

Case Study

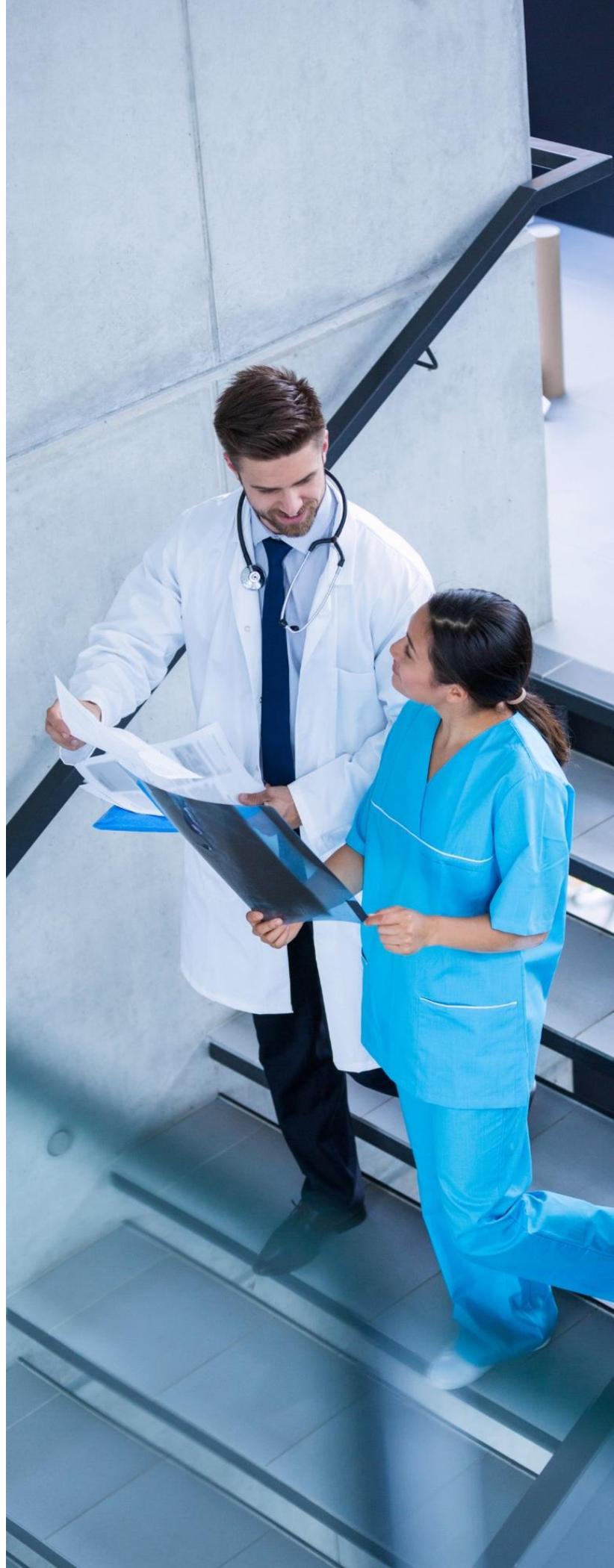


Establishing End-to-End Information Security Across a Healthcare Ecosystem



Summary

A leading healthcare provider partnered with us to elevate its security posture and embed proactive risk management across its IT infrastructure. The engagement focused on building a security-first culture, implementing robust frameworks, and aligning cybersecurity measures with the organization's strategic goals. With a healthcare-specific lens, the program strengthened compliance, enabled secure delivery of projects, and enhanced overall organizational resilience.

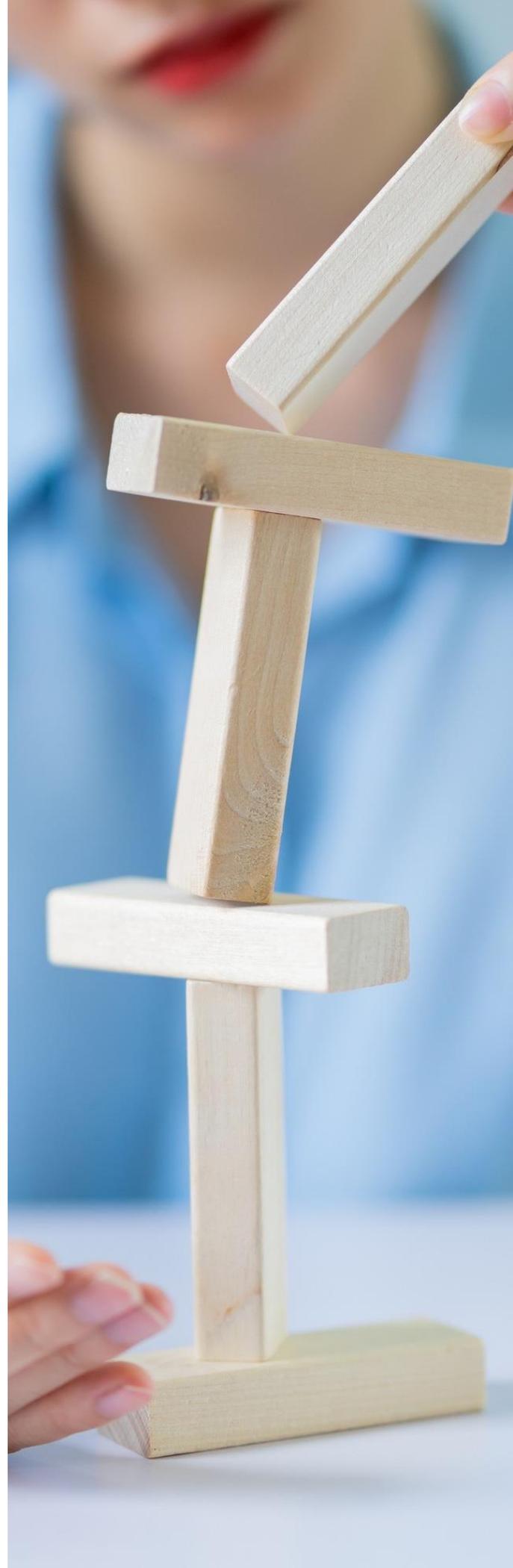


Scope

- Embed security across the organization's operations with the right rigor, maturity, and governance.
- Identify critical vulnerabilities and ensure timely, effective remediation.
- Address organizational exposure to social engineering and phishing attacks.
- Foster an enterprise-wide culture of security awareness and shared responsibility.
- Ensure compliance with leading security frameworks and standards.

Challenges

- Lack of a proactive risk identification or mitigation mechanism.
- Inconsistent security protocols during IT project execution.
- Low awareness of cybersecurity risks among employees.
- No centralized framework to align cybersecurity practices with business goals.
- Exposure to social engineering threats without adequate preventive controls.





Solution

- **Rapid Remediation:** Immediate patching and resolution of known vulnerabilities.
- **Secure-by-Design Approach:** Introduced security controls from the ground up for ongoing and future initiatives.
- **Contextual Implementation:** Aligned security efforts with business priorities to improve adoption and executive sponsorship.
- **Framework-Based Governance:** Applied COBIT capability model and ISO 27000-series (27001, 27002, 27005) for policy standardization, operations, and risk management.
- **Awareness & Training:** Delivered structured information security training to reduce insider risk and improve resilience against social engineering threats.
- **Security Talent Model:** Deployed a core team of seven full-time security experts, supplemented by elastic sourcing through external SMEs for specialized engagements.



Business Value

- **Framework-Driven Operations:** Embedded COBIT and ISO standards to ensure continuous security improvements across daily functions.
- **Reduced Vulnerability Surface:** Accelerated resolution timelines for existing security risks, minimizing potential impact.
- **Workforce Readiness:** Uplifted internal security posture by educating employees, fostering a vigilant security culture.
- **Strategic Alignment:** Gained stronger stakeholder buy-in by contextualizing cybersecurity within business objectives.
- **Scalable Security Model:** Enabled flexible expansion of security resources with external expert partnerships to handle evolving threats and compliance needs.



*****-*****



For more information, please visit www.infinite.com

