DXC.technology

DXC Labs | Security — White Paper

DXC Cyber Reference Architecture

An enterprise-focused path to cyber resilience and secure digital transformation

At the heart of digital transformation is data. The importance of protecting this critical business asset is bringing cybersecurity into sharp focus in the boardroom as well as the data center.

In the past, an enterprise's cybersecurity team focused on IT security risks and threats, with little reference to business risks, objectives and strategy. The team would deploy controls within a defined corporate network boundary, driving a very technology-focused approach to cybersecurity. The team generally spoke its own language of cybersecurity terms and acronyms, little understood by the business.

Aligning cybersecurity strategy with business objectives — and obtaining board-level sponsorship — is key to attaining and maintaining a strong security posture.

Digital transformation, however, means that cybersecurity can no longer be handled as an after-the-fact bolt-on, separate from the rest of the business. Organizations must consider security as part of their strategic approach, viewing cybersecurity and resilience as business enablers that help enterprises safely embrace the benefits of digital transformation.

Even the World Economic Forum recognizes the importance of high-level responsibility for the strategic governance of cyber risk and cyber resilience. In a report for boards of directors, "Advancing Cyber Resilience: Principles and Tools for Boards," the forum concluded that "cyber strategy must be determined at the oversight board level."

Aligning cybersecurity strategy with business objectives — and obtaining board-level sponsorship — is key to attaining and maintaining a strong security posture.

Closing the security posture gap

Most organizations are struggling to reduce the growing gap between their security posture and the threat landscape, with its ever-increasing cyberattack sophistication — and at the same time, they are trying to stay on top of changing security-related regulatory and legislative obligations that differ across geographies.

Spending more money isn't necessarily the answer. Security budgets are increasing, but the security posture gap is getting wider, as shown in **Figure 1**.

DXC Labs | Security

DXC Labs delivers thought leadership and technology prototypes to enable enterprises to thrive in the digital age.

DXC Labs | Security brings together our world-class advisors to develop strategic and architectural insights to reduce digital risk. DXC's Cyber Reference Architecture is at the heart of our research, providing clients with detailed guidance on methods to efficiently resolve the most challenging security problems. We help clients minimize risk while taking maximum advantage of the digital commons.

Learn more at **www.dxc.technology/securitylabs**

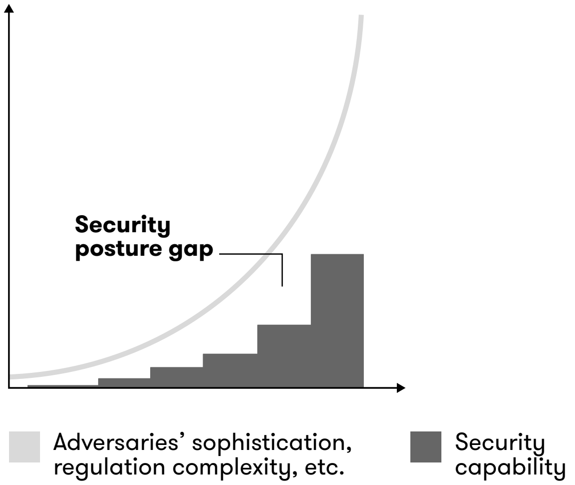


Figure 1. Security posture gap

Here are some reasons why:

- **Lack of integration**, with little or no understanding of the cybersecurity risk posture throughout the business, makes it difficult to reduce business risk.
- **Lack of prioritization** means security investments are often allocated to implement the latest security trend or technology, without first addressing security foundations.
- **Bottom-up technical siloes** cause a lack of alignment between the security solutions deployed and business objectives.
- **Lack of optimization** results in overlap of security controls and failure to take advantage of virtualization or new functionality in existing security tools.
- **Reinventing the wheel** increases time, cost and risk.

Closing the gap requires upper management to set a clear cybersecurity strategy and requires the cybersecurity team to focus on managing cyber risk appropriately, and proportionate to the business' goals and risk appetite.

If they want to be truly cyber resilient, enterprises must also be prepared for the worst to happen. It's no longer a question of whether they may be breached but when, and what the likely consequences are. The legislative and regulatory implications of data breaches continue to increase, and the reputational damage they can cause to a business can be extremely damaging. A Juniper Research report estimates the cost of cybercrime to businesses will total $8 trillion by 2022.

DXC Cyber Reference Architecture as security backbone

DXC Technology provides security services for major organizations around the globe, has implemented thousands of security solutions and provides managed security services for the world's largest companies. We've created a Cyber Reference Architecture (CRA) that draws on decades of experience monitoring billions of threats and responding to some of the world's largest cyberattacks. This architecture is now at the center of all DXC cybersecurity strategies and capabilities. In fact, DXC lead consultants and architects use CRA every day — and update it regularly.

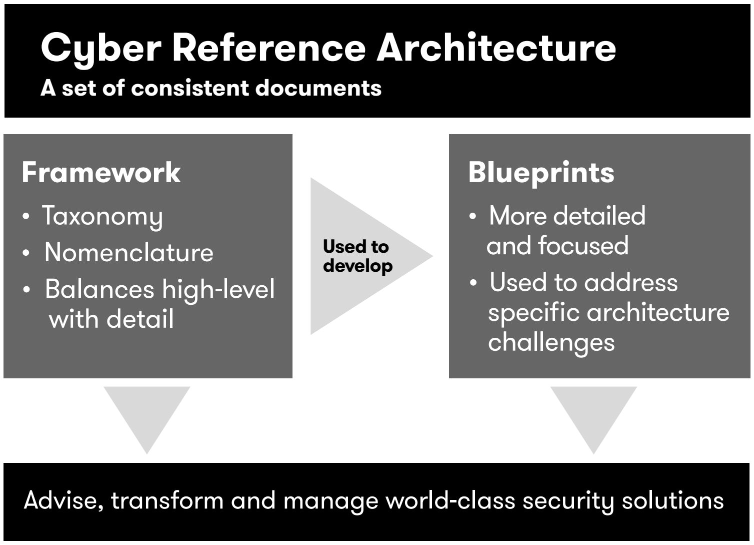
DXC CRA leverages our unparalleled expertise in consulting, architecture, transformation and operations to help people at all levels of an organization understand how to secure the enterprise while pursuing new digital initiatives. The architecture helps organizations develop business-aligned security strategies and accelerate their digital transformation.

DXC CRA helps organizations:

- Understand which objectives matter most to the business
- Define security requirements to achieve those objectives
- Map out the best approach for deploying targeted security capabilities to support the plan

DXC CRA serves as a security backbone, providing a common language, a consistent approach and a long-term vision. The architecture is composed of a framework and blueprints, as shown in **Figure 2**.

Figure 2. DXC Cyber Reference Architecture framework and blueprints

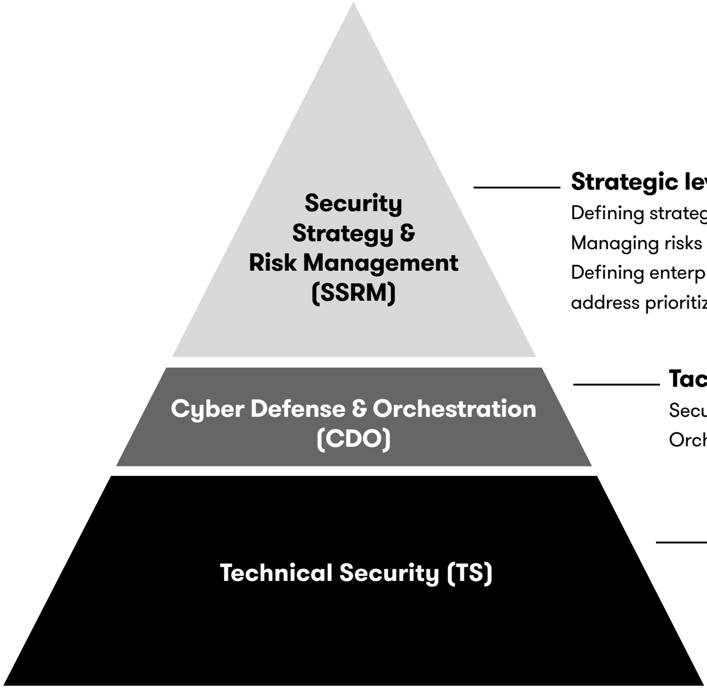

Cyber Reference Architecture
A set of consistent documents
Framework
• Taxonomy
• Nomenclature
• Balances high-level with detail
Used to develop
Blueprints
• More detailed and focused
• Used to address specific architecture challenges
Advise, transform and manage world-class security solutions

CRA framework

DXC's CRA framework describes security holistically and is aligned to security standards and methods such as The Open Group Architecture Framework (TOGAF), Sherwood Applied Business Security Architecture (SABSA), Control Objectives for Information and Related Technology (COBIT), National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO). CRA also has a defined taxonomy and nomenclature.

The framework consists of three levels: strategic, tactical and operational, and technical (see **Figure 3**). These levels are used to logically group the 12 domains that make up the CRA framework, as shown in **Figure 4**.

Figure 3. The three levels in the CRA framework

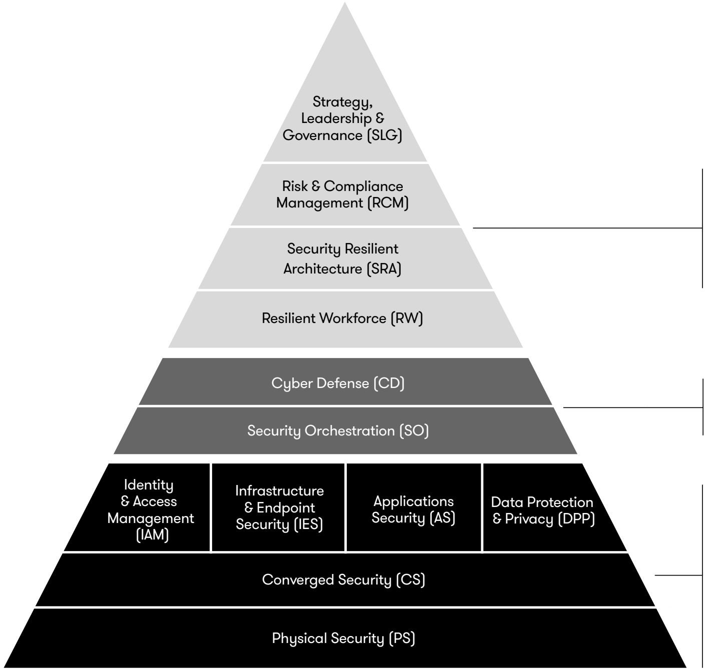

Security Strategy & Risk Management (SSRM)
Cyber Defense & Orchestration (CDO)
Technical Security (TS)

Strategic level
Defining strategy
Managing risks and compliance
Defining enterprise security architecture to address prioritized risks and enable the business

Tactical and operational level
Security monitoring and breach response
Orchestrate intelligent security operations

Technical level
Design, size, implement and run technical security solutions

Figure 4. The framework's 12 domains and their related functions


Strategy, Leadership & Governance (SLG)
Risk & Compliance Management (RCM)
Security Resilient Architecture (SRA)
Resilient Workforce (RW)
Cyber Defense (CD)
Security Orchestration (SO)
Identity & Access Management (IAM)
Infrastructure & Endpoint Security (IES)
Applications Security (AS)
Data Protection & Privacy (DPP)
Converged Security (CS)
Physical Security (PS)

SLG	Define a strategy aligned to business objectives
RCM	Manage risk and ensure compliance
SRA	Translate business strategies into security solutions
RW	Security-conscious culture and knowledge management
CD	Security monitoring, incident management and response
SO	Processes, including management and measurement
IAM	Management of identities and access controls
IES	Enterprise threat detection and prevention
AS	Secure development and maintenance of software
DPP	Data classification, modeling and protection
CS	IT and OT security integration
PS	Protect assets from physical threats

Each domain supports a set of objectives and is decomposed into subdomains and capabilities, as shown in **Figure 5**, while **Figure 6** outlines domain topology.

Figure 5. Objectives supported by the domains

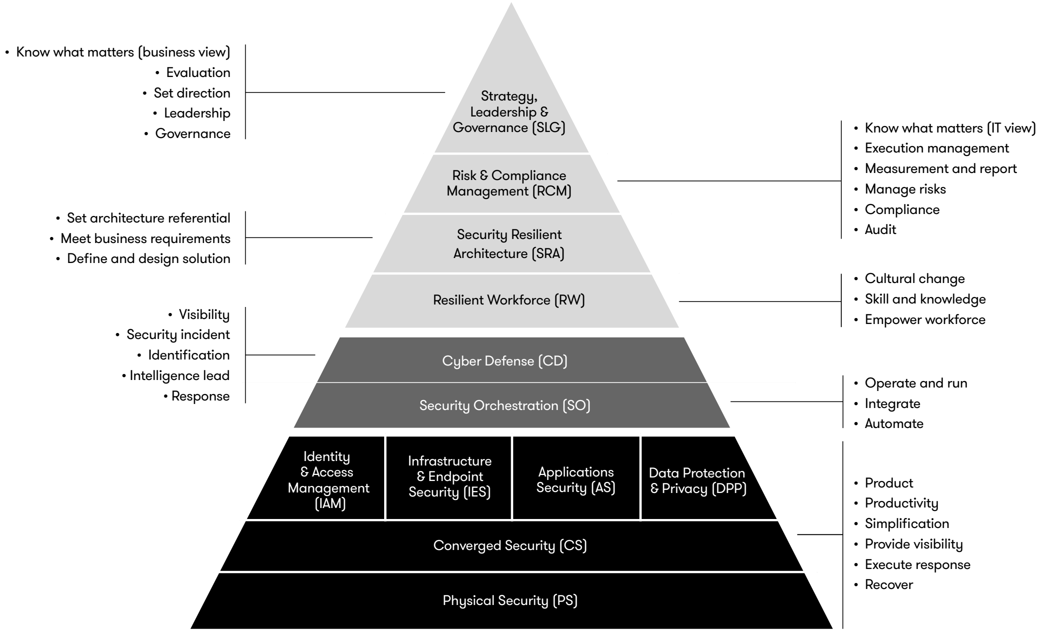
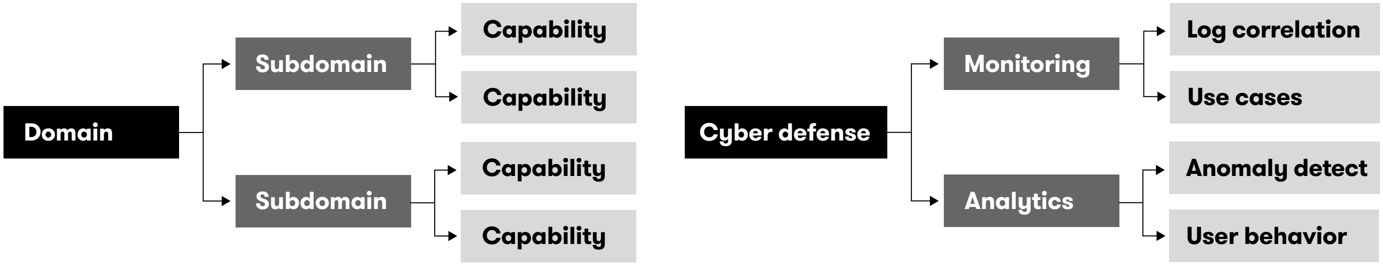


Figure 6. Domain topology, at left, and a partial example of a cyber defense domain



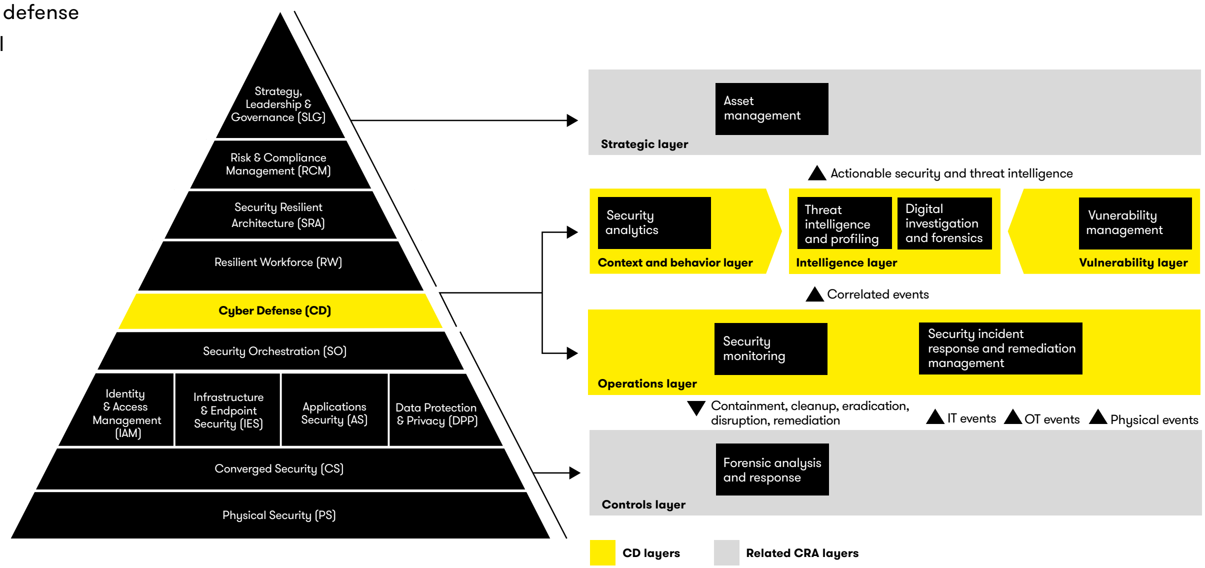
Capabilities support the execution of the security strategy. A capability represents a security requirement plus an ability or capacity that an organization may possess to achieve a specific security purpose or outcome.

By not specifying below the capability level, the CRA remains agnostic to compliance/controls frameworks — such as Payment Card Industry Data Security Standard (PCI DSS), ISO/ISE 27002, National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA) and Cloud Controls Matrix (CCM) — but is easily mapped against any of these frameworks.

CRA blueprints

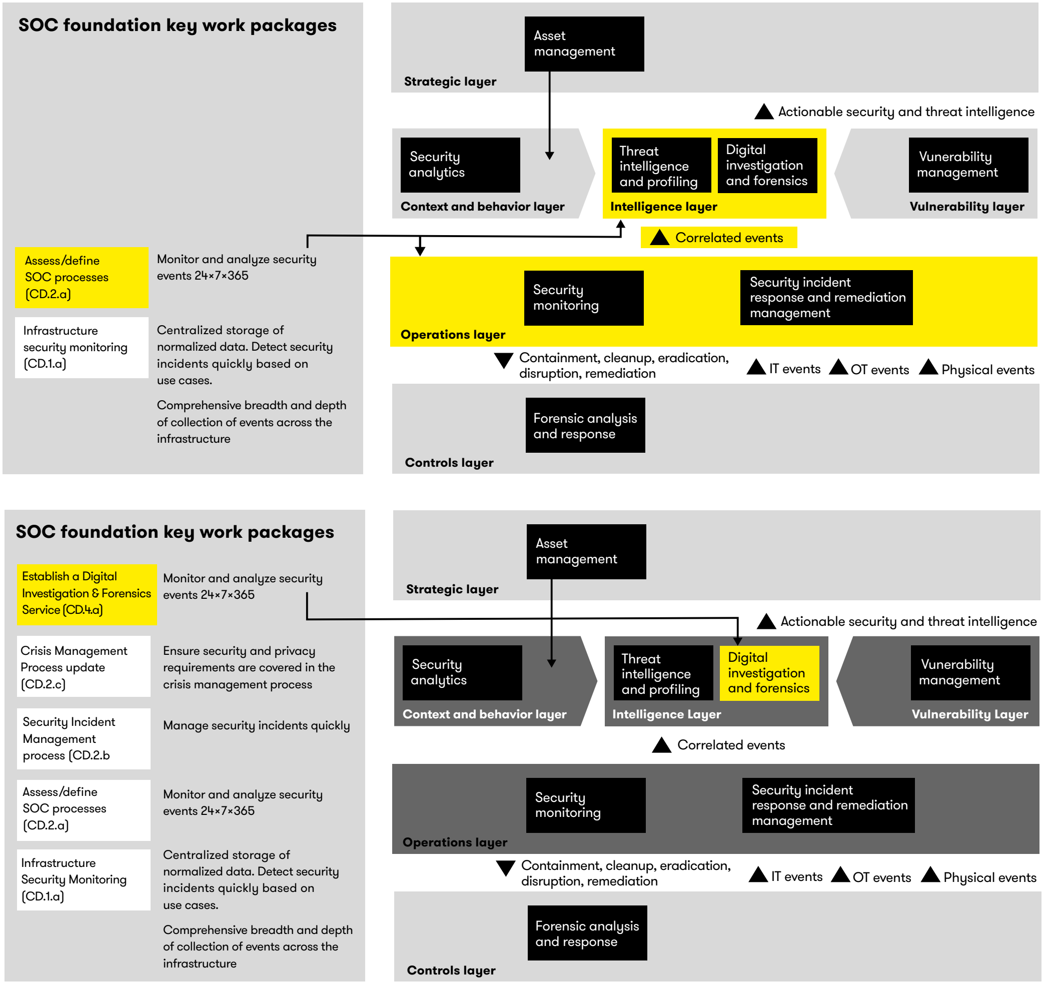
CRA blueprints are a set of reference architectures defined against the CRA framework. The blueprints start with a conceptual view, mapping layers and key functional areas to the applicable domains and subdomains in the CRA framework (see **Figure 7**).

Figure 7. CRA cyber defense blueprint conceptual view example


Strategy, Leadership & Governance (SLG)
Risk & Compliance Management (RCM)
Security Resilient Architecture (SRA)
Resilient Workforce (RW)
Cyber Defense (CD)
Security Orchestration (SO)
Identity & Access Management (IAM)
Infrastructure & Endpoint Security (IES)
Applications Security (AS)
Data Protection & Privacy (DPP)
Converged Security (CS)
Physical Security (PS)
Asset management
Strategic layer
Actionable security and threat intelligence
Security analytics
Context and behavior layer
Threat intelligence and profiling
Digital investigation and forensics
Intelligence layer
Vulnerability management
Vulnerability layer
Correlated events
Security monitoring
Security incident response and remediation management
Operations layer
Containment, cleanup, eradication, disruption, remediation
IT events
OT events
Physical events
Forensic analysis and response
Controls layer
CD layers
Related CRA layers

The conceptual view is then used in a storyboard to build the work packages required to implement the capabilities or the subdomains mapped to the layers. Each work package is a discrete statement of work but relies on the work packages identified before it in the storyboard, as shown in **Figure 7** and **Figure 8**.

Figure 8. CRA cyber defense blueprint storyboard example



SOC foundation key work packages

Assess/define SOC processes (CD.2.a)	Monitor and analyze security events 24×7×365
Infrastructure security monitoring (CD.1.a)	Centralized storage of normalized data. Detect security incidents quickly based on use cases. Comprehensive breadth and depth of collection of events across the infrastructure

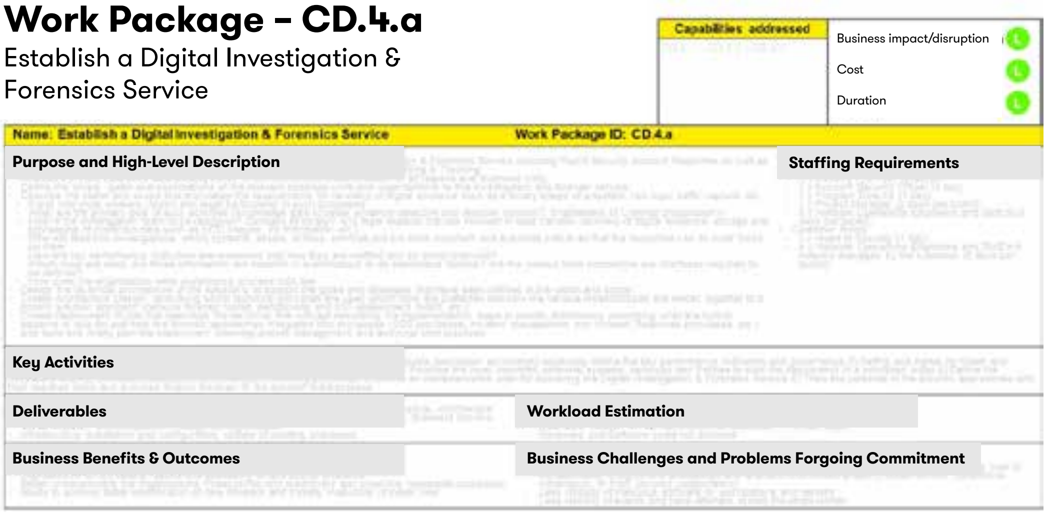
Strategic layer
Asset management
Actionable security and threat intelligence
Security analytics
Context and behavior layer
Threat intelligence and profiling
Digital investigation and forensics
Intelligence layer
Vunerability management
Vulnerability layer
Correlated events
Security monitoring
Security incident response and remediation management
Operations layer
Containment, cleanup, eradication, disruption, remediation
IT events
OT events
Physical events
Forensic analysis and response
Controls layer

SOC foundation key work packages

Establish a Digital Investigation & Forensics Service (CD.4.a)	Monitor and analyze security events 24×7×365
Crisis Management Process update (CD.2.c)	Ensure security and privacy requirements are covered in the crisis management process
Security Incident Management process (CD.2.b	Manage security incidents quickly
Assess/define SOC processes (CD.2.a)	Monitor and analyze security events 24×7×365
Infrastructure Security Monitoring (CD.1.a)	Centralized storage of normalized data. Detect security incidents quickly based on use cases. Comprehensive breadth and depth of collection of events across the infrastructure

Strategic layer
Asset management
Actionable security and threat intelligence
Security analytics
Context and behavior layer
Threat intelligence and profiling
Digital investigation and forensics
Intelligence Layer
Vunerability management
Vulnerability Layer
Correlated events
Security monitoring
Security incident response and remediation management
Operations layer
Containment, cleanup, eradication, disruption, remediation
IT events
OT events
Physical events
Forensic analysis and response
Controls layer

Figure 9. CRA cyber defense blueprint storyboard example



Work Package – CD.4.a

Establish a Digital Investigation & Forensics Service

Capabilities addressed	
	Business impact/disruption L
	Cost L
	Duration L

Name: Establish a Digital Investigation & Forensics Service   Work Package ID: CD.4.a

Purpose and High-Level Description

Staffing Requirements

Key Activities

Deliverables

Workload Estimation

Business Benefits & Outcomes

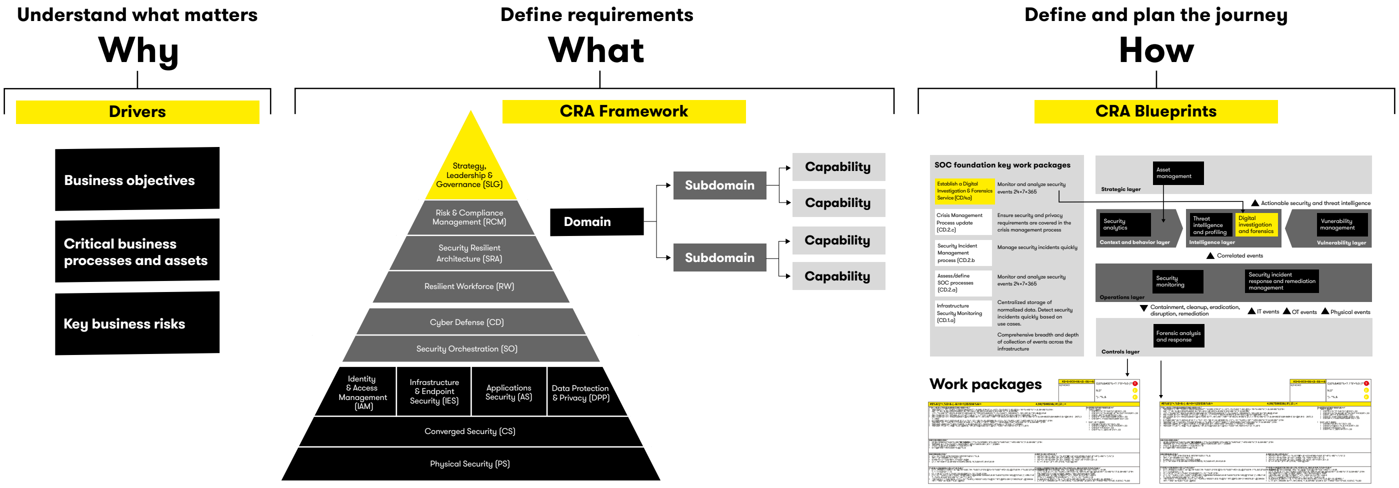
Business Challenges and Problems Forgoing Commitment

How DXC uses the CRA

There is no single way to use the CRA, and it's not mandatory to apply all the components. How an organization deploys them depends on its business objectives, risk appetite, current state of maturity and budget. As shown in **Figure 10**, the CRA structure simply provides a unified, comprehensive approach to enterprise security, helping an organization:

- Understand what matters and define security objectives
- Define the security requirements needed to achieve the objectives by identifying from the CRA framework what security capabilities have to be deployed
- Describe how to deploy the targeted capabilities

Figure 10. CRA cyber defense blueprint storyboard example


Understand what matters
Why
Drivers
Business objectives
Critical business processes and assets
Key business risks
Define requirements
What
CRA Framework
Strategy, Leadership & Governance (SLG)
Risk & Compliance Management (RCM)
Security Resilient Architecture (SRA)
Resilient Workforce (RW)
Cyber Defense (CD)
Security Orchestration (SO)
Identity & Access Management (IAM)
Infrastructure & Endpoint Security (IES)
Applications Security (AS)
Data Protection & Privacy (DPP)
Converged Security (CS)
Physical Security (PS)
Domain
Subdomain
Capability
Capability
Subdomain
Capability
Capability
Define and plan the journey
How
CRA Blueprints
SOC foundation key work packages
Establish a Digital Investigation & Forensics Service (CD.4.a)
Monitor and analyze security events 24×7×365
Crisis Management Process update (CD.2.c)
Ensure security and privacy requirements are covered in the crisis management process
Security Incident Management process (CD.2.b
Manage security incidents quickly
Assess/define SOC processes (CD.2.a)
Monitor and analyze security events 24×7×365
Infrastructure Security Monitoring (CD.1.a)
Centralized storage of normalized data. Detect security incidents quickly based on use cases.
Comprehensive breadth and depth of collection of events across the infrastructure
Asset management
Strategic layer
Actionable security and threat intelligence
Security analytics
Context and behavior layer
Threat intelligence and profiling
Digital investigation and forensics
Intelligence layer
Vunerability management
Vulnerability layer
Correlated events
Security monitoring
Security incident response and remediation management
Operations layer
Containment, cleanup, eradication, disruption, remediation
IT events
OT events
Physical events
Forensic analysis and response
Controls layer
Work packages

Objectives

- Support and enable business
- Protect critical business processes
- Manage key business risks

What needs to be done

- Identify from the CRA framework (catalog of capabilities) what security capabilities (security requirements) have to be deployed in the organization to achieve objectives

How to deploy targeted capabilities

- Understand the maturity of existing capabilities and use relevant blueprints; select and adapt work packages explaining how to deploy targeted capabilities

Improve cyber maturity

To attain and maintain cyber resilience and embrace digital transformation, an enterprise must understand its overall cyber maturity, recognize its areas of weakness, continuously improve its overall maturity and make sure that its cyber risk is being treated appropriately and proportionately.

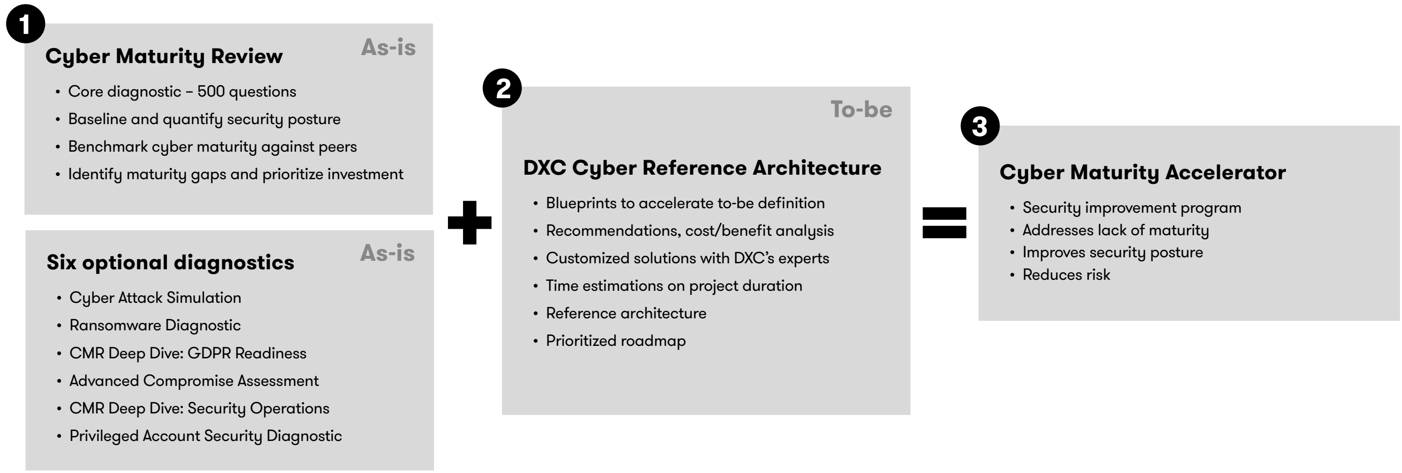
DXC CRA helps organizations in all industries improve and maintain their cyber maturity, so they can:

- Develop a business-aligned security strategy — the “to be” state describing the business need, vision, objectives and accountabilities
- Define an adaptive security transformation roadmap — a series of tactical and strategic initiatives and activities to be performed over a set time period to enable the execution of the security strategy
- Develop a resilient and agile security architecture providing a risk-based approach to support the business strategy
- Enable budgetary planning and justification

Accelerate security improvements

The CRA is at the core of DXC’s Cyber Maturity Accelerator methodology, which is designed to help companies rapidly get on the road to security improvement (see **Figure 11**)

Figure 11. DXC’s Cyber Maturity Accelerator methodology



1

Cyber Maturity Review As-is

- Core diagnostic – 500 questions
- Baseline and quantify security posture
- Benchmark cyber maturity against peers
- Identify maturity gaps and prioritize investment

Six optional diagnostics As-is

- Cyber Attack Simulation
- Ransomware Diagnostic
- CMR Deep Dive: GDPR Readiness
- Advanced Compromise Assessment
- CMR Deep Dive: Security Operations
- Privileged Account Security Diagnostic

+

2

To-be

DXC Cyber Reference Architecture

- Blueprints to accelerate to-be definition
- Recommendations, cost/benefit analysis
- Customized solutions with DXC’s experts
- Time estimations on project duration
- Reference architecture
- Prioritized roadmap

=

3

Cyber Maturity Accelerator

- Security improvement program
- Addresses lack of maturity
- Improves security posture
- Reduces risk

DXC’s Cyber Maturity Review diagnostics evaluate a client’s cybersecurity against the CRA, identifying areas of weakness. DXC consultants use the CRA, and specifically the blueprints, to rapidly develop a security improvement roadmap of costed and prioritized security improvement initiatives. From this roadmap, they develop and shape a security improvement program to align cyber maturity with the client’s business priorities and objectives.

Once the organization attains an acceptable level of cyber maturity, the CRA continues to provide the basis for an ongoing security improvement program throughout the digital transformation.

The fast track to cyber resilience and transformation

DXC CRA provides an unmatched foundation for understanding, transforming and managing best-in-class cybersecurity solutions. It gives companies the strategic framework to elevate cybersecurity to the boardroom, as well as supplying the tactical tools and methodology to create and execute a clear technology roadmap to cyber maturity.

When security goals are aligned with an organization's goals, the result is cyber resilience that supports and accelerates digital transformation and business success.

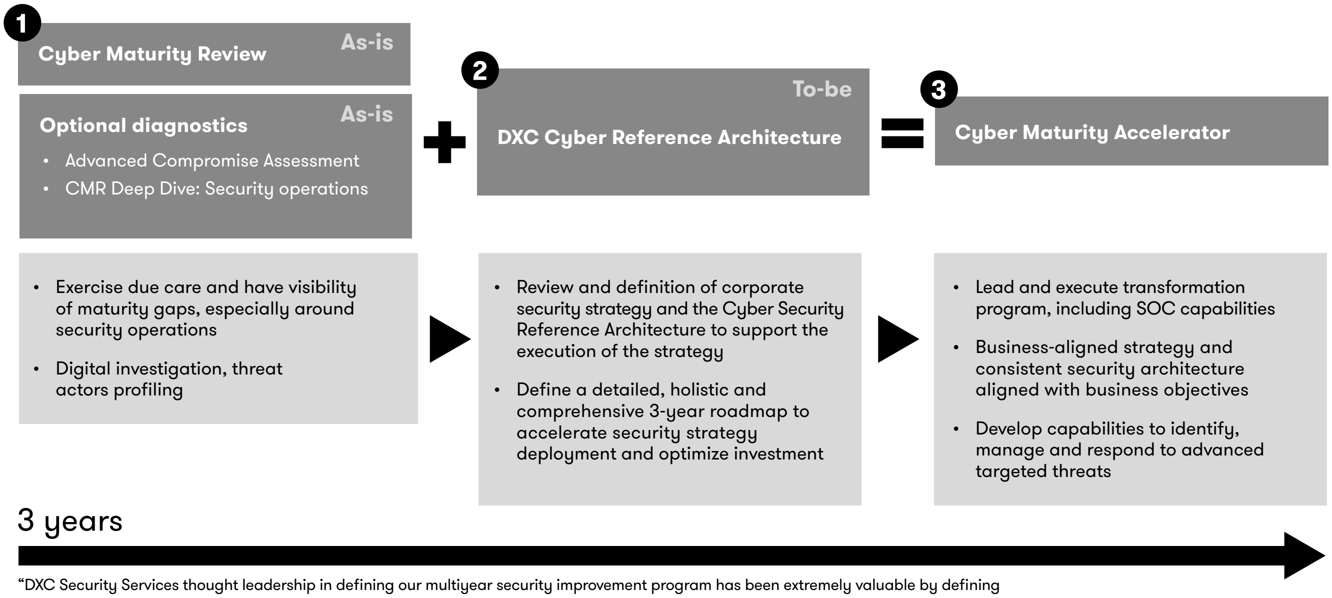
Here are two examples of the CRA in action:

Multinational manufacturer

A leading global manufacturer needed to review its corporate security strategy and associated security improvement program and establish a security operations center to align with business objectives and optimize its investments. DXC worked with the firms to define a CRA to support the execution of the strategy.

Multinational manufacturer

Approximately 50,000 employees in 130 countries
Security strategy, security roadmap, definition and execution



1 **Cyber Maturity Review** As-is

Optional diagnostics As-is

- Advanced Compromise Assessment
- CMR Deep Dive: Security operations

+

2 **DXC Cyber Reference Architecture** To-be

=

3 **Cyber Maturity Accelerator**

- Exercise due care and have visibility of maturity gaps, especially around security operations
- Digital investigation, threat actors profiling

▶

- Review and definition of corporate security strategy and the Cyber Security Reference Architecture to support the execution of the strategy
- Define a detailed, holistic and comprehensive 3-year roadmap to accelerate security strategy deployment and optimize investment

▶

- Lead and execute transformation program, including SOC capabilities
- Business-aligned strategy and consistent security architecture aligned with business objectives
- Develop capabilities to identify, manage and respond to advanced targeted threats

3 years

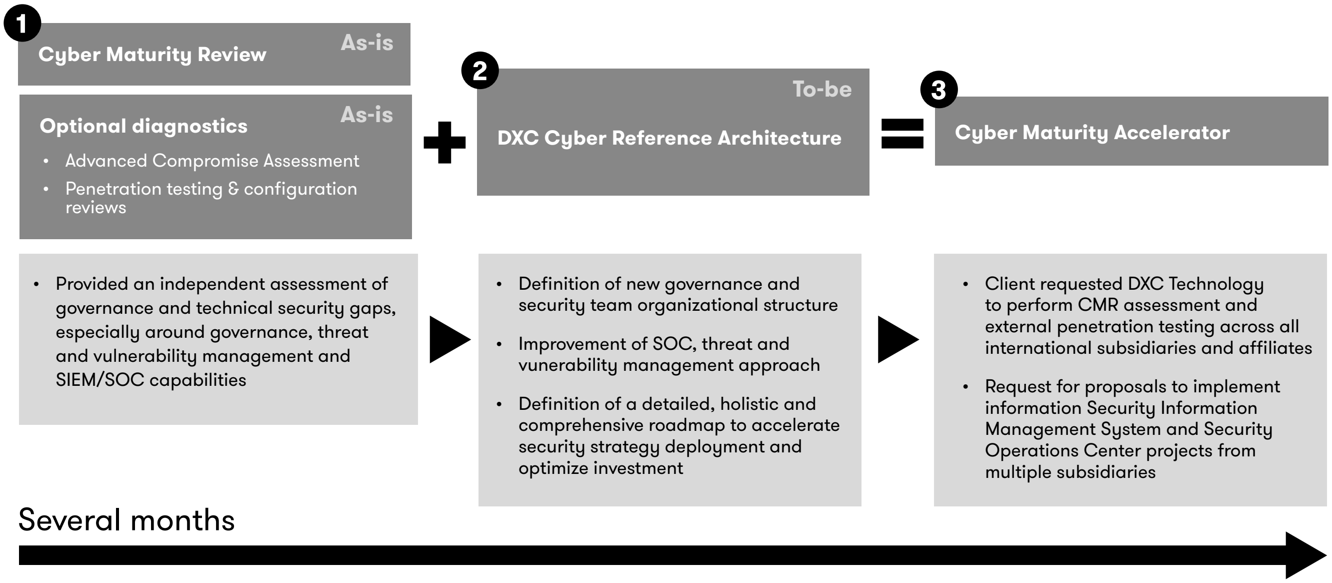
"DXC Security Services thought leadership in defining our multiyear security improvement program has been extremely valuable by defining an overall security architecture, setting the right priorities and the right sequence of deliverables in the program." — **Group CIO**

Global financial services group

A large global banking group with offices in 30 countries had been breached, with sensitive bank and customer data being made available publicly over the internet. DXC worked closely with the chief risk officer and the information security team to identify and close the technical and governance gaps within its headquarters. DXC also assessed the cyber maturity and conducted penetration tests of five other banks in Switzerland, Turkey, Indonesia, Egypt, Ghana and the United Arab Emirates.

Global financial services group

Approximately 28,000 employees in 31 countries
Security strategy, security roadmap, forensics and penetration testing



1 Cyber Maturity Review — As-is

Optional diagnostics — As-is

- Advanced Compromise Assessment
- Penetration testing & configuration reviews

+

2 DXC Cyber Reference Architecture — To-be

=

3 Cyber Maturity Accelerator

- Provided an independent assessment of governance and technical security gaps, especially around governance, threat and vulnerability management and SIEM/SOC capabilities

- Definition of new governance and security team organizational structure
- Improvement of SOC, threat and vunerability management approach
- Definition of a detailed, holistic and comprehensive roadmap to accelerate security strategy deployment and optimize investment

- Client requested DXC Technology to perform CMR assessment and external penetration testing across all international subsidiaries and affiliates
- Request for proposals to implement information Security Information Management System and Security Operations Center projects from multiple subsidiaries

Several months

The first step toward a more secure future

It’s time for people at all levels of the organization to get involved in securing the enterprise while pursuing new digital initiatives. The DXC Cyber Reference Architecture helps organizations develop business-aligned security strategies and accelerate their digital transformation. The first step begins with a cyber maturity assessment and a commitment to improve the organization’s security posture.

[1] “Advancing Cyber Resilience: Principles and Tools for Boards,” World Economic Forum, in collaboration with The Boston Consulting Group and Hewlett Packard Enterprise, January 2017, p. 4. http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

[2] The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017-2022,” Juniper Research, May 30, 2017, https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn

About the authors

Christophe Menant is the global strategy lead for security risk management at DXC Technology. He is the principal author of and global lead for the DXC Cyber Reference Architecture. With 26 years of experience in IT and security, he has helped clients develop security and transformation strategies, manage major breaches and remediation programs, and develop reference security architectures and offerings. Prior to DXC, he worked for IBM and previously specialized in security architecture and compliance, cloud security, and SAP and Oracle SaaS solutions.

Mark Evans is the chief security architect, Security Consulting, Integration and Compliance, for the UK, Ireland, India, Middle East and Africa (UKIIMEA) region at DXC Technology. He has a background in enterprise security architecture and cloud security. Previously, Mark was the chief security architect for HP/HPE's UK Government Cloud Program (formerly known as Helion-G and now known as DXC UK Restricted Secure Cloud Delivery), designing and delivering secure cloud services for the UK government.

Learn more at www.dxc.technology/cra

MD_9467a-19. March 2019