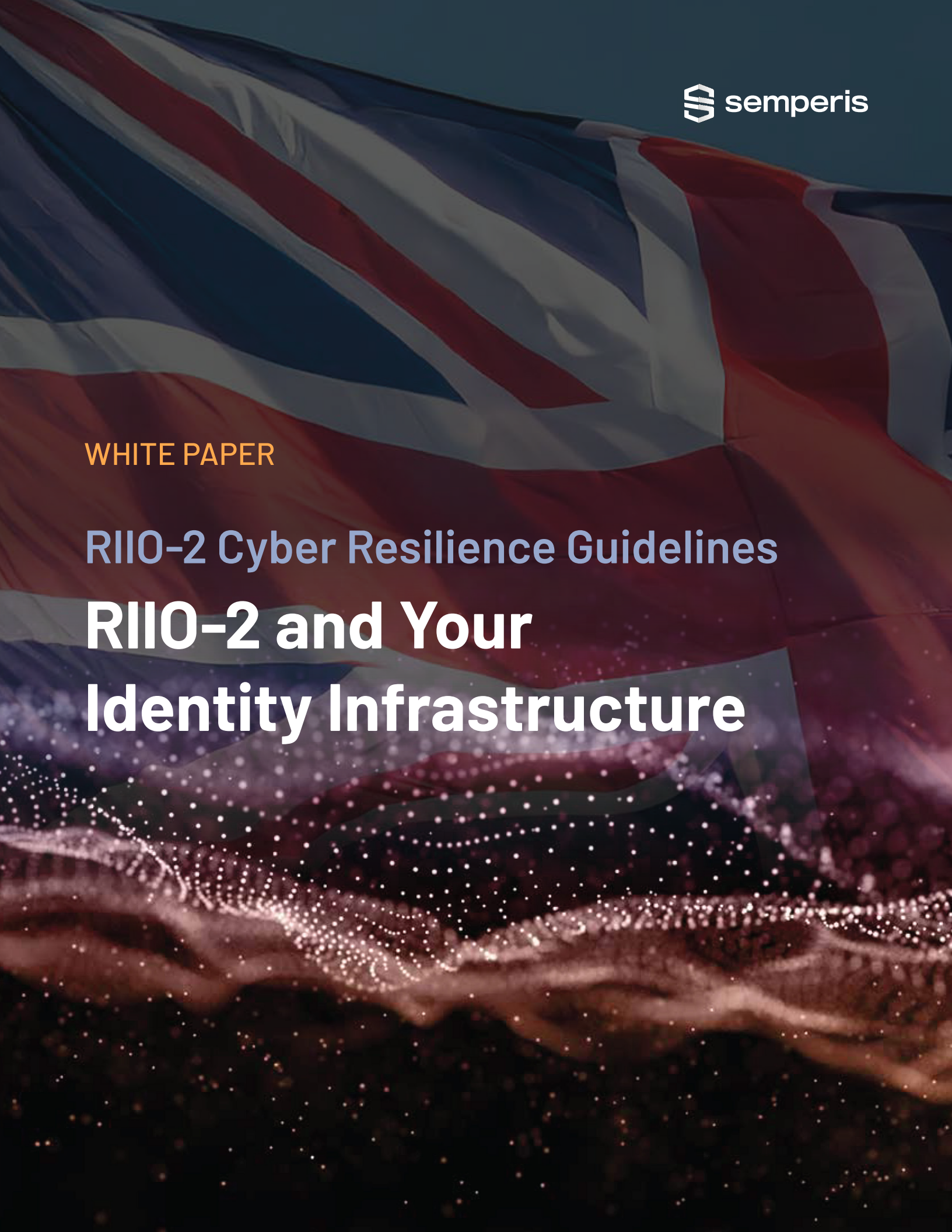

semperis

WHITE PAPER

RIIO-2 Cyber Resilience Guidelines

RIIO-2 and Your Identity Infrastructure

TABLE OF Contents

Introduction

The United Kingdom's Office of Gas and Electricity Markets (Ofgem), an independent National Regulatory Authority, helps balance consumer protections and business viability across critical utilities infrastructure. Through comprehensive guidelines published in accordance with its Revenues = Incentives + Innovation + Outputs (RIIO) methodology, Ofgem oversees policy-driven requirements for price controls and resilient utility operations across the UK.

Updates to RIIO guidelines are published every five years. The current **RIIO-2 requirements in effect through March 2026** include specific Cyber Resilience Guidelines,[1] which were originally published in 2020. Supplementary guidance published in 2023[2] assists operators of essential services (OESs) in downstream gas and electricity sectors to maintain up-to-date compliance with cybersecurity requirements as defined in the EU's Network and Information Systems Regulations (NIS)[3] and the UK's Cyber Assessment Framework, compiled by the National Cyber Security Centre.[4]

This paper will examine how these guidelines apply to your enterprise identity system and the importance of identity security for the overall resilience of utility operations.

1 RIIO-2 Cyber Resilience Guidelines | Ofgem
2 NIS Supplementary Guidance and CAF Overlay for DGE Sector
3 The Guide to NIS | ICO
4 Cyber Assessment Framework - NCSC.GOV.UK

Why RIIO-2 for cyber resilience?

In 2016, the EU and UK recognised the marked increase in threats against critical national infrastructure. The NIS directive,[5] updated and extended in 2022,[6] noted that energy networks are particularly under threat from both organised crime and nation-state threat actors.

The importance of cyber resilience in energy utilities was becoming apparent as early as 2011, when cyberattacks from Russia's Federal Security Service (known as the FSB) targeted North American and Middle Eastern energy companies using Industrial Control System–focused malware, including TRITON and Havex.[7]

In the intervening years, attacks on European energy providers, gas distributors, and end-to-end electricity providers have increased, punctuated by high-profile attacks like the infamous NotPetya campaign of 2017;[8] attacks on the Creos Luxembourg gas pipeline,[9] the Greek natural gas distributor DESFA,[10] and the Spanish energy provider Iberdrola in 2022;[11] and the highly destructive Colonial Pipeline breach in 2021.[12]

Semperis' 2025 report *The State of Critical Infrastructure Resilience* reveals that cyber threats pose a continual and growing risk to utility operators. Among UK respondents:

57% reported being targeted by cyberattacks in the past year

74% of those were attacked multiple times

It's notable that 43% of UK utility operators surveyed reported not being targeted. However, cybersecurity experts caution it's more likely that a good portion of these organisations simply can't detect attacks that are designed to remain hidden.[13]

Hostile nation-states looking for a tactical or strategic advantage are using these stealthy attacks, known as *sleeper* or *Living-off-the-Land* attacks, more often. In contrast to ransomware attacks, which typically seek a quick monetary return, nation-state–sponsored attacks often involve keeping a malicious actor hidden, planting backdoors, gathering information, and waiting to strike—sometimes for years.

In the face of this complex cyber threat landscape, the RIIO-2 Cyber Resilience Guidelines aim to provide the controls UK energy utilities need to establish security resilience for their networks.

---

5 DIRECTIVE (EU) 2016/ 1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 6 July 2016 - concerning measures for a high common level of security of net work and information systems across the Union

6 Directive - 2022/2555 - EN - EUR-Lex

7 Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector | CISA

8 The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED

9 BlackCat ransomware claims attack on European gas pipeline

10 Greek natural gas operator suffers ransomware-related data breach

11 Spanish energy giant hit by data breach - IT Security Guru

12 Colonial Pipeline ransomware attack - Wikipedia

13 The State of Critical Infrastructure Resilience | Semperis Guides

Identity security: A critical focus for utility operators

When pressed to identify the top cybersecurity risks in their operations, utility operators typically point to a range of possibilities, including compromise of systems and supply chains, patching and maintenance of legacy systems, nation-state threats, and insider threats. Only a third consider identity systems among those risks; yet 67% of utility infrastructure attacks in the UK and US definitively compromised identity systems—specifically Active Directory (AD), Entra ID, and Okta.[14]

Cyberattack campaigns like NotPetya show clearly why identity security should be on every operational risk manager's and CISO's agendas. More recently, Volt Typhoon, a nation-state–affiliated group, has targeted a number of critical sectors, including, famously, telecommunications, but also government and energy.[15] The group makes extensive use of exposure in AD by extracting the NTDS.dit database for full domain compromise—just one method in an extensive catalogue of identity-focused attack techniques.[16]

AD's role in cyberattacks means its security is paramount for business resilience for multiple reasons.

- Identity systems are Tier 0 assets that directly manage access to the users, groups, applications, and resources that support an organisation's essential and important services. If AD is down, everything is down.
- Identity, together with data security, forms the new perimeter of cyber resilience. AD provides foundational value in an organisation's defence-in-depth and Zero Trust strategies for cyber resilience.
- Because of its importance to defenders and the significant complexity and age of on-premises identity systems, threat actors are increasing their attention on compromising an organisation's enterprise identity system. Compromising AD lets attackers gain initial access, mask their presence in the environment, elevate privileges, and initiate endless shady activities.

Additionally, for a big enterprise, restoring AD is a significant undertaking. The NotPetya breach saw Maersk spend more than a week to restore its AD, and it almost wasn't possible at all because both the company's primary and backup systems were crippled.[17]

Unfortunately, the process to restore AD has changed little since 2017. The official Microsoft guidance requires 28 steps—covered in a 150-page document—to restore a single AD forest. For many organisations, recovery is further complicated because of other services (such as DHCP and DNS) running on AD, hybrid cloud and on-premises integrations, and the sheer number of changes that occur daily in a large AD forest. In addition, depending on backup frequency, AD backups may also be compromised, increasing the challenge of restoring AD to a known-secure state.[18]

The confluence of these factors compels OESs to devote particular attention to identity systems when implementing the RIIO-2 Cyber Resilience Guidelines.

---

14 The State of Critical Infrastructure Resilience | Semperis Guides

15 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA

16 NTDS.DIT Extraction Explained | Semperis Identity Attack Catalog

17 Maersk CISO Says NotPeyta Devastated Several Unnamed US firms

18 Top Manual AD Forest Recovery Pitfalls | Semperis Guides

RIIO-2 controls for identity resilience

Due to the scale of the RIIO-2 guidelines, this paper does not attempt to detail all required controls. Instead, the following sections outline the controls that involve securing your identity system. The analysis bundles controls in logical groupings as far as possible and in a meaningful way.

Risk, governance, and threats

To conform with RIIO-2 requirements, you must have good identification and ownership of assets, risks, and vulnerabilities.

Area	Section	Description summary
Board direction, roles and responsibilities, and decision-making	A1.a-c	• Provide strong board-level ownership of cyber risk combined with a comprehensive management system. • Clearly define and communicate roles and responsibilities pertaining to cyber risk in information communications technology (ICT) and operational technology (OT) and ensure positions are filled by people with the right level of knowledge and experience. • Establish decision-making and risk decisions as part of the management framework.
Risk management and assurance	A2.a-b	• Identify and manage risks as they pertain to services, assets, and ICT. • Identify and manage vulnerabilities of your network and services.
Asset management	A3.a	• Create and manage a register of all assets. Assign ownership and manage all asset life cycles.
Supply chain risk	A4.a	• Ensure you understand any risks stemming from or managed by third-party suppliers.

All cyber resilience programmes require certain foundational aspects. You need to set the tone from the top through executive or board-level engagement and drive. Risk management and assurance are also required but will only be effective if based on a strong understanding of the protected assets and their risks to the organisation.

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Establish key information about the identity system and the Tier 0 assets it manages. Understand the risks the identity system is subject to and how identity risks can negatively impact the resilience of other essential or important services should a breach occur.
2. Be clear about ownership of risk pertaining to identity systems, including services in both the ICT space and the OT domain.
3. Establish a top-down view of vulnerabilities related to the identity system, including where vulnerabilities may arise from a supplier relationship or where relevant controls and mitigations rely on such suppliers.
4. Establish active assurance measures for your identity controls, including scanning for misconfigurations and vulnerabilities as well as active red-teaming and penetration testing of your identity system.

Identity verification, authentication, and authorisation

The identity system is vital to the underlying cybersecurity of all enterprises. In utilities, where highly motivated and skilled nation-state actors actively seek to compromise the identity system, specific and proactive controls are even more important.

Area	Section	Description summary
Identity verification, authentication, and authorisation	B2.a	• Require authentication for all users and services. • Restrict logical access on a need-to-know basis. • Require both multifactor authentication and remote access controls.
Privileged user management	B2.c	• Establish additional verification and layers of authentication for privileged users. • Establish joiner, mover, and leaver processes, role-based access, and access reviews and monitoring.
Identity and access management	B2.d	• Combine joiner, mover, and leaver processes with user access reviews. • Regularly review access monitoring and logs.

Microsoft sees 600 million attacks daily against its cloud identity system, Entra ID. Both AD and Entra ID receive high volumes of targeted and opportunistic attacks, making your organisation's identity security vital to your cyber resilience.[19]

19 Microsoft Digital Defense Report 2024

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Establish a privileged access management programme, enhancing security for privileged access users and including the identification and governance of service accounts.
2. Establish appropriate logging for security monitoring that continuously monitors and captures changes in AD and Entra ID.
3. Ensure identity system change detection, logging, and reporting are in place for threat hunting.
4. Invest in automation of identification, scanning, and remediation capabilities for the identity infrastructure.

Secure by design and secure configuration

To ensure a truly resilient operation, establish security principles early and integrate them into your identity systems.

Area	Section	Description summary
Secure by design	B4.a	• Establish the right level of experience and training for the team that's designing and implementing your security controls. • Establish network segmentation, resilience, and attack mitigations, factoring in access control and identity for effective incident response and system restoration.
Secure configuration	B4.b	• Securely configure all network and information systems, including asset hardening, access control, and remote access. • Monitor and proactively manage assets to maintain secure configuration. • Regularly review security configuration across assets and establish change management processes, especially in regard to monitoring changes to account permissions.

Identity system configuration is complex, and the velocity and volume of changes can enable the introduction of malicious, unauthorised, or problematic settings, which may go undetected for long periods. Cyber resilience requires transparency from the organisation to identify and control such changes.

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Establish a baseline of security settings and configurations across major system capabilities.
2. Set up configuration change logging and establish a programme to monitor risky changes.
3. Confirm toxic settings and enable immediate remediation.
4. Automate validation of configuration controls against policy, and automate remediation of high-risk configurations and changes that may indicate compromise.
5. Scan and manage security configurations across services.

Vulnerability management

Vulnerabilities have become a major vector for threat actors to access enterprise environments, establish persistence, and escalate privileges.

Area	Section	Description summary
Vulnerability identification and management	B4.d	• Establish a programme to identify, assess, track, prioritise, and remediate vulnerabilities in your ICT systems that support essential services. • Regularly perform vulnerability assessments, preferably in a nonproduction or laboratory environment.

Application and operating system vulnerabilities keep increasing, with the NCC Group reporting a jump from just under 30,000 in 2023 to more than 40,000 in 2024. Only a small number of these are actively exploited, but certain areas like perimeter devices constitute key vectors of initial access for malicious actors.[20] As an example, Emsisoft reported that nearly 3,000 organisations were breached with one zero-day vulnerability in the file transfer tool MOVEit.[21]

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Establish a programme that uses automated tools to scan for and identify vulnerabilities and misconfigurations in your identity infrastructure.
2. Establish a project to remediate vulnerabilities based on priority, starting with the most critical items requiring the least effort and moving towards the least critical items requiring the most effort.
3. Include in your vulnerability programme reporting from third parties, including vendors, open-source data sources, and your regulators.
4. Overlay third-party information on your asset management capability with a focus on critical services and internetfacing capabilities.
5. Build an operating system and application patching process that focuses on the remediation of identified critical services and their high-impact vulnerabilities.

20 Cyber Threat Monitor Report 2024 | NCC Group

21 Clop ransomware claims responsibility for Cleo data theft attacks

Resilience and backups

All your essential ICT services need to be recoverable in case the service is subject to a critical error or successful attack.

Area	Section	Description summary
Preparation and design for resilience	B5.a-b	• Establish a robust recovery plan that considers relevant dependencies, supporting technologies, and dependent systems. • Ensure compromised states can be contained in an outage through a defence-in-depth approach, segmentation, and logical access control.
Backups	B5.c	• Ensure you have accessible, secure, and current backups of data and information that you need to recover. • Regularly test backups and restore procedures.

Avoiding the spread of destructive states in your identity environment is critical for operational resilience. This includes planning for recovery and restore and eliminating points of failure such as identity systems, notably AD. Working, trusted backups are key for avoiding risks.

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Define a plan for identity infrastructure recovery and restore.
2. Confirm measures to ensure you can achieve a known clean-state recovery—meeting your required recovery point objective (RPO) within your recovery time objective (RTO).
3. Implement ongoing testing and assurance of your identity security posture by regularly performing cyber incident response and recovery exercises to ensure your backups are resilient.
4. Establish a nonproduction test environment and perform frequent restore testing, integrating a lessons-learned approach to update recovery playbooks.
5. Ensure ICT disaster recovery activities are implemented and integrated with broader business continuity and crisis management plans and exercises.

Proactive monitoring

Cyber threats are never fully preventable. Enterprises must rely on automated monitoring, detection, and alerts to stop an attack.

Area	Section	Description summary
Monitoring, securing logs, and managing alerts	C1.a-c	• To detect attacks, create a monitoring strategy with a clear scope and validated security monitoring use cases. • Monitor key areas, such as access to network and privileged user accounts. • Secure logs and ensure they are accessible to authorised users as read-only. • Review, prioritise, investigate, and respond to security alerts relating to networks and systems supporting essential services.

Monitoring is key to combating threats to identity systems like AD. When thousands of users operate across your ICT systems, alerting and logging are essential for detecting unusual behaviours and malicious actions.

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Configure and manage security monitoring on your identity infrastructure.
2. Ensure logging is enabled and a trained team is automatically alerted to suspicious and potentially harmful events.
3. Establish a playbook for incident response, including designating staff members who are responsible for managing incidents and laying out the details of their roles during a critical incident.
4. Consider identity-focused analytics tools for a richer data set.
5. Ensure logs cannot be tampered with or deleted.

Attack detection and response

Whereas the fundamental controls for monitoring involve monitoring base events and analysing them for threats, it's increasingly important to implement advanced threat intelligence and identity- and access management–specific tools to detect unusual or abnormal behaviours.

Area	Section	Description summary
Identifying security incidents, monitoring staff coverage and tools, and monitoring skills	C1.d-e	• Leverage advanced threat intelligence from vetted sources to ensure accurate, contextually appropriate indicators of exposure (IOEs) and indicators of compromise (IOCs) in your identity system. • Determine staff and tool requirements needed to meet monitoring needs across systems and shifts. • Ensure monitoring staff have appropriate skills and investigative competence to perform their assigned roles—and the means to independently execute their required tasks.
Understanding system abnormalities for attack detection and discovery	C2.a-b	• Develop baseline understanding of normal user and system behaviours and define abnormal behaviours. • Establish enhanced monitoring as needed on essential systems, such as failed log-on attempts or access outside of business hours. • Identify and investigate anomalies and employ threat-hunting techniques to detect potential malicious activity. • Be ready to report (meaningfully) on a breach within 72 hours of the discovery of an attack.

Establish capability-focused monitoring capabilities for the identity systems and empower security teams to employ contextually relevant responses to threats to your organisation's identity resilience.

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Map a baseline of normal behaviours for your identity system.
2. Monitor for IOEs and IOCs.
3. Monitor for outliers and abnormal behaviours.
4. Define and integrate matching playbooks for the security operations centre (SOC).
5. Ensure the SOC's processes integrate with broader business continuity management and crisis management procedures.

Incident response planning, testing, reporting, and improvement

When it comes to identity systems, the devil is in the details. Your response plan needs to be highly optimised to enable you to respond well to a crisis in a complex service like AD.

Area	Section	Description summary
Response plan, response and recovery capability, testing and exercising	D1.a -c	• Document a comprehensive incident response plan, ensuring it covers the entire incident management life cycle and includes system component restoration activities and sequence. Consider and include known attack patterns to anticipate as many continencies as possible. • Ensure you have the capability to execute your response plan: the people, processes, information, communications, and technology support required to fully restore operations. • Execute comprehensive incident response exercises, including disaster recovery tests and functional tabletop exercises that prepare teams for real-world scenarios.
Analysing incident root cause and driving improvements	D2.a-b	• Establish policies and processes for forensic analysis of cyber incidents, ensuring investigative teams have full data access and details to compile detailed reports and recommendations. • Document learning from exercises and forensic investigations and update response plans accordingly.

The RII0-2 guidelines discuss the requirements for response and recovery, focusing on the assignment of roles and responsibilities for all staff responding to a cyber incident, documentation of system component restore activities, validation of recovery capabilities, and continuous improvement and adaptation of incident response plans.

KEY STEPS FOR A CYBER-RESILIENT IDENTITY SYSTEM

1. Ensure you have an up-to-date, comprehensive, documented incident response plan that includes all relevant information, contacts, and communication capabilities.
2. Consider establishing and maintaining your incident response plan and related resources in a centralized system outside of your production systems so it can be used when your systems are not functioning.
3. Validate and test your response and restore plans against the finer details of the service, its dependencies, and the steps required for restoring essential service.
4. Build increasingly comprehensive scenarios for attack patterns and dependencies.
5. Report and review lessons learned from testing exercises to enable continuous plan improvement.

Tool specialisation

Compliance with the RIIO-2 Cyber Resilience Guidelines requires capabilities that are difficult to execute without detailed knowledge of identity systems and their enterprise-specific configurations—as well as significant automation.

Your identity system is foundational for many, if not most, of your essential services. Your teams are likely to be fully occupied with day-to-day maintenance and operations, leaving limited time to delve deep into the details of full AD forest restore and hardening.

In our view, achieving these resilience capabilities requires application of specialised identity-focused tools in most medium to large enterprises—especially those with extensive OT environments like utilities.

How can Semperis help?

Semperis offers products that specifically address the requirements analysed above. The following section outlines these capabilities against the requirements of RIIO-2.

Challenge	How can Semperis help	Solution
Risk management To comply with the RIIO-2 Cyber Resilience Guidelines, it's vital that those responsible for ICT resilience have a strong understanding of the true risks associated with your identity system.	• Visualise identity security posture. • Identify risks to cyber resilience and compliance. • Map dependencies to enable restore of AD. • Ensure a resilient identity system.	• Security Assessment services provide a clear view of identity and operational security posture and guidance for addressing security exposures at the strategic, operational, and tactical levels. • Purple Knight provides point-in-time security assessment of AD. • Active Directory Forest Recovery (ADFR) maps and automates AD forest recovery, including for relevant dependencies. • Directory Services Protector (DSP) enables continuous threat and vulnerability detection and automatic rollback of malicious changes. • DSP provides change tracking by capturing every change made in AD to identify malicious changes.

Challenge	How can Semperis help	Solution
Identity verification, authentication, and authorisation To achieve privileged access management and identity access management objectives, you must be able to rely on the integrity and resilience of AD and Entra ID.	• Identify and eradicate IOEs. • Reveal identity-based threats across hybrid identity environments. • Rapidly restore AD during outages to enable teams to continue working securely. • Reveal attack paths that can be used to gain administrative access.	• DSP enables continuous monitoring of AD and Entra ID security posture and automated rollback of risky configurations. • Lightning Identity Runtime Protection uses machine learning to perform attack pattern detection by capturing, analysing, and correlating authentication activities with Semperis' identity threat intelligence to signal malicious behavior. • ADFR provides up to 90% faster AD restore. • Forest Druid (no-cost community tool) discovers and automatically maps attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit.
Security design, configuration, and vulnerability management Cyber resilience depends on your ability to identify, prioritise, and mitigate vulnerabilities and IOEs in alignment with your key security objectives.	• Provide both automated and expert-led researchbased views of software vulnerabilities and misconfigurations. • Create point-in-time vulnerability and misconfiguration snapshots. • Enable continuous, automated vulnerability and misconfiguration scanning.	• Lightning Intelligence provides clear security posture insights across hybrid AD and Entra ID environments in an easily deployed SaaS solution to simplify security posture assessments. • Purple Knight enables teams to find and fix existing security vulnerabilities. • DSP provides continuous threat and vulnerability detection.
Resilience and backup To align with RII0-2 guidance, you need to be able to restore your identity systems rapidly and have tests to validate that you can do so successfully.	• Proactively detect or avoid a security breach of your identity infrastructure and dependent ICT services. • Provide a clean-state restore with validated recovery point objectives and recovery time objectives. • Enable well-maintained ICT services.	• ADFR automates the complicated AD recovery process and recovers AD up to 90% faster than manual recovery. • ADFR accelerates post-breach forensics to identify persistence and recover AD to a trusted state. • ADFR ensures AD backup security by leveraging automated cloud backups. • Disaster Recovery for Entra ID recovers Entra ID objects and multitenant service principals.

Challenge	How can Semperis help	Solution
Monitoring, attack detection, and response Your identity infrastructure is a rich source of vulnerabilities and misconfiguration, requiring skill and dedication for meaningful detection.	• Monitor AD and Entra ID to detect attacks and accurately report on incidents. • Comprehensively control the constantly changing AD environment with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities.	• DSP enables continuous assessment of AD IOEs, automated rollback of malicious changes, and AD machine learning–based attack detection. • DSP provides comprehensive logging and highly specialised AD and Entra ID threat analysis, enabling up-to-date, industry-leading insights and enrichment of SOC visibility through SIEM integration. • Semperis products are enhanced by deep research from the identity security-focused threat team.
Incident response planning and testing When a cyber crisis occurs, you need a comprehensive plan of action and the confidence that you'll be capable of executing it effectively and quickly.	• Centralize and streamline cyber crisis planning and incident response. • Ensure incident response capabilities can be executed, even when production systems are down. • Ensure crisis preparedness through tabletop exercises, rigorous incident response plan testing, and continuous improvement.	• Ready1 empowers IR teams by ensuring clear roles and responsibilities. • Ready1 centralizes and unifies all aspects of cyber crisis planning and incident response, ensuring seamless crisis response through preparation, collaboration, and enterprise-wide communications. • Ready1 operationalizes 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.

Conclusion

The critical nature of utility services sets these organisations apart from many other industries. If a downstream gas and electricity operator is compromised, the potential risks to public health and safety can put the entire nation at risk. Our experts note that resilience to cyberattacks that threaten operations should be the top priority for every organisation involved in critical infrastructure.

RIIO-2 provides guidance to electricity and gas utilities in the UK subject to cyber resilience regulations like NIS. Identity security and resilience are key aspects of compliance to this standard. We recommend organisations follow these seven steps:

1. Establish risk management and ownership for your identity system.
2. Establish a least-privilege model for identity management and ensure you have preventative and detective controls for prominent identity and access threats.
3. Establish comprehensive and automated exposure, threat, and vulnerability monitoring and integrate these capabilities into your SOC.
4. Mitigate AD vulnerabilities to reduce the identity attack surface.
5. Build a tested incident response capability for your ICT services, including your identity system, to enable rapid incident response, reporting, and forensic capabilities.
6. Develop an automated and tested recovery process to enable rapid, clean identity system restoration in case of a destructive incident.
7. Establish a project of continuous improvement that includes best practices from leading experts in the cybersecurity industry.

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