Controls to Continuity

Introduction

In today's digital environment organisations face a rapidly evolving threat landscape that makes digital operational resilience as important as prevention and detection. This challenge examines the fictional organisation TechCorp Ltd, which suffered an incident that impaired its resilience and which likely could have been prevented with stronger controls, higher maturity and a broader IT audit scope. Using the 11 resilience dimensions, the NIST Cybersecurity Framework 2.0 and the associated maturity model, you will identify control gaps, assess detection and response, evaluate maturity levels and propose practical IT audit procedures to strengthen the organisation's resilience.

Background Information: TechCorp Ltd.

TechCorp Inc. is a mid-sized FinTech headquartered in Johannesburg, South Africa, founded in 2015 and employing around 500 people; it provides digital payment solutions and mobile banking services to retail and corporate clients across five African countries, processing roughly two million transactions and managing customer financial records including account information, transaction history and personally identifiable information (PII). The company's technology estate is primarily cloud-based, with AWS hosting its payment processing systems, complemented by an on-premises data centre for legacy systems and backups; the environment supports a customer-facing mobile app and web portal, integrates with multiple third-party services (payment gateways, banks and other fintech partners), and is operated by a workforce with varying levels of technical expertise.

TechCorp Inc. maintains a suite of seven controls across governance, asset management, risk, technology, people and recovery. Governance is partially implemented: a CISO reports to the CTO and a cyber security committee meets quarterly, but governance is only partially integrated into business strategy (NIST CSF: Govern; maturity: Partial). Asset management is also partial; a basic hardware and software inventory is updated annually, yet data classification is inconsistent and critical assets are not clearly identified (NIST CSF: Protect; maturity: Partial). The annual risk assessment is implemented with an external consultant and documented in a risk register, though risk appetite has not been formally defined (Risk Identification & Assessments; NIST CSF: Govern; maturity: RiskInformed). Endpoint protection is implemented—all employee devices run antivirus and EDR with monthly updates—reflecting a managed approach to cyber technology and infrastructure (NIST CSF: Protect; maturity: Managed). Security awareness training is provided annually to all staff covering password management, phishing recognition and data handling, but it is not role specific and no phishing simulations are conducted (People, Culture & Awareness; NIST CSF: Respond; maturity: Partial). Backup and recovery are implemented with daily backups stored on premises and in the cloud, documented recovery procedures and a four hour RTO for critical systems (Recovery; NIST CSF: Recover; maturity: Managed and regularly tested). Finally, an incident response plan exists with defined roles and escalation procedures, but it has not been tested in the past 18 months and no incident response team has been formally trained (Incident Detection & Response; NIST CSF: Detect & Respond; maturity: Partial).

On 15 February 2026 TechCorp's IT team discovered unusual activity on its payment processing servers; a subsequent investigation revealed that an attacker had gained unauthorised access via a compromised third-party vendor account after a phishing email to a vendor employee on 20 January 2026. The attacker used the vendor credentials to access TechCorp's payment processing API on 25 January and then exfiltrated customer data—including account numbers, transaction history, names and email addresses—for approximately 50,000 users over an 18-day period to 14 February. Unusual outbound data transfer patterns and anomalous API calls from the vendor account were the indicators that led to detection, which occurred 18 days after initial compromise during a routine log review on 15 February. The incident response team was activated on 16 February and a forensic investigation commenced, with the breach publicly disclosed and regulatory notifications issued on 20 February; there were no direct financial losses to customers thanks to fraud detection systems, but the estimated financial impact to TechCorp is US$2.5 million when accounting for investigation, notification, regulatory fines and reputational damage.

Tasks and Objectives

Utilise your understanding of Cyber resilience dimensions, the NIST 2.0 framework and IT Audit to demonstrate its application through analytical skills, showcasing your insights and conclusion based on the findings regarding TechCorp Ltd.'s cybersecurity resilience

Key Tasks

Your 3-minute video proposal must cover the following:

1. Identify which resilience dimensions have control gaps and recommend missing controls.
2. Analyze why the breach was not detected earlier and recommend detection/response improvements.
3. Assess TechCorp's current resilience maturity using NIST 2.0 CSF maturity levels.
4. Recommend IT audit procedures that would have identified the control gaps and assessed TechCorp's resilience maturity.

Final Requirement

Your plan should be simple, practical, and realistic, helping the company protect its systems while ensuring that operations remain safe and uninterrupted.

April 7th, 12:00PM CET/SAST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

Africa Talent by Deloitte is making an impact that matters by addressing high unemployment rates in South Africa while addressing talent shortages in Europe. Africa Talent professionals provide professional services to Deloitte clients as part of extended teams with European Deloitte firms. Remotely working from the comforts of South Africa. Key expertise areas consist of IT audit, Sustainability Advisory & Assurance, advisory services in Regulatory Risk, Cyber, Business Resilience, Digital Controls, Internal Audit and Internal Support. Guided by the Deloitte ethos of purpose beyond profit, Africa Talent specialists help drive our clients' needs for top class expertise to navigate global changes while supporting their local communities.