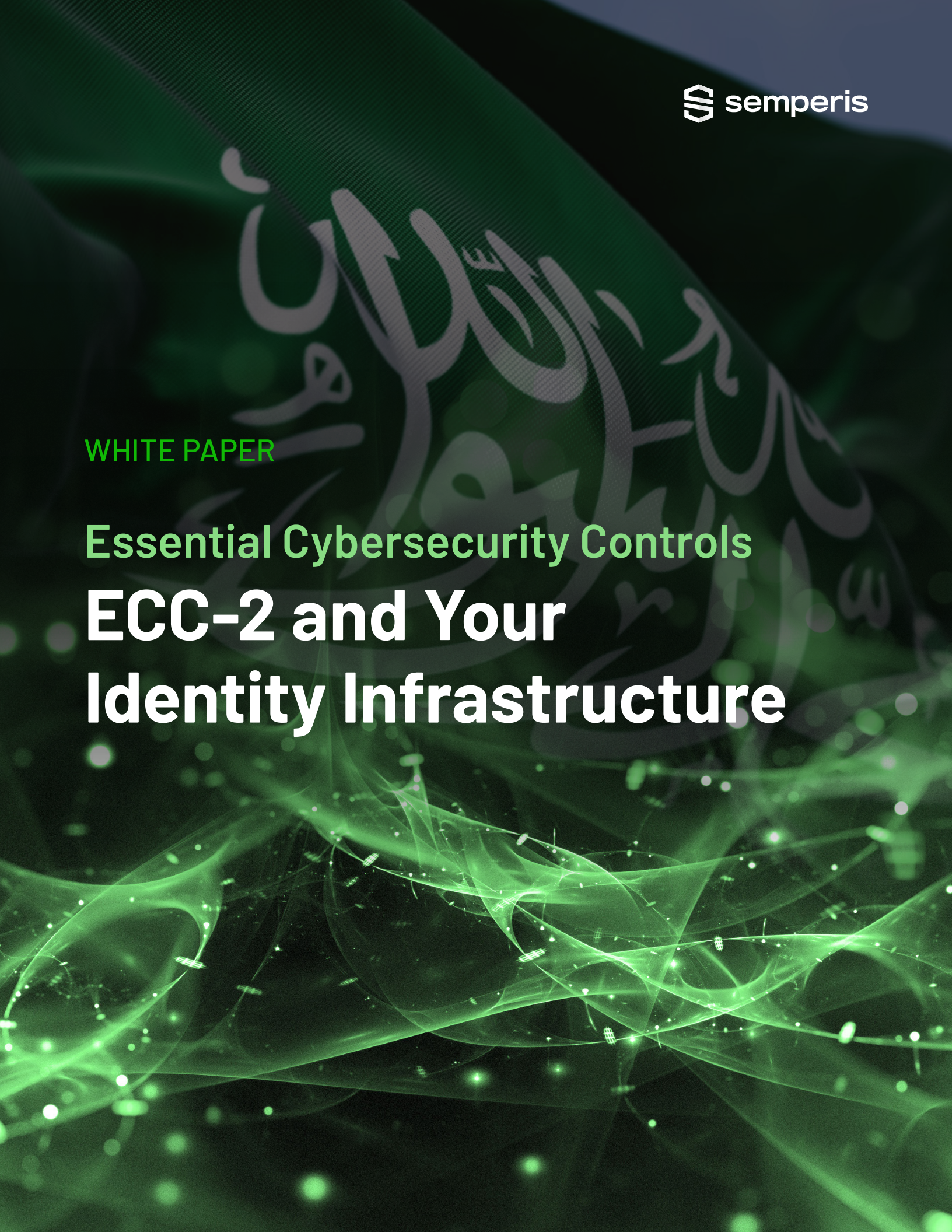


semperis

WHITE PAPER

Essential Cybersecurity Controls

ECC-2 and Your Identity Infrastructure

TABLE OF Contents

semperis

Introduction

The National Cybersecurity Authority (NCA) of Saudi Arabia created the nation's landmark Essential Cybersecurity Controls (ECC-1:2018) standard with a twofold purpose: as a strategic response to address emerging risks and to support Vision 2030,[1] the initiative to build a secure, resilient, and technologically advanced future.

The latest version of the standard, ECC-2:2024, not only mitigates cybersecurity risks but also plays a crucial role in fostering national security and economic diversification.

By securing critical infrastructure, supporting digital transformation, and ensuring compliance with international standards, the ECC strengthens Saudi Arabia's position as a leading player in the global economy and a champion of innovation and technological progress.

The ECC comprises a comprehensive set of regulatory measures and operational frameworks established to safeguard the Kingdom's critical infrastructure, industries, and data. The controls are designed to mitigate emerging risks in cybersecurity, data protection, and operational stability, ensuring that the Kingdom can respond effectively to global challenges in the digital era.

1 Saudi Vision 2030

The emerging threat landscape

The cyber threat landscape is evolving and heavily influenced by geopolitical tensions, rapid technology improvements, and increasing reliance on digital infrastructure. Saudi Arabia's high level of digital transformation, position in the global economy, and importance as a regional political leader make them a target for malicious actors.

Identity remains one of the main threat vectors for organised crime.[2] Password spraying attacks, weak passwords, unhardened access environments, and vulnerabilities in multifactor authentication configuration routinely give attackers an easy way in. In fact, Microsoft reported 7,000 identity-based attacks per second in 2024. Ninety-nine percent of them were password attacks.[3]

With account access, most attackers target **identity systems such as Active Directory (AD) and Entra ID** first. AD presents a large attack surface, and the complexity of its internal relationships makes misconfigurations and vulnerabilities hard to secure. Once AD is compromised, attackers can perform reconnaissance, seize control of data and assets, or launch attacks.

Ransomware continues to cause high-profile, destructive attacks while increasingly exposing sensitive personal and business data from major organisations. Attackers gain access through social engineering or stolen credentials, then quickly pivot to the identity infrastructure, which provides controls for authentication and authorisation across most critical business systems.

Even a prolific ransomware actor like Akira,[4] which is otherwise known for leveraging perimeter device vulnerabilities, makes good use of the AD infrastructure, using tools such as Mimikatz and LaZagne to steal credentials, then creating new administrative accounts on domain controllers for persistence and lateral movement.

2 Ransomware Risk Report - Semperis

3 Microsoft Digital Defense Report 2024

4 Akira, GOLD SAHARA, PUNK SPIDER, Howling Scorpius, Group G1024 | MITRE ATT&CK®

Scope of the ECC-2: 2024

The NCA developed the ECC to establish a minimum cybersecurity baseline for national organisations to align to. The standard is essential for supporting the Kingdom's Vision 2030 and particularly helps secure the continued transformation of the nation's digital infrastructure.

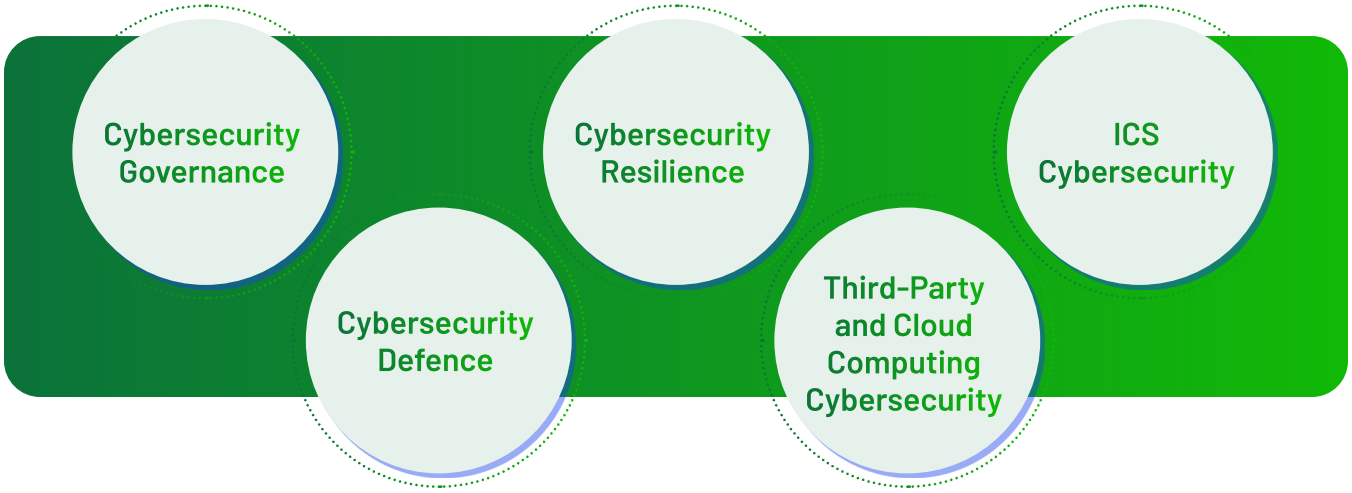
The NCA's mandate states that its responsibility for cybersecurity does not absolve any public, private, or other organisation from its own cybersecurity responsibilities as confirmed by Royal Decree number 57231, dated 10/11/1439H,[5] which states that "all government organisations must improve their cybersecurity level to protect their networks, systems, and data, and comply with NCA's policies, framework, standards, controls, and guidelines."

All national organisations must implement all necessary measures to ensure continuous compliance with the ECC, per item 3 of article 10 of the NCA's mandate and per Royal Decree number 57231, dated 10/11/1439H.

The ECC consists of:

- 5 cybersecurity main domains
- 29 cybersecurity subdomains
- 114 cybersecurity controls

Figure 1. The main domains of the ECC organise the control standard



5 National Cybersecurity Authority Guide to Essential Cybersecurity Controls (ECC) Implementation

ECC and identity infrastructure

The ECC is a comprehensive standard, so we won't cover all of its requirements. Instead, we'll focus on the controls that relate specifically to understanding, monitoring, protecting, and ensuring resilience of identity systems.

Cybersecurity governance

1-6	Cybersecurity in Information and Technology Project Management	How Semperis Can Help
Objective 1-6-2	The cybersecurity requirements in project and assets (information/technology) change management must include at least the following: **1-6-2-1** Vulnerability assessment and remediation **1-6-2-2** Conducting a configurations review, secure configuration, and hardening and patching before changes or going live for technology projects	• Continuously monitor for indicators of exposure and compromise in AD and Entra ID using multiple data sources, including the AD replication stream. • Automatically revert changes to individual attributes, groups, members, objects, and containers in on-premises AD and Entra ID. • Analyse and map attack paths and Tier-0 access. • Evaluate and communicate overall security posture with risk scoring, enabling drill-down into individual security categories for deeper analysis.

Cybersecurity defence

2-2	Identity and Access Management	How Semperis Can Help
Objective 2-2-3	The cybersecurity requirements for identity and access management (IAM) must include at least the following: **2-2-3-1** User authentication based on username and password **2-2-3-2** Multifactor authentication for remote access **2-2-3-3** User authorisation based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege, and Segregation of Duties **2-2-3-4** Privileged access management **2-2-3-5** Periodic review of users' identities and access rights	• Ensure AD hygiene to ensure key identity principles, such as least privilege. • Identify and eradicate misconfigurations and vulnerabilities associated with users in identity systems. • Understand attack paths used to gain administrative access. • Discover attack paths to Tier 0 assets and help identify excessive privileges that attackers can exploit.
2-9	**Backup and Recovery**	**How Semperis Can Help**
Objective 2-9-3	The cybersecurity requirements for backup and recovery management must include at least the following: **2-9-3-1** Scope and coverage of backups to cover critical technology and information assets **2-9-3-2** Ability to perform quick recovery of data and systems after cybersecurity incidents **2-9-3-3** Periodic tests of backup's recovery effectiveness	• Deliver proven, clean-state restore of identity services and dependent capabilities with validated recovery point objectives (RPOs) and recovery time objectives (RTOs). • Automate the complicated AD recovery process to recover identity systems 90% faster than with manual recovery. • Complete post-breach forensics to remove persistence and recover AD to a trusted state. • Recover Entra ID objects and principles to a known good state.

2-10	Vulnerabilities	How Semperis Can Help
Objective 2-10-3	The cybersecurity requirements for technical vulnerabilities management must include at least the following: **2-10-3-1** Periodic vulnerabilities assessments **2-10-3-2** Vulnerabilities classification based on criticality level **2-10-3-3** Vulnerabilities remediation based on classification and associated risk levels **2-10-3-4** Security patch management	• Automate monitoring to combat security posture regression caused by configuration drift—compromised configuration settings that accrue over time, leaving you vulnerable to attacks. • Continuously monitor for indicators of exposure that could result in security compromises to your hybrid on-premises and cloud identity environment. • Leverage built-in threat intelligence from a community of security researchers. • Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation.

2-12	Cybersecurity Event Logs and Monitoring Management	How Semperis Can Help
Objective 2-12-3	The cybersecurity requirements for event logs and monitoring management must include at least the following: **2-12-3-1** Activation of cybersecurity event logs on critical information assets **2-12-3-2** Activation of cybersecurity event logs on remote access and privileged user accounts **2-12-3-3** Identification of required technologies (e.g., security information and event management—SIEM) for cybersecurity event logs collection **2-12-3-4** Continuous monitoring of cybersecurity events **2-12-3-5** Retention period for cybersecurity event logs (must be 12 months minimum)	• Use comprehensive change tracking to identify identity system changes even if security logging is turned off, logs are deleted, agents are disabled or not working, or changes are injected directly. • Identify suspicious changes and isolate changes made by compromised accounts. • Strengthen Identity Forensics and Incident Response (IFIR) operations by automating discovery of the sources and details of incidents. • Send alerts through email notifications as operational and security-related changes happen in your hybrid AD environment. • Integrate with Microsoft Sentinel and Splunk SIEM solutions.

2-13	Cybersecurity Incident and Threat Management	How Semperis Can Help

Objective 2-13-3	The requirements for cybersecurity incidents and threat management must include at least the following:
	2-13-3-1 Cybersecurity incident response plans and escalation procedures
	2-13-3-2 Cybersecurity incidents classification
	2-13-3-3 Cybersecurity incidents reporting to NCA
	2-13-3-4 Sharing incidents notifications, threat intelligence, breach indicators, and reports with NCA
	2-13-3-5 Collecting and handling threat intelligence feeds
		• Review and develop a streamlined crisis and incident response (IR) capability.
		  ◦ Define skill-based roles, responsibilities, and expectations for cross-functional teams and external vendors.
		  ◦ Operationalise crisis and IR frameworks, enhanced with expert playbooks. From preparation to after-action review, establish a complete library to respond effectively.
		  ◦ Consider consolidating fragmented crisis management, IR, downtime planning, and communication tools into a single, secure platform.
		• Leverage attack path analysis to identify dangerous or unintended attack paths to Tier 0 assets and other critical assets. Attackers could abuse these paths to elevate privileges and could introduce these paths to install domain persistence and regain privileged access.
		• Automate the complicated AD recovery process to recover identity systems 90% faster than with manual recovery.
		• Establish post-breach forensics to remove persistence and recover the identity system to a trusted state.
		• Provide comprehensive analysis of IOEs and step-by-step analysis on closing security gaps.

Cybersecurity resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management	How Semperis Can Help
Objective 3-1-3	The cybersecurity requirements for business continuity management must include at least the following: **3-1-3-1** Ensuring the continuity of cybersecurity systems and procedures **3-1-3-2** Developing response plans for cybersecurity incidents that may affect the business continuity **3-1-3-3** Developing disaster recovery plans	• Provide expert review of existing identity disaster recovery plan and understand the business goals, onward dependencies, SLAs, disaster scenarios, and methods currently in place to recover the identity system in the event of a disaster. • Deliver expert-developed plans and build identity system recovery programmes. • Operationalise crisis and IR frameworks, enhanced with expert playbooks. • Test recovery of your identity infrastructure and ensure that it can support dependent capabilities for your wider organisational RTO and RPO.

How can Semperis help?

Semperis leads the industry with Microsoft MVPs in AD and Entra ID recovery and resilience to ensure organisations have AD resilience built into their AD backup, recovery, and security plan. Semperis products are enhanced by deep research from the AD-focused threat team.

Challenge	How Semperis Can Help	Solution
Identification and accountability To comply with the ECC, your organisation should appoint someone responsible for core information technology resilience.	Semperis supports a comprehensive understanding of your identity security posture with identity-focused solutions that enable your teams to: • Assess dependencies to enable AD recovery • Provide visibility into identity system security posture • Conduct risk identification and management, which are key for ECC compliance	• Purple Knight provides point-in-time security assessment of AD that empowers you to understand vulnerabilities and delivers remediation guidance to help you reduce risks in your identity system. • Directory Services Protector (DSP) provides continuous threat and vulnerability detection, capturing every change made in AD, helping identify malicious changes, and automatically rolling back risky changes.
Access control You rely on the integrity, security, and resilience of AD and Entra ID to achieve privileged access and identity and access management (IAM) objectives.	Semperis solutions enable you to strengthen your IAM controls by: • Identifying and eradicating misconfigurations and vulnerabilities • Accelerating recovery in case of an outage to enable teams to continue working securely • Understanding attack paths used to gain administrative access	• DSP enables continuous monitoring of AD and Entra ID security posture. • ADFR reduces AD forest recovery time by up to 90%. • Forest Druid (a no-cost community tool) discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit. • Forest Druid supports AD teams with automatic attack path mapping.

Challenge	How Semperis Can Help	Solution
Resilience and business continuity To comply with the ECC, you need to be able to restore your identity infrastructure rapidly, and you must have tests that validate you can accomplish this.	Semperis solutions empower business resilience by helping you: • Enable early detection or avoidance of a security breach of your identity infrastructure and dependent ICT services • Achieve proven, clean-state restore with validated RPOs and RTOs. • Maintain secure and efficient ICT services	• ADFR automates the complicated recovery process for AD and recovers AD up to 90% faster. • ADFR also enables post-breach forensics to remove persistence and recover AD to a trusted state. • Disaster Recovery for Entra Tenant (DRET) recovers Entra ID objects.
Monitoring and detection Your identity infrastructure is a rich source of vulnerabilities and misconfigurations, requiring skill and dedication for meaningful detection.	Semperis supports cybersecurity teams with solutions that automate critical tasks and enable: • Monitoring for AD and Entra ID core dependency to all IT systems—aligning with the strong ECC requirement to detect attacks and enable accurate incident reporting • Comprehensive control of the constantly changing AD environment with its rich attack surface • Visibility into AD-focused attacks and changing vulnerabilities	• DSP continuously monitors AD and Entra ID for indicators of exposure and compromise and automatically rolls back malicious changes in AD. • DSP provides comprehensive logs and highly specialised AD and Entra ID threat analysis, enabling up-to-date, industry-leading insights, automation of identity security monitoring, and enrichment of SOC visibility through SIEM integration.

Challenge	How Semperis Can Help	Solution
Incident response and forensics The ECC imposes strict incident preparedness and reporting requirements on organisations.	Semperis provides modern solutions for identity system defence before, during, and after an attack, enabling your teams to: • Centralise and streamline cyber crisis planning and incident response • Ensure incident response capabilities can be executed, even when production systems are down • Detect actions of malicious actors and rapidly report incidents and attacks impacting AD and Entra ID • Secure your logs for forensic analysis	• Ready1 centralises and unifies all aspects of cyber crisis planning and incident response, ensuring seamless crisis response through preparation, collaboration, and enterprise-wide communications. • DSP's comprehensive change tracking enables you to track changes even if security logging is turned off, logs are deleted, agents are disabled or not working, or changes are injected directly into AD or Entra ID. • Lightning IRP uses machine learning to detect ongoing attacks on AD, which are traditionally buried in logs and difficult to detect.
Continuous improvement Auditors and regulators will seek evidence of your continuous improvement.	With the guidance of industry-leading experts, Semperis partners with you to: • Ensure crisis preparedness through tabletop exercises and rigorous incident response plan testing • Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation	• Ready1 operationalises proven crisis and incident response frameworks, enhanced with expert playbooks—from preparation to after-action review—enabling teams to develop, test, remediate, and continuously improve incident response planning. • DSP and ADFR drive best-of-breed resilience and risk reduction for your identity systems. They are essential tools that can integrate with your organisation's overall security programme.

Conclusion

Saudi Arabia's ECC standard applies to the Kingdom's government sector and private sector organisations that own, operate, or host Critical National Infrastructures. This robust standard requires significant measures to achieve compliance. As you put in place the measures needed to comply, we recommend that you establish seven major capabilities for the resilience of your AD and Entra ID services:

1. Establish governance and ownership for your identity systems.
2. Build visibility into risks and dependencies.
3. Establish comprehensive and automated exposure, threat, and vulnerability monitoring, and integrate this capability into your SOC.
4. Reduce your identity system vulnerabilities to decrease the attack surface for penetration testers and attackers alike.
5. Build robust response capabilities for your identity services to enable rapid incident response, reporting, and forensic capabilities.
6. Have an automated and tested recovery process to enable rapid restoration in case of a destructive incident.
7. Establish a project of continuous improvement, including adopting best practices from the cybersecurity industry.

In our experience, achieving these capabilities is challenging. Sustaining them over time is not possible without significant automation. Semperis' market-leading products can provide you with this threat-led, automated capability.