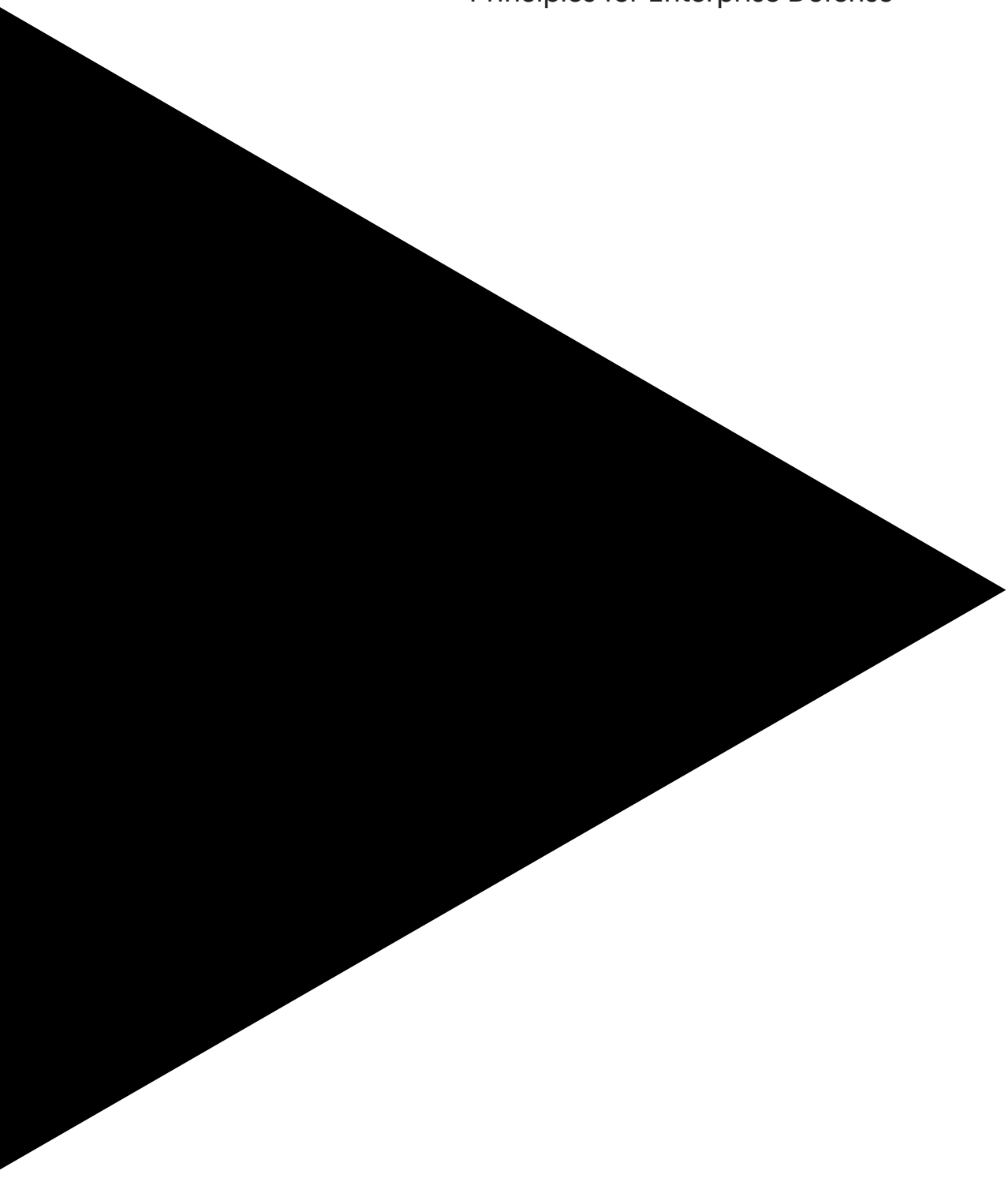
Secure Digital Transformation

Principles for Enterprise Defense



Security is complex, and complexity is the enemy of security. This complexity makes it hard for C-level executives to easily comprehend security requirements for the enterprise.

Enterprise leaders recognize security as an enable of digital services crucial to business growth. However, given the complexity of security architectures, they often struggle to understand what it is they need to do in order to enable their secure digital transformation.

This white paper provides a set of succinct and simplified high-level architectural principles designed for executive consumption. Applying these principles will allow executives to build digital resilience into the fabric of their enterprise, ensuring they can gain all of the advantages of the digital age while minimizing associated risks.

Current architectural practices are too complicated

Critical to aligning security strategies with the business is a security architecture, a framework of strategies, tactics and capabilities that provides a common language, a consistent approach and a long-term vision. It incorporates the key objectives of the organization, defines the security requirements and maps out the best approach for deploying targeted security capabilities to support the plan.

However, a detailed Cyber Reference Architecture (CRA) can be overwhelming for executives. To address this challenge, a security architecture should include a set of high-level architectural principles that can be understood by executives and specialists alike.

As a foundation, business leaders must understand the challenges facing security organizations. They should recognize that security must be built into application development and testing processes, and understand how critical it is to have a steady supply of skilled security resources.

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**

Moving to DevSecOps

A fundamental shift underway is the movement from "bolted on" security to "baked in" security, from adding security after production to building in security from the earliest point of development.

That typically involves transitioning from waterfall development practices (finish all development before launching into production), to DevOps (iterative development taking into account what is involved in operating the software, with constant improvements pushed into production as necessary), enabling much more rapid application development, especially for the cloud. Now we're seeing movement to DevSecOps, which ensures that security is considered from project inception.

It is a progression already witnessed in other industries. For instance, drivers once used aftermarket locking bars to connect their steering wheel to their brake pedal, preventing the use of either. Today, baked-in security measures in cars abound, with modern vehicles boasting an array of digital-enabled capabilities including GPS trackers, ignition token proximity sensors, and even tilt sensors to prevent unauthorized attempts to tow vehicles away.

Besides DevSecOps helping address time-to-market requirements, bringing the disciplines together also helps solve another problem: the security talent gap. Recent research from International Information System Security Certification Consortium, or $(ISC)^2$, puts the global skills shortfall at just under 3 million. But with DevSecOps, security is becoming a secondary competency for all developers.

The IT industry has recognized that close-knit, multiskilled teams are the most efficient way to develop new products, rather than relying on monolithic siloed teams such as separate applications and security development departments.

Expediency is vital in the digital era, which means that rather than passing applications and products to a separate team for a lengthy security treatment, the development team itself must validate an application's security — only using the central security team where absolutely necessary. This allows a faster deployment of new capabilities aligned to market demand.

The transition of security responsibility for individual products to the DevSecOps team means that the risk ownership model across the business will look very different in the near future. A central security team will own risk for enterprise-wide issues such as strategy, compliance and threat hunting, while the DevSecOps teams and associated business units will own risk for their products and applications.

The central security team also will be responsible for enabling a secure environment for DevSecOps teams. This includes providing a secure continuous integration/continuous delivery (CI/CD) pipeline, deploying automated security evaluation tooling, and providing mentorship and support for DevSecOps teams as required.

Secure digital transformation imperatives

Trying to make enterprise security easier to understand is an exercise fraught with hazards. Oversimplifying risks ignores the many nuances the risks hold, while an overly expansive approach leads back to complexity.

At the highest level, executives must recognize the need to address three key imperatives:

1. Encrypt everything
2. Verify everything
3. Monitor everything

These imperatives align with DXC's "9 Principles for Enterprise Defense" (**Figure 1**). The principles offered should be discussed with experts who are able to translate technical intricacies into business language.

	Principle	Description
1.	**Information as the key business asset**	Data mastery is the most valuable skill in the digital age.
2.	**Devolve cyber risk**	Move risk ownership to lines of business while preserving central oversight.
3.	**Develop an enterprise-wide resilient workforce**	Ensure that security is built in as property of all business functions and provide targeted training for high-risk groups.
4.	**Cyber resilience**	Design cyber resilient systems, supporting continuous operations during incidents. Assume compromise.
5.	**Implement continuous compliance**	Design systems for introspection, compliance and policy change.
6.	**Security as code**	Deploy security policies in machine-readable format.
7.	**Cloud-to-edge awareness and response (Monitor everything)**	Systems for actionable use of security event capabilities and APIs that enable full-stack response. Monitor everything.
8.	**Security and privacy by design (Encrypt everything)**	Adopt a shift-left approach to implement security and privacy in early design stages. Encrypt everything.
9.	**Identity as the core of trust (Verify everything)**	Make identity management key to digital trust and adopt a zero-trust approach. Verify everything.

Figure 1. 9 Principles for Enterprise Defense

Business drivers and benefits

Each of the architectural Principles for Enterprise Defense offers a set of business drivers and benefits for the enterprise:

1. Information as the key business asset

Data mastery is the most valuable skill in the digital age.

Drivers	Benefits
• Improved business agility • Need to react to changing legislation and regulations	• Reduced operating cost • Client-tailored experiences leading to increased revenue • Access to information by whoever requires it, wherever and whenever it is needed

2. Devolve cyber risk

Move risk ownership to lines of business while preserving central oversight.

Drivers	Benefits
• Agile decision making, made in the context and needs of the business unit • Effective risk governance through executive oversight of decision making and dissemination of corporate risk posture	• Increased accountability • Local risk management supports DevSecOps processes and field-based IoT decision making • Better-informed risk reporting by embedded risk owners

3. Develop an enterprise-wide resilient workforce

Ensure that security is built-in as property of all business functions and provide targeted training for high-risk groups.

Drivers	Benefits
• Threat actors targeting high-risk groups • Security expertise too concentrated in expert teams • The need for diffusion of skills and knowledge to create a resilient enterprise	• Improved awareness to ensure better understanding of risk and mitigation best practices • Targeted and effective engagement for protection of high-risk groups

4. Cyber resilience

Design cyber resilient systems, supporting continuous operations during incidents. Assume compromise.

Drivers	Benefits
• Effective cyber risk treatment • Surviving cyber incidents with minimal business impact • Maintaining competitiveness in an evolving threat landscape	• State of assumed compromise, creating effective planning for remediation and recovery • Planned legal and public relations response to manage client, stakeholder and regulator expectations • Reduced risk of fines and penalties

5. Implement continuous compliance

Design systems for introspection, compliance and policy changes.

Drivers	Benefits
• Infrequent and irregular compliance of traditional applications and projects • External stakeholders demanding more dynamic compliance	• Data-driven governance, risk and compliance • Systems open to internal review and continuous improvement • Free sharing of security state among partners, consumers and suppliers

6. Security as code

Deploy security policies in machine-readable format.

Drivers	Benefits
• Security quality that's typically project-specific • Discrete security that varies between builds and deployments • Cost reduction • Reduced policy change effort	• Security spending proportional to projects' digital risk • Group baselines with additional controls that are project-specific • Capitalize on underlying platform's security

7. Cloud-to-edge awareness and response

Design systems for actionable use of security event capabilities and APIs that enable full-stack response.

Drivers	Benefits
• Need for better informed and more rapid decision making • Move to cost reduction through automation • Continuous third-party supplier assurance	• Enabling predictive analytics • Increased systems visibility • Automated remediation to enable faster mitigation and reduced risk

8. Security and privacy by design

Adopt a shift-left approach by considering security and privacy in early design stages.

Drivers	Benefits
• Lack of good security practice across life-cycle projects • Cost and risk reduction • Regulatory compliance	• Robust security embedded from project instantiation • Decreased total cost of projects • Increased consistency in security and enterprise architecture

9. Identity as the core of trust

Make identity management key to digital trust, verify everything and adopt a zero-trust approach.

Drivers	Benefits
• User, device and bot identity fundamentally weakened without a secure means to authenticate	• Identity and attestation protocols that ensure a chain of trust • Identity controls that provide an additional layer of audit • Access control enabled with identification

Cyber Reference Architecture

To connect these principles to the next level of architectural detail, DXC has created a map between the principles and our Cyber Reference Architecture in Figure 2. DXC Technology has spent the last 5 years pioneering this architectural framework.

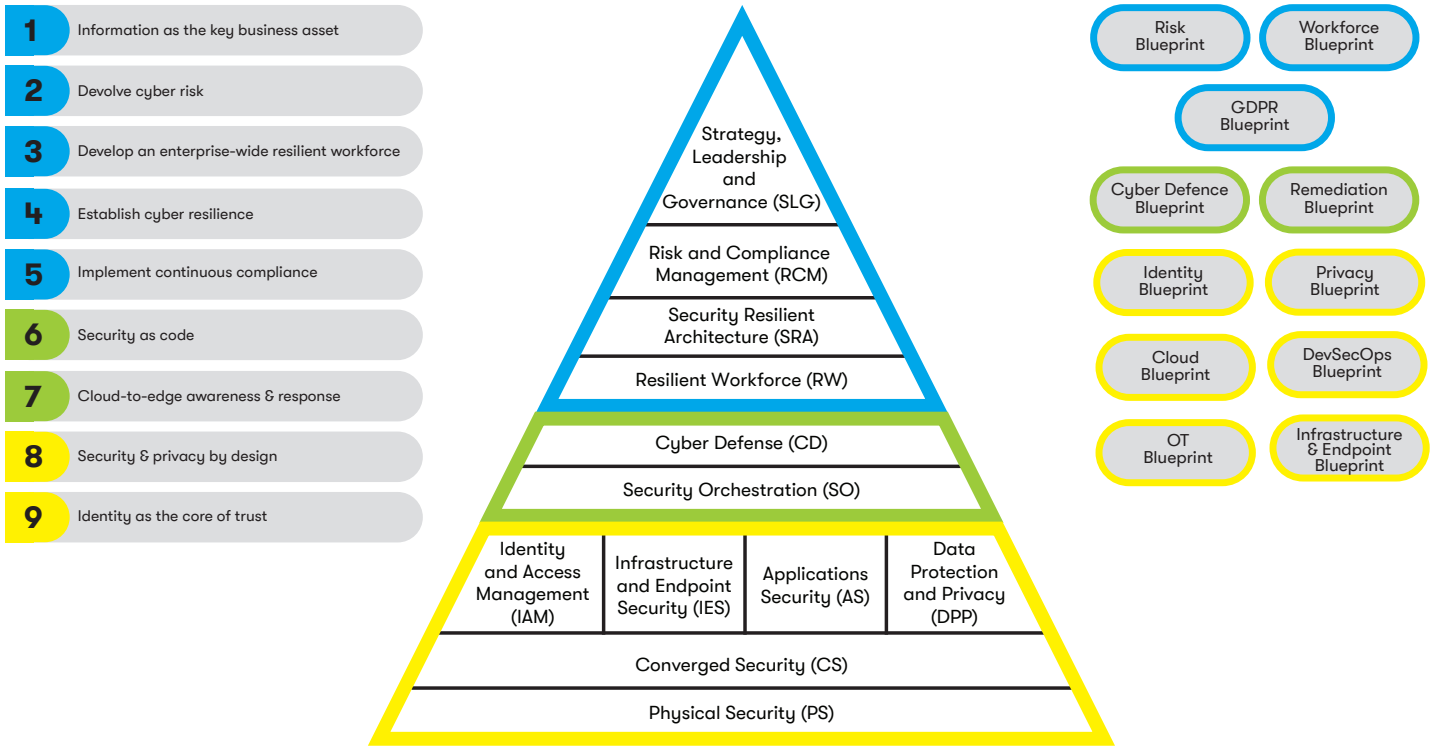


Figure 2. DXC Cyber Reference Architecture

The principles in action

Using the principles, and an architectural framework such as DXC's CRA, allows enterprises to ensure a rigorous approach from the strategic to tactical level. There should be a continuing cycle, as shown in Figure 3, to ensure that security performance is always enabling business objectives.

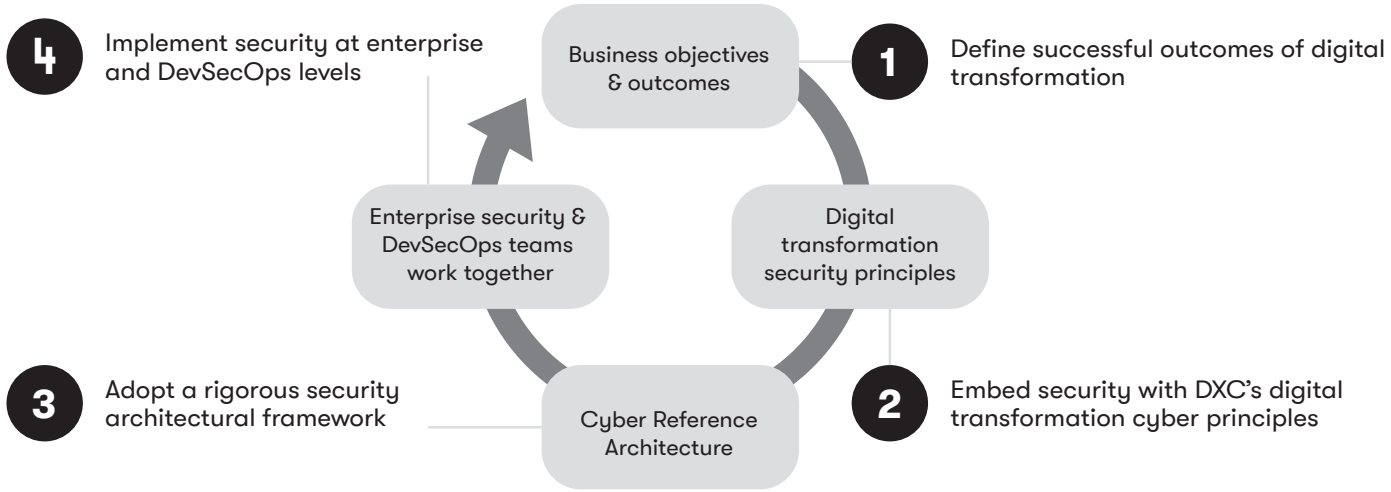


Figure 3. Digital transformation requires an ongoing process that bakes in security to application development and business change.

Looking to the future

The world is changing at an ever-faster rate, and the days of technology being perceived as a necessary evil for enterprises have long since passed. Technology experts now belong in the boardroom as much as they once belonged in the basement. Security leaders and subject matter experts must move the conversation forward by providing and explaining in simple terms the security architectural principles that underwrite modern technology practices and enable businesses to thrive in the digital age.

About the authors

Craig Jarvis is chief technology officer for security at DXC Technology. Craig specializes in the nexus of warfare and technology. He holds master's degrees in both computer forensics and international security. He is currently writing a book on the political history of encryption technologies. Craig previously studied history at Oxford University, and holds master's and bachelor's degrees in classical music.

Simon Arnell is chief security technologist at DXC Technology. Simon has a background in applied security research and development, and in running client proofs of concept. Previously, Simon led the commercialization of the DXC DNS monitoring service and pioneered the use of software-defined networks for rapid incident response, as well as the application of stochastic process modeling and simulation for strategic security-policy decision support.

Mark Evans is chief architect for security at DXC Technology. Mark has a background in enterprise security architecture and cloud security. Previously, Mark was chief security architect for HP/HPE's UK Government Cloud Program (formerly known as Helion-G and now known as DXC UK Restricted Cloud Delivery), designing and delivering secure cloud services for the UK government.

Learn more at www.dxc.technology/security

About DXC Technology

As the world's leading independent, end-to-end IT services company, DXC Technology (NYSE: DXC) leads digital transformations for clients by modernizing and integrating their mainstream IT, and by deploying digital solutions at scale to produce better business outcomes. The company's technology independence, global talent, and extensive partner network enable 6,000 private and public-sector clients in 70 countries to thrive on change. DXC is a recognized leader in corporate responsibility. For more information, visit **www.dxc.technology** and explore **thrive.dxc.technology**, DXC's digital destination for changemakers and innovators.

May 2019