🟩 WHITE PAPER

United Kingdom Secure by Design Zscaler Capabilities & Internal Alignment

Introduction

The United Kingdom's (UK) Secure by Design (SbD) strategy is a proactive approach aimed at bolstering the cyber resilience of the UK government and fostering enhanced collaboration among organizations. While not an assurance process or certification, the UK SbD framework operates as a set of guiding principles intended to consistently deliver robust security measures across the entire lifecycle of UK government services. Positioned as a foundational element within overarching government strategies such as the Government Cybersecurity Strategy and Transforming for a Digital Future, the SbD initiative sets the stage for integrating cybersecurity best practices into digital service delivery and fortifying service resilience. Central to the UK SbD strategy are ten distinct secure by design principles, comprising a comprehensive suite of 46 specific activities. While mandatory for government departments and arm's-length bodies (ALBs), these principles remain optional for other segments of the UK public sector.

As a trusted partner to the UK public sector, Zscaler is deeply committed to not only assisting UK government departments, ALBs, and other public sector entities in the implementation of these principles but also aligning its service offerings with the defined SbD principles internally as well. Through this commitment, Zscaler aims to contribute to the overarching objective of enhancing the UK's cybersecurity posture and ensuring the delivery of secure and resilient digital services across the UK public sector landscape.

Affected parties and timelines

For all central government departments and arm's-length bodies (ALBs), adherence to the UK SbD principles is mandatory for any new services or significant modifications to existing services subject to the digital and technology spend controls approval process. This ensures that these services integrate the requisite security measures mandated by the UK government.

Implementation priority have been categorized into two distinct groups:

- **Group 1** comprises ministerial departments, ALBs responsible for managing government Critical National Infrastructure (CNI), and entities overseeing priority government services.
- **Group 2** encompasses all remaining ALBs and other central government organizations.

While it is encouraged for all organizations to expeditiously adopt the SbD principles, the Cabinet Office will engage with each entity individually to establish tailored implementation schedules. Notably, support from the Central Digital and Data Office (CDDO) will be prioritized for Group 1 organizations, facilitating their swift and effective adoption of the SbD principles.

Security by design principles

The UK SbD principles have been established to provide foundational guidelines that emphasize integrating security measures into the design and development of systems, applications, and products from the outset. These principles aim to proactively address security risks and vulnerabilities, rather than retrofitting security as an afterthought.

Zscaler has built its services with security by design in mind, both in its service capabilities as well as the way in which its services are operated. Zscalers alignment with each of the UK SbD ten (10) foundational principles can be found below.

PRINCIPLE 1
Create Responsibility for Cybersecurity Risk

Objective: Assign risk owners to be accountable for managing cybersecurity risks for a service throughout its lifecycle. These must be senior stakeholders with the experience, knowledge and authority to lead on security activities.

Zscaler Capability Support: While Zscaler doesn't directly create information security programs and assign organizational responsibility, Zscaler services offer invaluable insights to aid senior leadership in decision-making. Leveraging Monte Carlo simulation, Risk360 empowers organizational leaders to assess and mitigate financial risks associated with potential threats, facilitating the establishment of robust security programs and leadership structures. Through its dashboarding capabilities, senior stakeholders access visibility into risk scores, contributing factors, and actionable insights across multiple categories like workforce, third parties, applications, and assets. Moreover, Risk360 streamlines operations by delivering comprehensive risk measurement, actionable recommendations, and real-time metrics across Zscaler services, alongside external vulnerability software integration.

Zscaler Internal Conformance: Zscaler assigns clear responsibilities for cyber risk management throughout its organizational structure. Senior stakeholders, including the VP of Product Management, VP of Cloud Operations, and the VP of Global Compliance oversee the integration of security measures during product development and operations, ensuring compliance with ISO 27001 and SOC 2 standards as a minimum baseline. Risk management is handled through a structured risk assessment process, with high-risk items requiring documented treatment plans and management review. Third-party vendor relationships are managed with thorough due diligence and legal oversight to ensure adherence to security and privacy standards. The privacy team ensures compliance with data protection laws and serves as a liaison for privacy-related inquiries. These measures collectively fortify Zscaler's security posture, ensuring security is a responsibility throughout the organization.

PRINCIPLE 2
Source Secure Technology Products

Objective: Where third-party products are used, perform security due diligence by continually assessing platforms, software, and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.

Zscaler Capability Support: Leveraging automated engines, Zscaler Risk360 analyzes real-time data from various sources, including third-party products, to provide actionable insights and guided investigative workflows for risk mitigation. This enables customers to conduct thorough security reviews before product implementation. Additionally, Zscaler's suite of capabilities, including internet-facing attack surface reduction and zero trust architecture, strengthens third-party risk management efforts by minimizing attack vectors and preventing lateral movement. Risk360 further enhances risk quantification and visualization, empowering leaders to make informed decisions balancing security and usability, with intuitive reporting and the ability to analyze top cybersecurity risk drivers in depth.

Zscaler Internal Conformance: Internally, Zscaler upholds the SbD principle of Source Secure Technology Products by conducting thorough security assessments on all third-party entities handling customer data. This includes ensuring ISO 27001 or SOC 2 certification for data centers storing customer data and performing due diligence on sub-processors to validate their security and privacy practices. Zscaler's Third-Party Risk Management program covers various assessment areas such as business resiliency, cybersecurity, and legal compliance. Additionally, Zscaler tracks vendor information and security issues, conducts annual security reviews, and mandates written commitments to security controls and data protection obligations. Through its Systems and Services Acquisition policy, Zscaler follows documented processes to communicate security needs, review vendor commitments, and assess risks regularly. Zscaler manages security and usability through a defined risk assessment process, encompassing risk identification, analysis, and evaluation, with a risk treatment plan mandated for high-risk scenarios and ongoing management oversight to ensure effective risk mitigation.

PRINCIPLE 3
Adopt a Risk-Driven Approach

Objective: Establish the project's risk appetite and maintain an assessment of cybersecurity risks to build protections appropriate to the evolving threat landscape.

Zscaler Capability Support: Zscaler provides customers with a risk-centric approach to cybersecurity. Utilizing the Zscaler Risk360 platform, which utilizes automation to gather real-time data from both internal and external sources. Customer's are provided with a risk score ranging from 0 to 100, enabling leaders to establish their project's risk appetite and compare their security posture with industry benchmarks over time. Risk360 facilitates the visualization of a customer's zero trust journey score, aiding organizations in quantifying their risk appetite for digital services. Detailed reports, such as the CISO board reports and AI-powered cybersecurity maturity assessments, offer insights into an organization's cyber risk posture and highlight areas for improvement. Additionally, Risk360 allows customers to analyze their risk using frameworks like MITRE ATT&CK, enabling the assessment of an organization's security posture and estimation of financial exposure. Intuitive visualization and reporting capabilities empower leaders to filter and analyze top cybersecurity risk drivers, facilitating informed security decisions and streamlined reporting processes.

Zscaler Internal Conformance: Zscaler implements a comprehensive risk-driven approach to cybersecurity internally, supported by a formal risk assessment and treatment plan process. This process entails identifying assets, threats, and vulnerabilities through extensive research and communication, aligning with the National Institute of Standards and Technology (NIST) 800-30 standard. Zscaler's risk analysis involves assigning values to risks, with high-risk scenarios requiring a detailed treatment plan. The management review team oversees progress against treatment plan targets and exceptions. Additionally, Zscaler utilizes a third-party vendor program to manage subcontractors, ensuring adherence to security standards and privacy practices. Due diligence is performed on subcontractors, and contractual obligations regarding security controls and data protection are documented. Zscaler's ThreatLabz Research team conducts expert-led research on emerging threats, sharing findings to enhance industry-wide cybersecurity. Compliance efforts align Zscaler products with internationally recognized standards such as ISO 27001 and SOC 2, fostering customer confidence. Lastly, Zscaler maintains a risk register evaluated annually as part of its ISO 27001 certification.

PRINCIPLE 4
Design Usable Security Controls

Objective: Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand.

Zscaler Capability Support: Zscaler offers a robust set of capabilities to embody the secure by design principle of Design Usable Security Controls by ensuring security processes are both effective and user-friendly. Zscaler's cloud security services feature a multidimensional role-based access control system that supports hierarchical administration and scope customization, allowing for the restriction of organizational and functional access and obfuscation of usernames. Additionally, Zscaler's Risk360 tool provides customers with detailed cost estimates of their organization's risk, employing financial loss quantification and Monte Carlo modeling to present a range of potential financial outcomes, thereby empowering organizations with quantifiable data for informed decision-making in business case scenarios.

Zscaler Internal Conformance: Zscaler implements a separation of duties model to prevent the misuse of authorized privileges and mitigate the risk of collusion. This model ensures that specific rights are assigned to users based on their defined job duties, with a focus on preventing individuals from simultaneously authorizing security-related accounts and administrative accounts. Additionally, Zscaler conducts a routine business impact analysis (BIA) to assess the implications of significant changes in the environment, with BIA validation included as part of the annual SOC 2 audit, thereby ensuring that security processes remain relevant, effective, and easy to comprehend.

PRINCIPLE 5
Build in Detect and Respond Security

Objective: Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting, and response capabilities. These must be continually tested and iterated.

Zscaler Capability Support: Zscaler's Nanolog Streaming Service (NSS) facilitates seamless communication between Zscaler cloud and third-party security solution devices, enabling real-time streaming of logs to customers' SIEM systems through VM-based or Cloud NSS options. Zscaler Cloud IPS, integrated with technologies like firewalls and sandboxes, provides comprehensive threat protection against various attacks, leveraging custom and industry-leading signatures for real-time monitoring and policy enforcement. Moreover, organizations can proactively identify and remediate vulnerabilities using Zscaler capabilities such as ZIA's Advanced Threats Protection and Mobile Malware Protection policies, while Risk360 offers insights into the external attack surface and lateral propagation risk, enabling informed decisions to enhance an organization's security posture.

Zscaler Internal Conformance: Zscaler continuously monitors business activities and system infrastructure components to identify potential security threats and vulnerabilities internally. Through logging and monitoring tools, Zscaler tracks system performance and alerts IT operations of any unusual activity or service requests. Weekly vulnerability assessments and annual penetration tests are conducted to address weaknesses in the environment. An Incident Response Plan (IRP) ensures efficient management of cyber incidents, with defined incident types and procedures for resolution and investigation to prevent recurrence. Zscaler's Information Security Risk Assessment Plan drives planned third-party risk assessments at defined intervals against industry recognized security frameworks, including ISO 27001 and SOC 2.

PRINCIPLE 6
Design Flexible Architectures

Objective: Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyberthreats and vulnerabilities.

Zscaler Capability Support: Zscaler's Zero Trust Exchange is designed for performance, scalability, and flexibility, enabling organizations to easily integrate new security controls in response to changes in business requirements, cyberthreats, and vulnerabilities. Zscaler leverages shared services internally and integrates with various "best in class" services to optimize overall security posture. Additionally, Zscaler's Risk360 provides mappings to security risk frameworks like MITRE ATT&CK and NIST CSF, ensuring that security controls are implemented and operating effectively. Through its native, multi-tenant cloud and proxy-based architecture for full inspection of encrypted traffic at scale, Zscaler ensures optimal performance, reliability, and strong security, meeting the needs of organizations seeking to implement flexible and adaptive security architectures.

Zscaler Internal Conformance: Zscaler's ISO 27001 and SOC 2 certifications ensure that their change management policies and procedures are rigorously audited, emphasizing the confidentiality of information. These certifications mandate formal operational change management processes, clear roles and responsibilities, and segregation of duties. Production and development environments are segregated, and all changes, whether routine or emergency, require approval and documentation. Additionally, Zscaler maintains high-level deployment requirements, including testing, management approval, establishment of restart points, code review by information security, impact assessments, documentation of system changes, and version control for all software. Through these processes, Zscaler ensures that digital services can be effectively implemented and updated to integrate new security controls in response to changes in business requirements, cyberthreats, and vulnerabilities.

PRINCIPLE 7
Minimize the Attack Surface

Objective: Use only the capabilities, software, data, and hardware components necessary for a service to mitigate cybersecurity risks while achieving its intended use.

Zscaler Capability Support: Zscaler provides comprehensive security features across its suite of services, designed to assist organizations in minimizing their attack surface. ZIA and ZPA enforce traffic flows and provide security event and transaction logs for correlation and management, enabling organizations to monitor and mitigate potential threats effectively. The Zscaler Zero Trust Exchange ensures that users are not placed on the network and applications are never exposed to the internet, significantly reducing the attack surface. Zscaler's SSL inspection capabilities further enhance security by decrypting HTTPS traffic to detect and block malicious content. Additionally, Zscaler's Risk360 and ZPC offerings enable continuous monitoring and vulnerability detection, allowing organizations to proactively address security risks. Through detailed documentation and administrator guides, Zscaler supports organizations in configuring and managing their security settings effectively. Lastly, ZDX provides device inventory tracking, ensuring that service components are appropriately identified and securely retired when necessary, contributing to minimizing the attack surface.

Zscaler Internal Conformance: Zscaler ensures that its service plane is accessible to the internet while the management plane is off-network, effectively reducing the potential attack vectors. Rigorous scanning of all traffic for malware, coupled with comprehensive protection against advanced threats using patented Bytescan technology, enhances the security posture. Zscaler's adherence to secure coding best practices, including static code analysis, quality assurance testing, and vulnerability scanning, further bolsters its defense mechanisms. Moreover, Zscaler's robust risk assessment and risk treatment plan, based on industry standards such as NIST 800-30, enable the identification, analysis, and mitigation of potential risks, ensuring that security measures are continually evaluated and improved. Additionally, Zscaler's Cloud Operations team meticulously manages hardware decommissioning, maintaining strict control over the disposal process to prevent any residual security risks.

PRINCIPLE 8
Defend in Depth

Objective: Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome.

Zscaler Capability Support: Zscaler provides layered controls across its services, making it challenging for attackers to fully compromise systems. Through control by policy content type, reputation-based blocking, content scanning, advanced/multi-feature tools, and behavioral analysis, Zscaler delivers a multi-faceted approach to cyberthreat protection. Zscaler Deception enhances this defense strategy by proactively detecting and disrupting sophisticated threats with decoys and false user paths, complementing the Zero Trust Exchange platform. Integration with endpoint protection platforms like CrowdStrike or Carbon Black further enhances visibility and containment for advanced persistent threats, reducing threat dwell time and time to remediation. Furthermore, Zscaler's Risk360 provides mappings to security risk frameworks and reporting support for regulatory compliance, ensuring that security controls are effectively implemented and operational. Together, these capabilities contribute to a comprehensive defense strategy that strengthens an organization's resilience against cyberthreats.

Zscaler Internal Conformance: Zscaler ensures adherence to internationally recognized standards such as ISO 27001, SOC 2, and Cyber Essentials, embedding diverse security controls throughout its service portfolio. Key components of Zscaler's multi-layer architecture include privacy protection at the web transaction, network, and administrator levels, safeguarding customer data through data segregation mechanisms. Zscaler's incident management function, overseen by the Chief Security Officer, includes a documented Incident Response Plan to efficiently manage cyber incidents and minimize their impact. Additionally, Zscaler conducts rigorous vulnerability assessments, penetration tests, and developer training to identify and mitigate potential vulnerabilities at various stages of the development lifecycle, reinforcing the defense-in-depth strategy. These comprehensive measures collectively strengthen Zscaler's resilience against cyberthreats and enhance its ability to protect customer data and infrastructure effectively.

PRINCIPLE 9
Embed Continuous Assurance

Objective: Implement continuous security assurance processes to create confidence in the effectiveness of security controls, both at the point of delivery and throughout the operation life of the service.

Zscaler Capability Support: Zscaler assists customers in ensuring the effectiveness of security controls throughout the service lifecycle. ZIA's Advanced Threats Protection and Mobile Malware Protection policies provide robust defense against fraud, unauthorized communication, and malicious apps, seamlessly integrating into the vulnerability management programs of organizations. ZDX's device and software inventory functionality enables the identification of active vulnerabilities on associated devices, providing valuable insights into potential security risks. Moreover, Zscaler's service scans all traffic bi-directionally for malware, employing heuristic analysis and patented Bytescan technology to detect and mitigate advanced threats effectively. Zscaler's ZIA Public Service Edges feature Single-Scan, Multi-Action technology, facilitating efficient policy enforcement with minimal latency. Additionally, customers can leverage Zscaler's embedded insights, reporting, logging, dashboards, and diagnostics to continuously monitor and analyze security posture, ensuring ongoing confidence in the effectiveness of security controls. Through these capabilities, Zscaler empowers organizations to embed continuous assurance into their security operations, enhancing resilience against evolving cyberthreats.

Zscaler Internal Conformance: Zscaler conducts information security and privacy risk assessments regularly, complemented by an ongoing cycle of penetration testing performed by external vendors. Furthermore, Zscaler's compliance team ensures alignment with internationally recognized standards such as ISO 27001, SOC 2, and Cyber Essentials, providing customers with the assurance of robust security measures. The dedicated ThreatLabz Research team conducts expert-led research on emerging threats, leveraging expertise from 150+ world-class researchers and threat intelligence from vast data signals. Zscaler's publicly available Cloud Activity Dashboard offers real-time insights into global threat landscapes. Additionally, Zscaler employs a range of tools for vulnerability scanning, logging, monitoring, and intrusion prevention, enabling proactive identification and mitigation of security threats. These comprehensive measures underscore Zscaler's commitment to continuous security assurance and customer protection.

PRINCIPLE 10
Make Changes Securely

Objective: Embed security into the design, development, and deployment processes to ensure that the security impact of changes is considered alongside other factors.

Zscaler Capability Support: Zscaler services are equipped with intuitive interfaces to support organizations in securely configuring their services according to industry best practices or specific organization requirements. Furthermore, Zscaler's Risk360 platform provides advanced risk management capabilities, offering a comprehensive view of risk across the customer's environment. By gathering and quantifying risk data from various sources, including internal entities, configurations, and external attack surface data, Risk360 empowers customers with actionable insights and recommendations through intuitive workflows. Leveraging features like User Risk Score and Configuration Risk Score, Risk360 enables customers to measure and evaluate risk dynamically or integrate it into their overarching risk register. This platform analyzes security data in real-time, allowing customers to quantify risk across key factors such as external attack surface, compromise likelihood, lateral propagation, and data loss, thereby embedding security considerations into the design, development, and deployment processes effectively.

Zscaler Internal Conformance: Zscaler implements robust configuration and change management practices throughout all service lifecycles. This includes adherence to the Configuration Management Plan (CMP) and the utilization of its internal ticketing system to document and approve changes. The responsibility for ensuring compliance with these processes lies with key stakeholders such as the CTO and VP of Engineering, who oversee development, QA, deployment, SecOps, and operations teams. Additionally, Zscaler employs both manual and automated monitoring tools and emphasizes management involvement in day-to-day operations, providing training and coaching as needed. Furthermore, management conducts periodic self-assessments to evaluate the performance of control activities and processes, ensuring consistent application and effectiveness in mitigating risks. Each control activity is assigned a risk level based on the assessed level of risk it addresses, determining the appropriate level of scrutiny and testing to validate its efficacy. Overall, Zscaler's approach prioritizes security throughout the organization's processes and operations, embedding security considerations into every stage of the design, development, and deployment lifecycle.

For additional information regarding the UK Secure by Design Principles, please reach out to our CISO team at Z-CISO@zscaler.com.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.