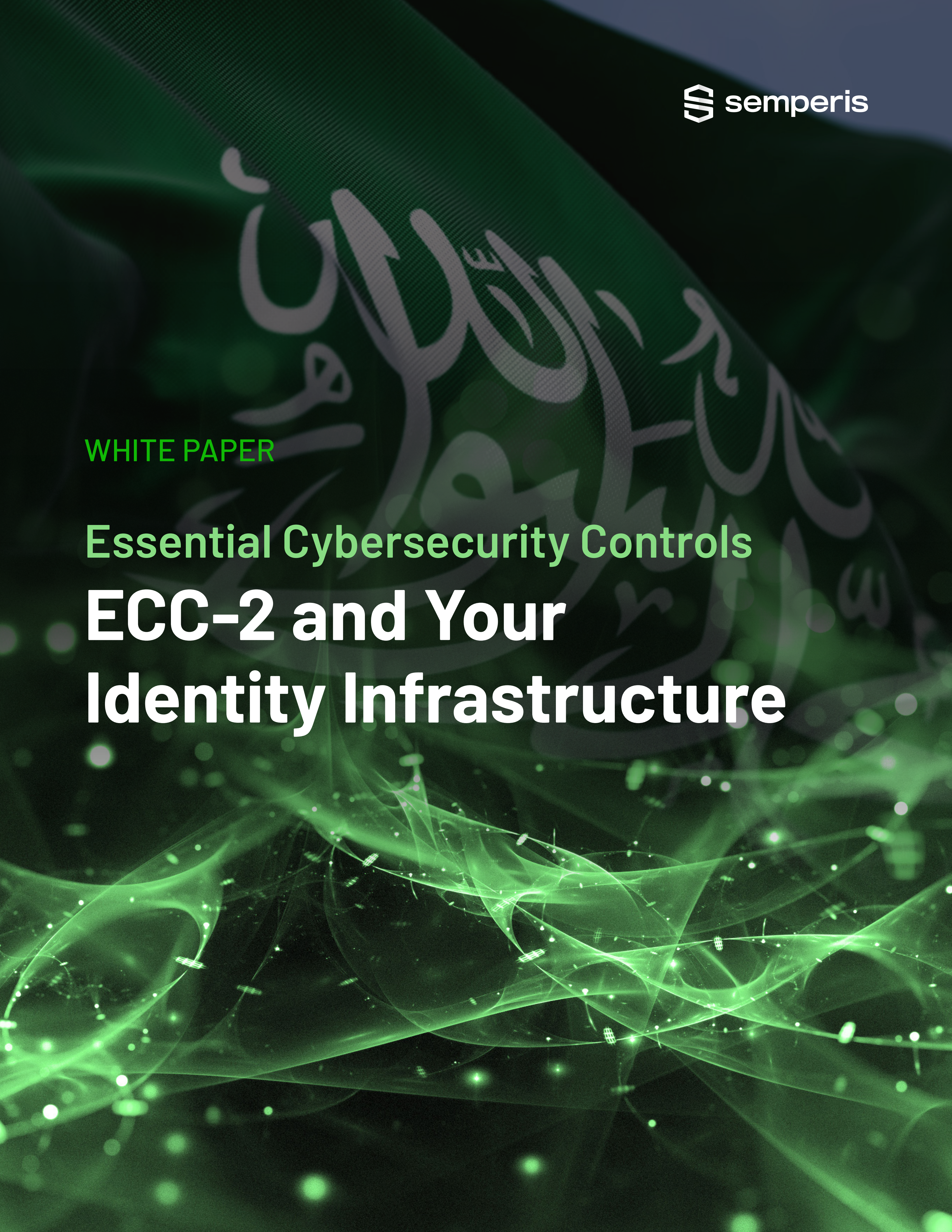


semperis

WHITE PAPER

Essential Cybersecurity Controls

ECC-2 and Your Identity Infrastructure

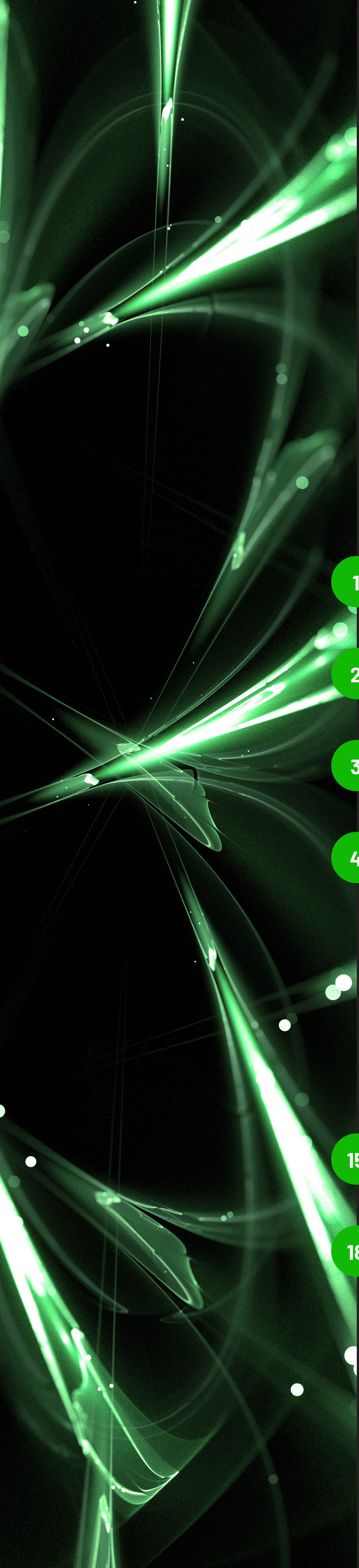


TABLE OF Contents

1 Introduction

2 The emerging threat landscape

3 Scope of the ECC-2: 2024

4 ECC and identity infrastructure

4 Cybersecurity governance

5 Cybersecurity defence

13 Cybersecurity resilience

14 Third-party and cloud computing cybersecurity

15 How can Semperis help?

18 Conclusion

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.

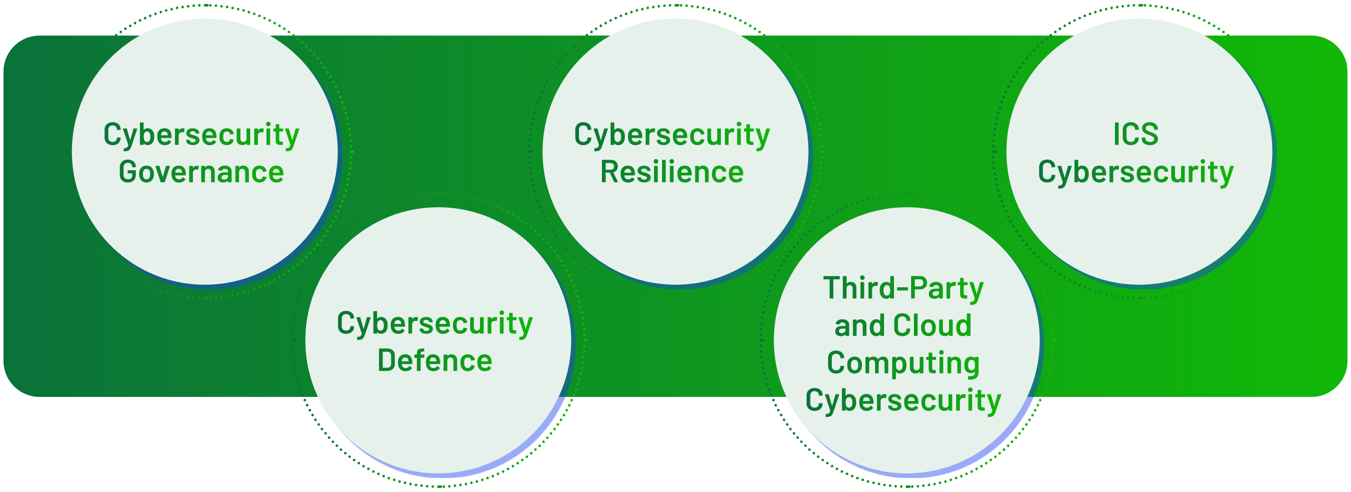
The NCA's mandate states that its responsibility for cybersecurity does not absolve any public, private, or other organisation from its own cybersecurity responsibilities as confirmed by Royal Decree number 57231, dated 10/11/1439H,[5] which states that "all government organisations must improve their 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	• Provide tamper-proof visibility by tapping into the immutable AD replication stream and multiple data sources. • Perform continuous and automated red-teaming to identify security posture, uncover AD vulnerabilities, and identify misconfigurations. • Analyse attack maps and map Tier 0 assets. • Find indicators of attacks, exposure, and compromise. • Review configuration and architecture. • Conduct risk and threat identification, mitigation, and remediation.

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 for Zero Trust. • Identify and eradicate misconfigurations and vulnerabilities associated with users in AD and Entra ID. • Accelerate recovery in case of an outage to enable teams to continue working securely. • Understand attack paths used to gain administrative access. • Discover attack paths to Tier 0 assets and help identify excessive privileges that attackers can exploit.
2-5	**Network Security Management**	**How Semperis Can Help**
Objective 2-5-3	The cybersecurity requirements for network security management must include at least the following: **2-5-3-7** Security of Domain Name Service (DNS)	• Provide tamper-proof logs and highly specialised AD and Entra ID threat analysis with Directory Services Protector (DSP), enabling up-to-date, industry-leading insights and automation for identity security and enrichment of Security Operations Centre (SOC) visibility through security information and event management (SIEM) integration. • Monitor AD and Entra ID to detect attacks and accurately report on incidents and the configuration state. • Provide comprehensive control of the constantly changing, rich AD attack surface, including DNS. • Deliver visibility into AD-focused attacks and changing vulnerabilities. • Continually assess indicators of exposure (IOEs) in AD, automatically roll back malicious changes, and detect machine learning (ML)-based attacks on AD.

2-9	Backup and Recovery	How Semperis Can Help
Objective 2-9-1	Cybersecurity requirements for backup and recovery management must be defined, documented, and approved.	• Review architectural, operational, and technical levels through a comprehensive assessment. • Provide a strategic roadmap for improving security posture and tactical steps for mitigating security exposures. • Align with industry best practices and hinder adversary tactics, techniques, and procedures (TTP). • Produce an actionable roadmap geared toward reaching the desired state. • Provide backup and disaster recovery review. • Provide consultation and planning services.
Objective 2-9-2	The cybersecurity requirements for backup and recovery management must be implemented.	• Reduce risk, create muscle memory, and enable rapid recovery without re-introducing the attacker. • Ensure the first step in a post-breach scenario is completed successfully with better, tested, and guaranteed recovery time objectives (RTOs) and recovery point objectives (RPOs). • Post cyber-first AD recovery using pre-configured integrations with traditional backup solutions to trigger recovery of other systems.

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	• Ensure early detection or avoidance of a security breach of your identity infrastructure and dependent information and communication technology (ICT) services. • Deliver proven, clean-state restore with validated RPOs and RTOs. • Ensure well-maintained ICT services. • Automate the complicated recovery process for AD and recover AD up to 90% faster than with manual recovery process. • Complete post-breach forensics with Active Directory Forest Recovery (ADFR) to remove persistence and recover AD to a trusted state. • Recover Entra ID objects and principles to a known good state with Disaster Recovery for Entra Tenant (DRET).
Objective 2-9-4	The cybersecurity requirements for backup and recovery management must be reviewed periodically.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation. • Reduce risk for your identity infrastructure services. • Conduct recovery drills for AD and review backup and recovery process. • Integrate with your organisation's security programme and drive continuous improvement in security posture, visibility, and resilience.

2-10	Vulnerabilities	How Semperis Can Help
Objective 2-10-1	Cybersecurity requirements for technical vulnerabilities management must be defined, documented, and approved.	• Review architectural, operational, and technical levels through a comprehensive assessment of AD and Entra ID. • Provide a strategic roadmap for improving security posture and tactical steps for mitigating security exposures. • Align with industry best practices and hinder adversary TTP. • Produce an actionable roadmap geared towards reaching the desired state.
Objective 2-10-2	The cybersecurity requirements for technical vulnerabilities management must be implemented.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation. • Drive best-of-breed resilience and risk reduction for your identity infrastructure services with DSP and ADFR. These essential tools can integrate with your organisation's overall security programme.
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	• Deliver real-time and periodic vulnerability assessments of AD and Entra ID. • Enable comprehensive control of the constantly changing AD environment, with its rich attack surface, including risk and criticality level. • Enable vulnerability management and exposure and threat detection with DSP. • Automatically remediate vulnerabilities and maintain a secure state. • In event of a breach or an AD disaster, provide automated, clean restore to any hardware or cloud solution with ADFR.

2-10	Vulnerabilities	How Semperis Can Help
Objective 2-10-4	The cybersecurity requirements for technical vulnerabilities management must be reviewed periodically.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation. • Identify and mitigate threats. • Drive best-of-breed resilience and risk reduction for your identity infrastructure services with DSP and ADFR. These essential tools can integrate with your organisation's overall security programme. • Provide automated, continuous, vulnerability assessment in cadence.

2-12	Cybersecurity Event Logs and Monitoring Management	How Semperis Can Help
Objective 2-12-1	Cybersecurity requirements for event logs and monitoring management must be defined, documented, and approved.	• Enable comprehensive control of the constantly changing AD environment, with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities. • Integrate with SIEM solutions and restore sight to SIEM if attackers manage to tamper with logs at the source in AD.
Objective 2-12-2	The cybersecurity requirements for event logs and monitoring management must be implemented.	• Review architectural, operational, and technical levels through a comprehensive assessment. • Align with industry best practices and hinder adversary TTP.

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., 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)	• Provide visibility into identity system security posture. • Conduct risk identification and management compliance. • Secure logs for forensic analysis. • Enhance ability to detect actions of malicious actors and rapidly report incidents and attacks impacting AD and Entra ID. • Enable continuous assessment of IOEs in AD, automated rollback of malicious changes, and detection of ML-based attacks on AD with DSP. • Provide tamper-proof logs and highly specialised AD and Entra ID threat analysis with DSP, enabling up-to-date, industry-leading insights and automation for identity security and enrichment of SOC visibility through SIEM integration. • Use AI-based learning in Lightning Identity Runtime Protection (IRP) to detect ongoing attacks on AD, which are traditionally buried in logs and difficult to detect.
Objective 2-12-4	The cybersecurity requirements for event logs and monitoring management must be reviewed periodically.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation. • Drive best-of-breed resilience and risk reduction for your directory infrastructure services with DSP and ADFR. These essential tools can integrate with your organisation's overall security programme.

2-13	Cybersecurity Incident and Threat Management	How Semperis Can Help
Objective 2-13-1	Requirements for cybersecurity incidents and threat management must be defined, documented, and approved.	• Enable comprehensive control of the constantly changing AD environment, with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities. • Contribute to incident and threat management by ensuring continuous identity threat detection and remediation. • Enhance cyber resilience by automating cyber-first AD forest recovery, one of the first and most critical elements of post-breach recovery.
Objective 2-13-2	The requirements for cybersecurity incidents and threat management must be implemented.	• Review architectural, operational, and technical levels through a comprehensive assessment. • Align with industry best practices and hinder adversary TTP. • Provide additional assistance as explained in 2-13-1.

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	• Secure logs for forensic analysis. • Enhance ability to detect actions of malicious actors and to provide rapid incident reporting of attacks impacting AD and Entra ID. • Deliver proven, clean-state restore with validated RPOs and RTOs. • Automate the complicated recovery process for AD with ADFR and recover AD up to 90% faster than with manual recovery. • Provide post-breach forensics with ADFR to remove persistence and recover AD to a trusted state. • Provide comprehensive analysis of IOEs and step-by-step analysis on closing security gaps with DSP. • Enable post-breach forensics investigations with ADFR. Results can be used during disaster recovery or penetration testing exercises to ensure a clean restore of AD services. • Provide additional assistance as explained in 2-13-1.
Objective 2-13-4	The requirements for cybersecurity incidents and threat management must be reviewed periodically.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation. • Drive best-of-breed resilience and risk reduction for your identity infrastructure services with DSP and ADFR. These essential tools can integrate with your organisation's overall security programme. • Provide additional assistance as explained in 2-13-1.

Cybersecurity resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management	How Semperis Can Help
Objective 3-1-1	Cybersecurity requirements for business continuity management must be defined, documented, and approved.	• Provide a clear view of current AD security posture and a report to address security exposures at the strategic, operational, and tactical levels. Semperis Identity Forensics & Incident Response (IFIR) service delivers these requirements, along with recovery guidance and tests.
Objective 3-1-2	The cybersecurity requirements for business continuity management must be implemented.	• Review architectural, operational, and technical levels through a comprehensive assessment of AD. • Align with industry best practices and hinder adversary TTP. • Enhance cyber resilience and business continuity by automating cyber-first AD forest recovery, one of the first and most critical elements for post-breach recovery.
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 AD disaster recovery plan and understand the business goals, service-level agreement, disaster scenarios, and methods currently in place to recover AD in the event of a disaster. • Deliver expert-developed plans and build AD and Entra ID recovery programmes. • Test recovery programmes and ensure that organisational RTOs and RPOs are improved and align to your organisational goals. • Provide additional assistance as explained in 3-1-2.
Objective 3-1-4	The cybersecurity requirements for business continuity management must be reviewed periodically.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation. • Provide expert biannual review of process and test recovery drill.

Third-party and cloud computing cybersecurity

4-1	Third-Party Cybersecurity	How Semperis Can Help
Objective 4-1-3	The cybersecurity requirements for contracts and agreements with IT outsourcing and managed services third parties must include at least the following: **4-1-3-1** Conducting a cybersecurity risk assessment to ensure the availability of risk mitigation controls before signing contracts and agreements or upon changes in related regulatory requirements.	• Provide a strong view of the security posture of outsourced identity infrastructure services. • Deliver evidence of resilience and restorability of your identity infrastructure services. • Enable vulnerability management and exposure and threat detection with DSP.

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 must appoint someone responsible for ICT resilience.	• Map dependencies to enable AD recovery. • Provide visibility into identity system security posture. • Conduct risk identification and management, which are key for ECC compliance.	• ADFR automates forest recovery, including relevant dependencies. • Purple Knight provides point-in-time security assessment of AD. Scans run over time provide ongoing threat and vulnerability detection and validation of security posture. • DSP provides tamper-proof tracking by capturing every change made in AD, helps identify malicious changes, and provides automatic rollback of malicious changes. • Migrator for AD streamlines AD modernisation by mapping dependencies and migrating objects to a greenfield AD environment.
Access control You rely on the integrity, security, and resilience of AD and Entra ID to achieve privileged access and IAM objectives.	• Identify and eradicate misconfigurations and vulnerabilities. • Accelerate recovery in case of an outage to enable teams to continue working securely. • Understand 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.	• 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. • DRET recovers Entra ID objects and principles to a known good state.
Monitoring and detection Your identity infrastructure is a rich source of vulnerabilities and misconfigurations, requiring skill and dedication for meaningful detection.	• 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. • Maintain comprehensive control of the constantly changing AD environment, with its rich attack surface. • Maintain visibility into AD-focused attacks and changing vulnerabilities.	• DSP enables continuous assessment of IOEs in AD, automated rollback of malicious changes, and detection of ML-based attacks on AD. • DSP provides tamper-proof logs and highly specialised AD and Entra ID threat analysis, enabling up-to-date, industry-leading insights and automation for directory security and enrichment of SOC visibility through SIEM integration.

Challenge	How Semperis Can Help	Solution
Managing ICT third-party risk If you outsource AD operations, you will need a strong focus on third-party risk. If you leverage Entra ID, Microsoft will be that supplier to your organisation.	• Maintain a strong view of the security posture of outsourced identity infrastructure services. • Provide evidence of resilience and restorability of your identity infrastructure.	• DSP enables vulnerability management and exposure and threat detection. • ADFR provides automated, clean restore to any hardware or cloud solution.
Threat-led penetration testing Your organisation must have the ability to avoid adverse findings in testing or rapidly address issues already found.	• Remediate critical vulnerabilities in your identity infrastructure before penetration testing. • Address test findings after the event. • Provision a realistic test environment to avoid the need to test live systems.	• DSP provides comprehensive analysis of IOEs and step-by-step analysis for closing security gaps. • ADFR enables post-breach forensics investigations, which can be used during disaster recovery or penetration testing exercises to ensure a clean restore of AD services.
Incident response and forensics The ECC imposes strict incident preparedness and reporting requirements on organisations.	• Secure your logs for forensic analysis. • Enhance ability to detect actions of malicious actors and rapidly report incidents and attacks impacting AD and Entra ID.	• DSP's tamper-proof 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 AI-based 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 dedication to continuous improvement.	• Drive continuous improvement and automation through Semperis' industry-leading threat intelligence and automation.	• 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 eight major capabilities for the resilience of your AD and Entra ID services:

1. Establish governance and ownership for your identity services.
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 vulnerabilities to decrease the attack surface for penetration testers and attackers alike.
5. Ensure you have the appropriate requirements and means of managing identity services risk in your supply chain.
6. Build robust response capabilities for your identity services to enable rapid incident response, reporting, and forensic capabilities.
7. Have an automated and tested recovery process to enable rapid restoration in case of a destructive incident.
8. 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.