multiple sources including industry-specific threat feeds, government advisories, and security research

Collection

Gather intelligence from multiple sources including industry-specific threat feeds, government advisories, and security research

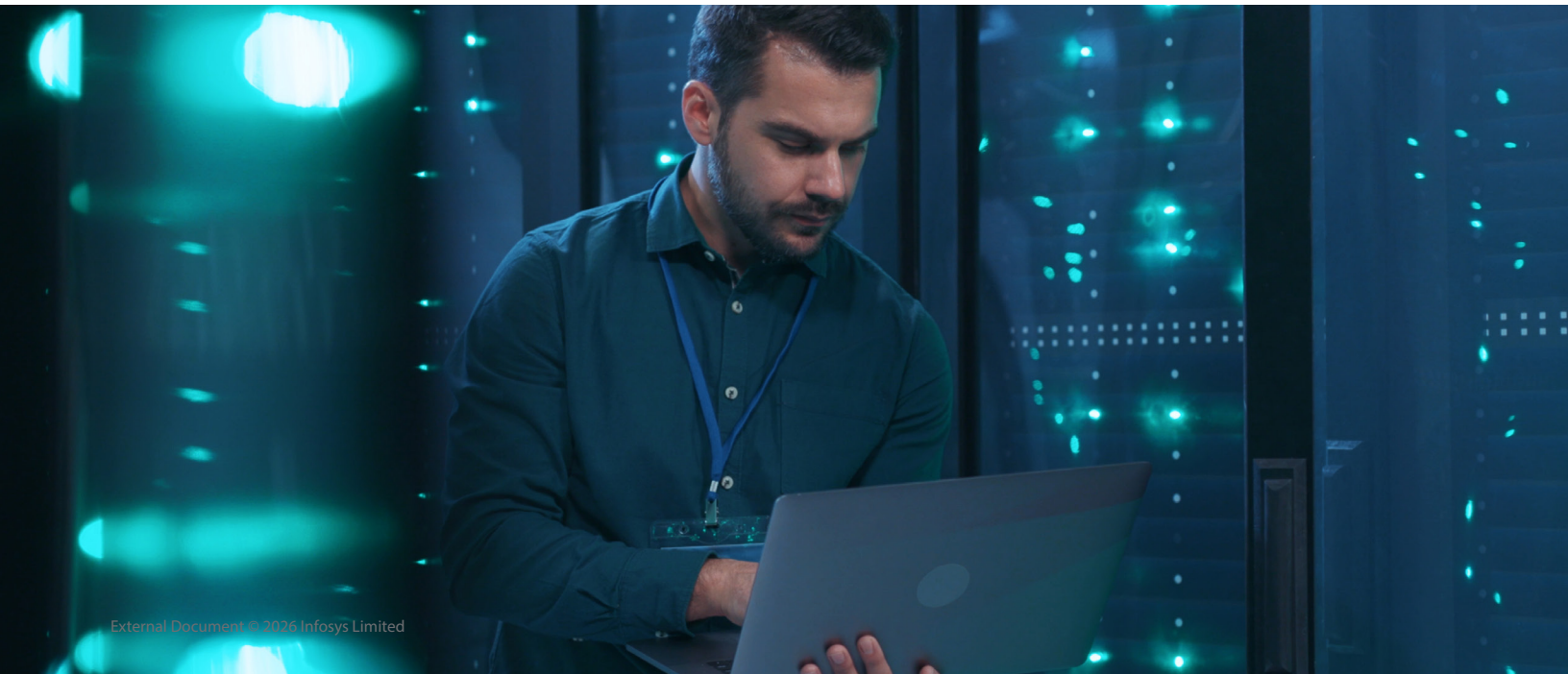
Dissemination

Distribute actionable intelligence to security teams, operations personnel, and leadership in formats appropriate to each audience

Action

Implement defensive measures, update detection rules, and modify security controls based on intelligence insights

Infosys provides comprehensive threat intelligence services that transform raw threat data into actionable security insights. Our threat intelligence team monitors adversary groups targeting critical infrastructure globally, with particular focus on the sectors and geographies where our clients operate. We deliver regular intelligence briefings tailored to different audiences within client organizations, from technical security teams requiring detailed indicators of compromise to executive leadership needing strategic threat assessments. Our intelligence feeds integrate seamlessly with security monitoring platforms, enabling automated detection of known threat actor TTPs while our analysts provide the human expertise necessary to identify novel threats and emerging attack patterns.



Secure Software Development: Addressing Supply Chain Risk

The introduction of secure software development requirements in CAF 4.0 reflects growing recognition of supply chain vulnerabilities as a critical attack vector. Modern industrial control systems comprise complex assemblies of software components, libraries, and frameworks sourced from multiple vendors. A vulnerability in a single widely-used component can expose thousands of systems to compromise, as demonstrated by vulnerabilities in common industrial protocol stacks and control libraries.

Organizations must now demonstrate understanding of their software composition at a granular level. This includes maintaining software bills of materials (SBOMs) that document all components within deployed systems, understanding the provenance of these components, and having processes to rapidly identify affected systems when vulnerabilities are disclosed. For new systems, organizations should require vendors to demonstrate secure development practices and provide comprehensive SBOMs as part of procurement processes. For legacy systems, organizations must work to retrospectively document software composition, a challenging but essential task.

1. **Vendor Assessment**
   Evaluate vendors' secure development practices during procurement, requiring evidence of secure coding standards, vulnerability management, and SBOM capabilities
2. **SBOM Generation**
   Obtain or generate comprehensive software bills of materials for all critical systems, documenting components, versions, and dependencies
3. **Vulnerability Tracking**
   Implement processes to monitor vulnerability disclosures affecting documented components and rapidly assess exposure across the environment
4. **Remediation Planning**
   Develop risk-based approaches to addressing identified vulnerabilities, balancing security concerns with operational stability requirements

Infosys brings extensive experience in secure software development and supply chain risk management to help clients address these enhanced requirements. Our services span the full lifecycle from vendor assessment and procurement support through SBOM generation and ongoing vulnerability management. We leverage advanced software composition analysis tools to document existing system components, even in legacy environments where original documentation may be incomplete. Our consultants work with clients to establish sustainable processes for maintaining SBOMs, monitoring for vulnerabilities, and making risk-based decisions about remediation priorities. For organizations developing custom software or integrating multiple vendor products, we provide secure development lifecycle consulting that embeds security throughout the development process rather than treating it as an afterthought.

Objective B: Protecting Against Cyber Attack - Evolving Defense Strategies

While Objective B contains no direct changes in CAF 4.0, the enhanced requirements in other objectives have significant implications for protective controls. Organizations must now verify that their protective measures align with current threat intelligence, that supply chain security controls address software composition risks, and that defensive architectures support the behavioral monitoring and threat hunting capabilities required by Objective C.

This interconnection between objectives reflects the holistic nature of effective cybersecurity. Protective controls cannot operate in isolation; they must be informed by threat intelligence, designed to generate telemetry for monitoring systems, and regularly tested through exercises that simulate realistic attack scenarios. Organizations should review their existing protective controls through the lens of CAF 4.0's enhanced requirements, identifying gaps and opportunities for improvement.

Access Control
Verify whether identity management systems can track vendor access and support supply chain security requirements

Network Security
Ensure network segmentation and monitoring capabilities support behavioral analysis and threat hunting

System Hardening
Implement secure configurations guided by threat intelligence and vulnerability assessments

Key considerations for Objective B in the context of CAF 4.0 include verifying supply chain security controls, ensuring protective measures generate appropriate telemetry for monitoring systems, designing secure architectures for new systems incorporating AI and automation, and regularly testing protective controls against realistic threat scenarios informed by current intelligence.

Infosys provides comprehensive security architecture and engineering services that help organizations design and implement protective controls aligned with CAF 4.0 requirements. Our approach begins with thorough assessment of existing controls, identifying gaps and opportunities for enhancement. We then work with clients to design defense-in-depth architectures that layer multiple protective measures, ensuring that compromise of any single control does not result in complete system failure. Our engineers have deep expertise in operational technology environments, understanding the unique requirements and constraints of industrial control systems. We design solutions that enhance security without compromising operational reliability, a critical balance in environments where availability is paramount.

Objective C: Detecting Cyber Security Events - The Shift to Behavioral Monitoring

Objective C introduces some of the most significant changes in CAF 4.0, with the addition of Section F focusing specifically on behavioral monitoring and threat hunting. This enhancement reflects recognition that traditional signature-based detection methods are insufficient against sophisticated adversaries employing living-off-the-land techniques and zero-day exploits. Organizations must develop capabilities to detect anomalous behaviors indicative of compromise, even when specific indicators of compromise are not yet known.

Behavioral monitoring requires understanding normal operational patterns within industrial control systems and identifying deviations that may indicate malicious activity. This is particularly challenging in OT environments where "normal" can vary significantly based on operational mode, production schedules, maintenance activities, and other factors. Effective behavioral monitoring must account for this operational context, distinguishing between legitimate operational changes and potentially malicious activities.

Network Behavior Analysis
Monitor network traffic patterns to identify anomalous communications, protocol violations, and suspicious data flows that may indicate reconnaissance or lateral movement

Host Behavior Analysis
Track process execution, file system changes, and system configurations to detect malicious activities on endpoints and servers

Protocol Analysis
Deep inspection of industrial protocols to identify malformed commands, unauthorized operations, or attempts to manipulate control systems

The emphasis on threat hunting represents another significant advancement. Threat hunting is a proactive process where security analysts actively search for threats that may have evaded automated detection systems. This requires not only appropriate data collection and retention but also skilled analysts who understand both cybersecurity and operational technology. Effective threat hunting develops hypotheses about how adversaries might compromise systems, then searches for evidence of those techniques within the environment.

Infosys delivers comprehensive security monitoring and threat hunting services specifically designed for operational technology environments. Our security operations centers combine advanced behavioral analytics platforms with expert analysts who understand industrial control systems. We deploy monitoring solutions that collect telemetry from both network and host-based sources, providing comprehensive visibility into OT environments. Our analysts develop detection rules based on current threat intelligence, identifying adversary TTPs relevant to our clients' industries and technologies. Beyond automated detection, our threat hunting teams proactively search for indicators of compromise, developing custom hypotheses based on emerging threats and conducting regular hunts across client environments. This combination of automated detection and human expertise provides defense-in-depth against both known and novel threats.

Data Collection and Retention: Foundation for Detection and Hunting

Effective behavioral monitoring and threat hunting depend fundamentally on comprehensive data collection and retention. Organizations must collect telemetry from multiple sources including network traffic, system logs, application logs, and security tool outputs. This data must be retained for sufficient periods to enable retrospective analysis, as sophisticated adversaries may dwell in environments for extended periods before their presence is detected.

CAF 4.0 emphasizes the importance of configuring systems to generate appropriate logs and ensuring these logs are collected, protected, and retained. This seemingly straightforward requirement can be challenging in OT environments where logging capabilities vary significantly across different device types and vendors. Some industrial control systems generate extensive operational data but limited security-relevant logs. Others may have logging capabilities that are disabled by default or that generate data in proprietary formats requiring specialized tools for analysis.

Network Telemetry

Capture network traffic through strategic placement of monitoring sensors, providing visibility into communications between systems and detecting anomalous network behaviors

Host-Based Logs

Collect system logs, application logs, and security logs from endpoints, servers, and industrial control systems to track activities and detect suspicious behaviors

Operational Data

Leverage operational technology data sources including historian systems, alarm logs, and process data to detect manipulation of control systems

Organizations must balance data collection comprehensiveness with storage costs and analysis capabilities. Collecting everything generates overwhelming data volumes that can be expensive to store and difficult to analyze effectively. A risk-based approach focuses collection efforts on the most critical systems and the data sources most likely to reveal adversary activity. This requires understanding both the operational importance of different systems and the techniques adversaries use to compromise them.

Infosys helps organizations design and implement comprehensive data collection strategies tailored to their operational environments and risk profiles. Our approach begins with thorough assessment of existing logging capabilities across the environment, identifying gaps and opportunities for enhancement. We work with clients to configure systems for optimal log generation, balancing security visibility with performance and storage considerations. Our data architecture specialists design scalable collection and retention infrastructures that can handle the data volumes generated by large industrial environments while maintaining the performance necessary for real-time analysis and historical investigation. We implement data lifecycle management policies that retain critical security data for appropriate periods while managing storage costs effectively.

Objective D: Minimizing the Impact of Cyber Security Incidents

While Objective D contains no direct changes in CAF 4.0, the enhanced requirements elsewhere in the framework have important implications for incident response capabilities. Organizations must ensure their response plans address the threat scenarios identified through threat intelligence consumption, that they can effectively investigate incidents using the behavioral monitoring and threat hunting capabilities developed under Objective C, and that they regularly test their response capabilities through exercises that simulate realistic attack scenarios.

The changing threat landscape, particularly the emergence of ransomware as a significant threat to OT environments, requires organizations to reconsider their incident response strategies. Traditional approaches focused primarily on containment and eradication may be insufficient when facing adversaries who can rapidly encrypt critical systems or manipulate industrial processes. Organizations need response plans that address both IT and OT impacts, that consider the unique operational requirements and constraints of industrial environments, and that have been tested against realistic scenarios.

01

Preparation

Develop comprehensive response plans, establish response teams, and ensure necessary tools and resources are available

02

Detection & Analysis

Identify incidents through monitoring systems, assess scope and impact, and determine appropriate response actions

03

Containment & Recovery

Isolate affected systems, eradicate adversary presence, and restore normal operations safely

04

Post-Incident Activity

Conduct lessons learned reviews, update response plans, and implement improvements to prevent recurrence

Backup and recovery capabilities deserve particular attention in the context of ransomware threats. Organizations must ensure they maintain offline or immutable backups of critical systems that cannot be encrypted by ransomware. These backups must be tested regularly to verify they can be restored successfully within required timeframes. Recovery plans should address not only technical restoration procedures but also the business decisions and operational considerations involved in recovering from significant incidents.

Infosys provides comprehensive incident response services that help organizations prepare for, respond to, and recover from cyber security incidents. Our incident response retainer services go beyond traditional "break glass" arrangements, providing ongoing engagement that helps clients continuously improve their preparedness. We conduct regular tabletop exercises that test response plans against realistic scenarios informed by current threat intelligence. These exercises involve not only technical security teams but also operational personnel, business leadership, legal counsel, and other stakeholders who would be involved in actual incident response. Through these exercises, we identify gaps in response plans, clarify roles and responsibilities, and build the muscle memory necessary for effective response under pressure.

Tabletop Exercises: Testing Response Capabilities

Tabletop exercises represent one of the most effective methods for testing and improving incident response capabilities. These facilitated discussions walk participants through realistic incident scenarios, requiring them to make decisions, coordinate responses, and address the complex challenges that arise during actual incidents. Unlike technical simulations that focus primarily on security team actions, tabletop exercises engage the full range of stakeholders involved in incident response, from technical personnel to executive leadership.

Effective tabletop exercises are carefully designed to reflect realistic threats and operational contexts. Scenarios should be based on current threat intelligence, incorporating the tactics and techniques that adversaries actually use against organizations in the client's sector. The exercise should unfold dynamically, with facilitators introducing new information and complications as participants make decisions, mirroring the uncertainty and time pressure of real incidents. Participants should include not only internal personnel but also external parties such as vendors, regulators, and other stakeholders who would be involved in actual response.

Scenario Development

Create realistic incident scenarios based on threat intelligence, incorporating technical details and business impacts relevant to the organization

Stakeholder Engagement

Involve all relevant parties including technical teams, operations, leadership, legal, communications, and external partners

Exercise Execution

Facilitate dynamic scenario progression, requiring participants to make decisions and coordinate responses under time pressure

Lessons Learned

Conduct thorough debriefs, document findings, and develop action plans to address identified gaps and improve response capabilities

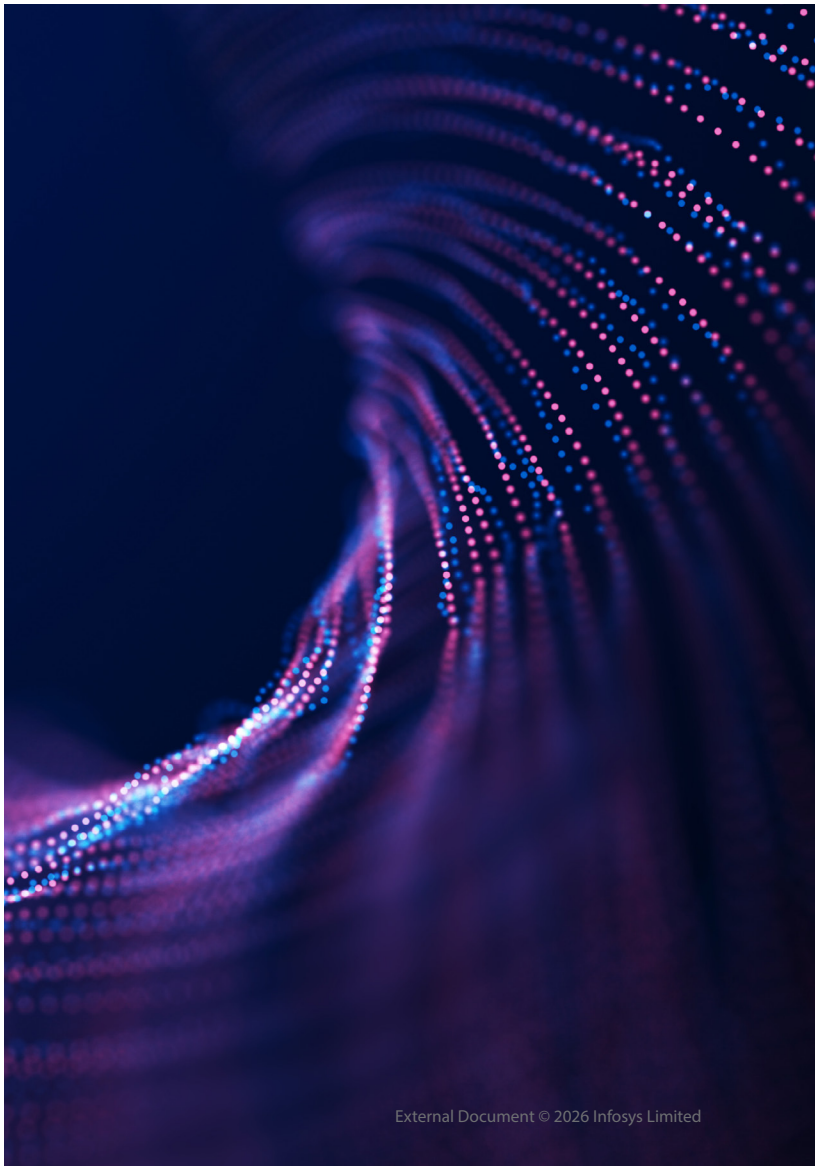
The value of tabletop exercises extends beyond identifying gaps in response plans. These exercises build relationships and understanding among different teams that must coordinate during incidents. Technical security personnel gain appreciation for operational constraints and business considerations. Business leaders develop realistic understanding of incident response timelines and capabilities. External partners clarify their roles and responsibilities. This shared understanding and relationship building proves invaluable during actual incidents when rapid coordination is essential.

Infosys designs and facilitates comprehensive tabletop exercises tailored to each client's operational environment, threat profile, and organizational structure. Our exercise scenarios reflect current threat intelligence and realistic operational impacts. We engage the full range of stakeholders, ensuring exercises test not only technical response capabilities but also business decision-making, communications, legal considerations, and coordination with external parties. Our facilitators bring extensive incident response experience, enabling them to create realistic, challenging scenarios that push participants while maintaining a constructive learning environment. Following each exercise, we provide detailed reports documenting findings and recommendations, then work with clients to implement improvements that enhance their response capabilities.

Emerging Technologies: AI, Automation, and New Risk Considerations

CAF 4.0 introduces explicit consideration of emerging technologies, particularly artificial intelligence and automation, recognizing both the opportunities and risks these technologies present. Organizations increasingly deploy AI and automation to improve operational efficiency, optimize processes, and reduce costs. These technologies offer significant benefits but also introduce new security considerations that must be addressed through risk assessment, secure design, and appropriate controls.

AI and automation systems can become targets for adversaries seeking to manipulate industrial processes. An adversary who compromises an AI-based optimization system might be able to manipulate process parameters in ways that cause physical damage or operational disruption. Automated control systems that operate with minimal human oversight may be vulnerable to manipulation that goes undetected until significant impacts occur. Organizations must consider these risks when deploying new technologies, implementing appropriate monitoring and safeguards.



Risk Assessment for New Technologies

Evaluate security implications of AI and automation deployments, considering both cyber risks and potential operational impacts of compromise or malfunction

Secure Design Principles

Implement defense-in-depth architectures for AI and automation systems, including input validation, output verification, and human oversight mechanisms

Monitoring and Validation

Deploy monitoring capabilities that can detect anomalous behaviors in AI and automation systems, validating outputs against expected operational parameters

Resilience and Fallback

Ensure critical operations can continue safely if AI or automation systems fail or are compromised, maintaining manual control capabilities where appropriate

The integration of AI and automation also creates new dependencies that must be considered in resilience planning. Organizations that optimize operations through AI-based systems may find it difficult to operate efficiently without those systems. If an incident compromises or disables AI infrastructure, can operations continue safely? What manual processes or fallback systems are available? These questions must be addressed through comprehensive resilience planning that considers dependencies on emerging technologies.

Infosys helps organizations navigate the security challenges of emerging technologies through comprehensive risk assessment, secure design consulting, and implementation support. Our consultants evaluate the security implications of proposed AI and automation deployments, identifying potential vulnerabilities and recommending appropriate safeguards. We help clients design secure architectures that incorporate defense-in-depth principles, ensuring that compromise of any single component does not result in catastrophic failure. Our monitoring and analytics capabilities extend to AI and automation systems, detecting anomalous behaviors that might indicate compromise or malfunction. We work with clients to develop resilience strategies that maintain safe operations even if emerging technologies fail or are compromised.

Supply Chain Security: Managing Third-Party Risk

Supply chain security emerges as a critical theme throughout CAF 4.0, reflecting growing recognition that organizations' security posture depends not only on their own controls but also on the security practices of their vendors, suppliers, and other third parties. The enhanced requirements around secure software development, vendor access management, and third-party risk assessment require organizations to take a more comprehensive and rigorous approach to supply chain security.

Supply chain risks manifest in multiple ways. Software vulnerabilities in vendor products can expose organizations to compromise. Insecure vendor remote access can provide adversaries with entry points into operational networks. Compromised vendor systems can be used as staging points for attacks against customers. Organizations must address these diverse risks through comprehensive supply chain security programs that span procurement, vendor management, and ongoing monitoring.

Vendor Assessment

Evaluate vendors' security practices during procurement, requiring evidence of appropriate controls and secure development practices

Contractual Requirements

Establish clear security requirements in vendor contracts, including SBOM provision, vulnerability disclosure, and incident notification

Access Management

Implement rigorous controls for vendor remote access, including multi-factor authentication, session monitoring, and time-limited access

Ongoing Monitoring

Continuously monitor vendor security posture and performance, conducting periodic reassessments and addressing identified issues

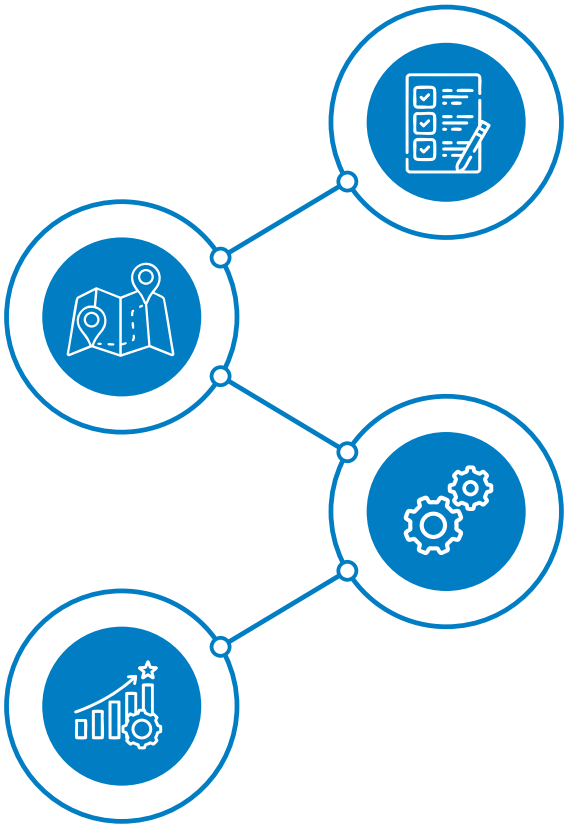
Vendor remote access deserves particular attention as a high-risk area frequently exploited by adversaries. Many organizations maintain always-on VPN connections for vendors, often with shared credentials and minimal monitoring. These connections provide adversaries who compromise vendor systems with direct access to operational networks. Organizations should implement more rigorous controls including individual user accounts, multi-factor authentication, just-in-time access provisioning, and comprehensive session monitoring and logging.

Infosys provides comprehensive supply chain security services that help organizations assess and manage third-party risks. Our vendor assessment services evaluate suppliers' security practices, providing clients with objective assessments to inform procurement decisions. We help clients develop and implement vendor security requirements, including contractual language that establishes clear expectations and obligations. Our access management solutions provide secure, monitored remote access for vendors, replacing risky always-on VPN connections with just-in-time access that is granted only when needed and comprehensively logged. We conduct ongoing vendor risk monitoring, alerting clients to security incidents or changes in vendor risk profiles that may require attention.

Implementation Roadmap: Achieving CAF 4.0 Compliance

Achieving compliance with CAF 4.0 requires a structured, phased approach that prioritizes activities based on risk and builds capabilities progressively. Organizations should resist the temptation to attempt everything simultaneously, instead focusing on establishing strong foundations before advancing to more sophisticated capabilities. The SANS 5 Critical Controls provide an excellent starting framework, addressing the most impactful security measures that mitigate the majority of common threats.

A successful implementation roadmap begins with comprehensive assessment of current capabilities relative to CAF 4.0 requirements. This assessment should identify gaps, prioritize remediation activities based on risk, and develop realistic timelines that account for resource constraints and operational considerations. The roadmap should be developed collaboratively with competent authorities, ensuring alignment with their expectations and assessment criteria.



Assessment

Evaluate current capabilities against CAF 4.0 requirements, identifying gaps and prioritizing remediation activities

Roadmap Development

Create phased implementation plan with realistic timelines, resource requirements, and success criteria

Implementation

Execute planned activities, building capabilities progressively while maintaining operational stability

Continuous Improvement

Monitor effectiveness, adapt to emerging threats, and continuously enhance security posture

Implementation should proceed in phases, with each phase building on the foundations established in previous phases. Early phases typically focus on governance, risk assessment, and basic protective controls. Middle phases implement monitoring and detection capabilities, leveraging the governance frameworks and protective controls established earlier. Later phases advance to more sophisticated capabilities such as threat hunting and continuous improvement processes. This phased approach ensures that organizations build sustainable capabilities rather than implementing point solutions that may not integrate effectively.

Throughout implementation, organizations should maintain focus on outcomes rather than simply checking compliance boxes. The goal is not merely to satisfy regulatory requirements but to genuinely improve security posture and operational resilience. This outcome focus ensures that investments deliver real value, protecting critical operations and enabling the organization to respond effectively to evolving threats.

Infosys provides comprehensive implementation support that guides organizations through their CAF 4.0 compliance journey. Our approach begins with thorough assessment using our proprietary maturity models that map current capabilities to CAF 4.0 requirements. We work collaboratively with clients to develop realistic, risk-based implementation roadmaps that account for their specific operational contexts, resource constraints, and business priorities. Our implementation teams bring deep expertise across all aspects of OT security, from governance and risk management through technical implementation of monitoring and response capabilities. We provide not only technical implementation support but also change management and training services that ensure new capabilities are effectively adopted and sustained. Throughout the engagement, we maintain close communication with competent authorities, ensuring that our approach aligns with their expectations and assessment criteria.

Infosys OT Security Services: Comprehensive Support for CAF 4.0

Infosys delivers comprehensive operational technology security services that address all aspects of CAF 4.0 compliance. Our service portfolio spans strategic consulting, technical implementation, managed security operations, and incident response, providing clients with end-to-end support throughout their security journey. We combine deep OT expertise with global delivery capabilities, enabling us to support organizations of any size and complexity across multiple geographies and sectors.

Our approach is built on several key principles that differentiate our services and ensure client success. We maintain sector-specific expertise, with dedicated teams focused on electricity, oil and gas, manufacturing, and other critical infrastructure sectors. This specialization ensures our consultants understand the unique operational requirements, regulatory contexts, and threat profiles of each industry. We emphasize practical, risk-based approaches that deliver measurable security improvements rather than pursuing compliance for its own sake. We build sustainable capabilities within client organizations through knowledge transfer and training, ensuring they can maintain and evolve their security programs over time.

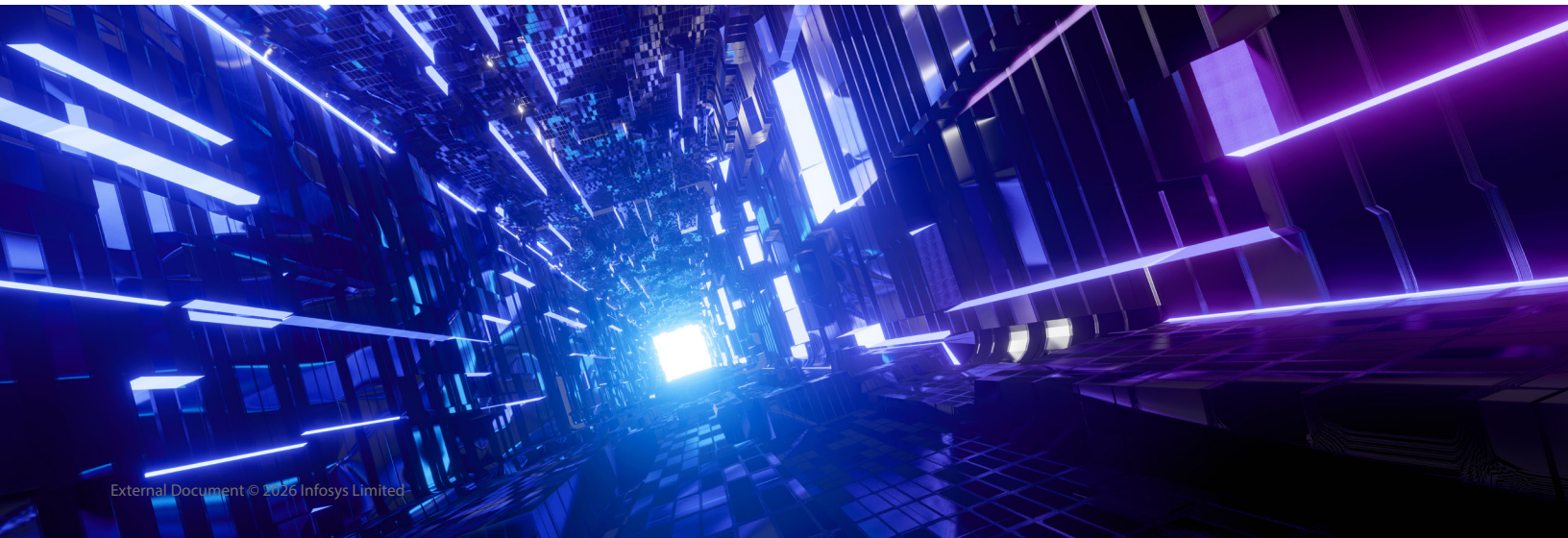
Strategic Consulting
Governance framework development, risk assessment, compliance roadmapping, and security program strategy aligned with business objectives and regulatory requirements

Technical Implementation
Security architecture design, technology selection and deployment, integration services, and technical configuration aligned with best practices

Managed Security Operations
24/7 security monitoring, threat intelligence, threat hunting, vulnerability management, and incident response through our global security operations centers

Training and Enablement
Security awareness training, technical skills development, tabletop exercises, and knowledge transfer to build internal capabilities

Our service delivery model provides flexibility to meet diverse client needs. Some organizations engage us for comprehensive managed services, outsourcing security operations to our expert teams. Others prefer co-managed models where we augment internal capabilities with specialized expertise and 24/7 coverage. Still others engage us for specific projects or consulting engagements, leveraging our expertise to address particular challenges or build specific capabilities. Regardless of engagement model, we maintain consistent quality and leverage our global resources to deliver exceptional outcomes.



Technology Partnerships: Best-of-Breed Solutions

Infosys maintains strategic partnerships with leading technology providers in the OT security space, enabling us to deliver best-of-breed solutions tailored to each client's requirements. These partnerships provide our consultants with deep technical expertise on leading platforms, early access to new capabilities, and direct channels to vendor support and engineering teams. For clients, these partnerships ensure they receive solutions that are properly designed, implemented, and supported throughout their lifecycle.

Our technology partnerships span the full spectrum of OT security capabilities. We partner with leading providers of network monitoring and threat detection platforms, endpoint security solutions, security information and event management (SIEM) systems, vulnerability management tools, and incident response technologies. These partnerships enable us to design comprehensive security architectures that integrate multiple best-of-breed solutions, providing defense-in-depth while avoiding vendor lock-in.

Platform Expertise
Certified consultants with deep technical knowledge of leading OT security platforms and proven implementation experience

Vendor Relationships
Direct access to vendor support, engineering, and product management teams for rapid issue resolution and solution optimization

Integration Capabilities
Proven methodologies for integrating multiple security solutions into cohesive architectures that maximize effectiveness

Lifecycle Support
Ongoing support throughout solution lifecycle including upgrades, optimization, and evolution as requirements change

Our vendor-agnostic approach ensures we recommend solutions based on client requirements rather than vendor relationships. We conduct thorough requirements analysis and technology evaluation, considering factors including technical capabilities, operational fit, total cost of ownership, and vendor viability. This objective approach ensures clients receive solutions that truly meet their needs and deliver long-term value.

For CAF 4.0 compliance, our partnerships with leading threat intelligence and monitoring platform providers are particularly valuable. These partnerships enable us to deliver the sophisticated threat intelligence, behavioral monitoring, and threat hunting capabilities that CAF 4.0 requires. We leverage these platforms' advanced analytics and detection capabilities while adding our own OT expertise and managed services to deliver comprehensive solutions that address all aspects of Objective C requirements.

Measuring Success: Metrics and Continuous Improvement

Effective security programs require measurement and continuous improvement. Organizations must establish metrics that provide meaningful insight into security posture, track progress toward compliance objectives, and identify areas requiring attention. These metrics should span multiple dimensions including governance maturity, control effectiveness, threat detection and response performance, and overall risk reduction.

CAF 4.0's risk-based approach emphasizes outcomes over outputs, requiring organizations to demonstrate not just that they have implemented controls but that those controls are effective at managing risk. This outcome focus requires sophisticated measurement approaches that go beyond simple compliance checklists. Organizations should track leading indicators that predict future security performance as well as lagging indicators that measure historical outcomes.

24/7
Monitoring Coverage
Continuous security monitoring across all critical systems and networks

<15min
Detection Time
Mean time to detect security incidents through behavioral monitoring

99.9%
Availability
Operational availability maintained while implementing security controls

100%
Coverage
Critical assets with comprehensive security monitoring and protection

Key performance indicators for CAF 4.0 compliance should address multiple dimensions. Governance metrics might include percentage of staff completing security awareness training, frequency of risk assessments, and timeliness of policy reviews. Technical metrics could track vulnerability remediation rates, patch compliance levels, and security control coverage. Operational metrics should measure threat detection rates, incident response times, and exercise completion. Together, these metrics provide comprehensive visibility into security program performance.

Continuous improvement processes use these metrics to identify opportunities for enhancement. Regular reviews should analyze trends, compare performance against targets, and identify areas requiring attention. Organizations should conduct periodic maturity assessments to track progress over time and benchmark against industry peers. Lessons learned from incidents, exercises, and assessments should be systematically captured and used to drive program improvements.

Infosys helps clients establish comprehensive measurement and continuous improvement programs. We work with clients to define meaningful metrics aligned with their risk profiles and compliance objectives. Our reporting platforms provide executive dashboards that communicate security posture clearly to leadership while also providing detailed operational metrics for security teams. We conduct regular maturity assessments using our proprietary frameworks, tracking progress over time and identifying improvement opportunities. Our continuous improvement services help clients systematically enhance their security programs, ensuring they remain effective against evolving threats and aligned with changing business requirements.

Conclusion: Partnership for Cyber Resilience

CAF 4.0 represents a significant evolution in cybersecurity regulation for UK critical infrastructure, introducing enhanced requirements that reflect the contemporary threat landscape and available defensive capabilities. Organizations must develop sophisticated capabilities spanning threat intelligence, secure development, behavioral monitoring, and proactive threat hunting. These requirements demand not only technical implementation but also organizational transformation, building security into governance processes, operational procedures, and business decision-making.

Infosys stands ready to partner with organizations on their CAF 4.0 compliance journey. Our comprehensive service portfolio, deep OT expertise, and proven delivery capabilities enable us to support clients through all phases of their security program development. From initial assessment and roadmap development through technical implementation and ongoing managed services, we provide the expertise and resources necessary for success.

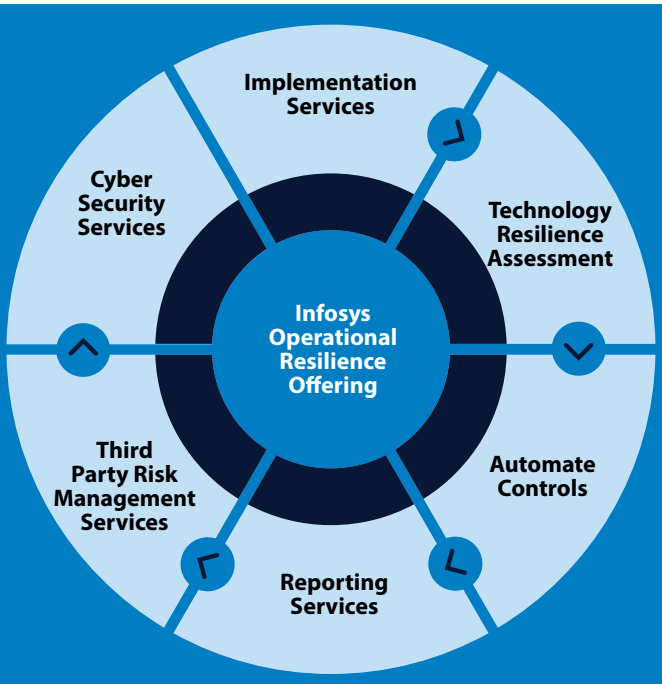


Fig. Infosys Operational Resilience Offering

Our approach emphasizes practical, risk-based solutions that deliver genuine security improvements rather than pursuing compliance for its own sake. We build sustainable capabilities within client organizations, ensuring they can maintain and evolve their security programs over time. We maintain close relationships with competent authorities, ensuring our approaches align with regulatory expectations and assessment criteria. Most importantly, we bring a genuine commitment to protecting critical infrastructure, understanding that the systems we help secure provide essential services upon which society depends.

Collaborative Partnership
We work alongside your teams, building capabilities and transferring knowledge throughout our engagement

Outcome Focus
We prioritize genuine security improvements and risk reduction over checkbox compliance

Global Resources
We leverage worldwide expertise and delivery capabilities to support clients across all geographies

Continuous Innovation
We continuously evolve our services to address emerging threats and leverage new technologies

The journey to CAF 4.0 compliance need not be undertaken alone. Infosys brings the expertise, resources, and commitment necessary to help organizations navigate this complex landscape successfully. We invite you to engage with our team to discuss your specific requirements and explore how we can support your security program development. Together, we can build the cyber resilience necessary to protect critical infrastructure and ensure the continued delivery of essential services upon which the society depends.

Learn more about Infosys CyberSecurity services

References

UK Cyber Assessment Framework 4.0 - Reference Links
UK Cyber Assessment Framework (CAF) 4.0 Official Documentation
https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

NIS Directive (EU Directive on Security of Network and Information Systems)
https://digital-strategy.ec.europa.eu/en/policies/nis-directive

MITRE ATT&CK Framework
https://attack.mitre.org/

TRITON Malware Analysis · FireEye
https://www.mandiant.com/resources/triton-malware-targets-safety-systems

CrashOverride Report · Dragos
https://www.dragos.com/blog/crashoverride/

SolarWinds Attack Summary · CISA
https://www.cisa.gov/news-events/news/cisa-updates-guidance-solarwinds-and-related-threats

Software Bill of Materials (SBOM) Guidance
https://www.ntia.gov/SBOM

OWASP Secure Software Development Lifecycle (SSDLC)
https://owasp.org/www-project-secure-software-development-life-cycle/

SANS Threat Hunting
https://www.sans.org/cyber-security-courses/advanced-threat-hunting/

Elastic Security Platform
https://www.elastic.co/security

NCSC Incident Management Guidance
https://www.ncsc.gov.uk/guidance/incident-management

CISA Tabletop Exercise Package
https://www.cisa.gov/resources-tools/resources/tabletop-exercise-package

NCSC AI Security
https://www.ncsc.gov.uk/blog-post/securing-ai-systems

ENISA AI Threat Landscape
https://www.enisa.europa.eu/publications/artificial-intelligence-threat-landscape

NCSC Supply Chain Security
https://www.ncsc.gov.uk/collection/supply-chain-security

CISA Secure Software Development Framework (SSDF)
https://www.cisa.gov/resources-tools/resources/secure-software-development-framework-ssdf

About the Author

Michel Bruggeman
EMEA IoT & OT Lead | Principal Cybersecurity Consultant

Michel Bruggeman is a distinguished cybersecurity leader with over 25 years of experience specializing in operational technology (OT) security, cyber resilience, and industrial cybersecurity architecture. He has held strategic roles across the manufacturing, insurance, energy, and semiconductor sectors, focusing on OT/ICS risk assessments, secure cloud adoption, and incident response readiness.

Michel is a SANS/ISA Mentor and Microsoft Certified Trainer, with deep expertise in ISO 27001, IEC 62443, NIST, DORA, and NIS2.

For more information, contact askus@infosys.com

Infosys®
Navigate your next