ISACA®

# Resilience and Security in Critical Sectors: Navigating NIS2 and DORA Requirements

Risk

# CONTENTS

4 Introduction
5 Scope
6 Risk Management, Business Continuity, and Disaster Recovery
8 Information and Cybersecurity
8 / Audits
9 Incident Reporting
11 Testing Obligations
12 Third-Party Service Provider Requirements
12 Governance and Accountability
13 Information Sharing
14 Noncompliance
14 Conclusion
16 Acknowledgments

# ABSTRACT

Given the significant consequences resulting from incidents, some jurisdictions have enacted laws and regulations to address resilience and incident response. The interconnectedness of European member states led to a need to harmonize incident response requirements and reporting across the European Union. The Digital Operational Resilience Act (DORA) and the Network and Information Systems (NIS2) Directive provide guidance to enterprises in certain key sectors. They cover areas such as risk management, information security, and cybersecurity, with new requirements on incident reporting, plans and testing, third-party and supply chain security evaluation, cross-border collaboration, information sharing, and periodic testing.

This white paper compares DORA and NIS2 across several topic areas. It includes the consequences of noncompliance, incident reporting timelines, and the role of third-party service requirements. It is important to note that enterprises located outside the European Union may be subject to NIS2 and/or DORA, so familiarity with their requirements is valuable for enterprises worldwide.

# Introduction

Many essential, important, and critical services, such as energy, water, finance, and entities providing domain name registration services leverage information and communication technology (ICT). The resilience of this technology is essential to ensure uninterrupted provision of essential services. Outages and cybersecurity incidents in these sectors can lead to significant health, safety, financial, legal, reputational, and operational harm for affected individuals and enterprises.

To address the continuity of vital services, some jurisdictions have enacted directives and regulations applicable to certain entities. In the European Union, two key pieces of guidance in this area are the Digital Operational Resilience Act (DORA) and the Network and Information Systems (NIS2) Directive.

DORA applies to the financial sector, while NIS2 is not limited to the financial sector and is aimed at essential and important entities. Enterprises may be subject to DORA, NIS2, neither, or both. Because it is a regulation, DORA is more prescriptive than NIS2. It outlines specific obligations for enterprises. In contrast, NIS2 is a directive, which means it provides goals that EU countries must achieve, but it is the responsibility of EU member states to create laws that help achieve these goals.[1] Note that DORA also has some supplementary EU Commission-delegated regulatory technical standards (RTS) and supporting guidance, and these are legally binding.[2] NIS2 has one implementation regulation relating to technical and methodological requirements.[3]

NIS2 replaced the original NIS1 directive. NIS2 has a broader scope than its predecessor, incorporating public electronic communications services, digital services, critical product manufacturers, postal services, and public administration.[4]

Another important European directive, the Payment Services Directive (PSD), is aimed at electronic payments. While this directive has an impact on many enterprises across the European Union and enterprises could be subject to PSD in addition to NIS2 and/or DORA, the latest version, PSD3, is currently in draft form[5] and is out of scope for this white paper.

NIS2 and DORA compliance can support resilience, continuity, and risk management activities. Enterprises covered by NIS2 and DORA should learn their obligations to ensure resiliency, maintain customer access to their services, and avoid potential penalties for noncompliance.

[1] European Union, "Types of legislation," https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

[2] Official Journal of the European Union, RTS 2024/1772, RTS 2024/1773, RTS 2024/1774, RTS 2025/295, RTS 2025/301, ITS 2024/2956, and ITS 2025/302, https://european-union.europa.eu/index_en

[3] Official Journal of the European Union, "Commission Implementing Regulation (EU) 2024/2690," 17 October 2024, https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

[4] European Commission, "NIS2 Directive: new rules on cybersecurity of network and information systems," https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[5] European Union, "Modernising payment services and opening financial services data: new opportunities for consumers and businesses," 27 June 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

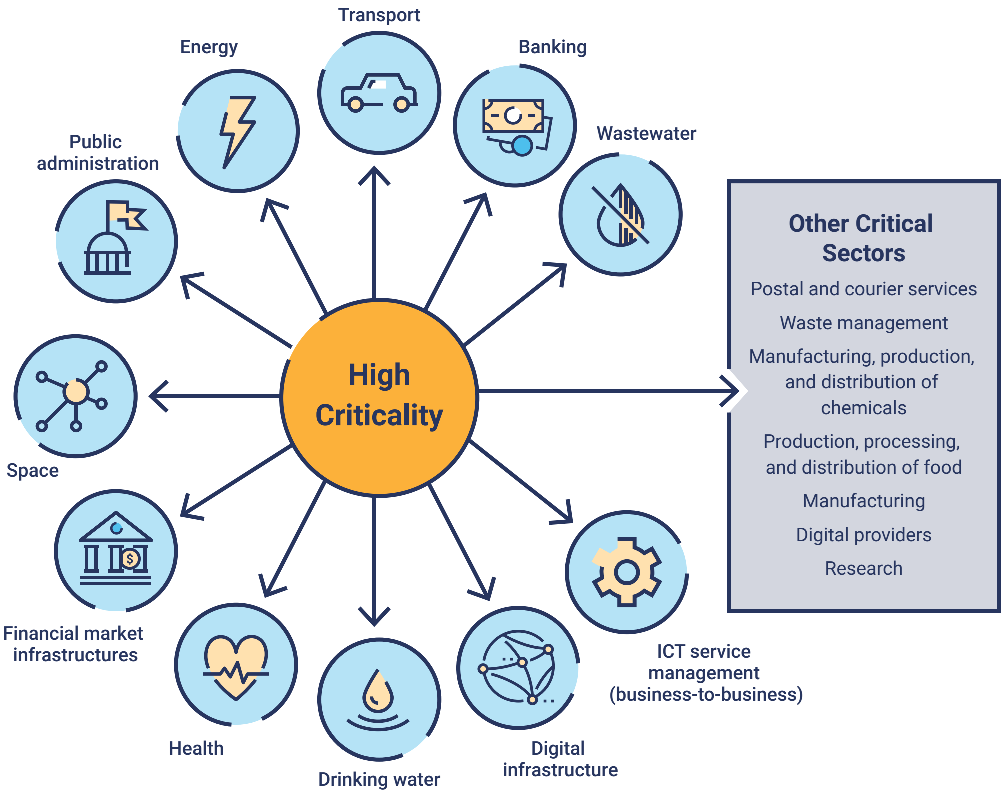
# Scope

NIS2 and DORA were enacted in the European Union, but they may have impacts for enterprises around the world. This is especially true for third parties working with entities in the European Union that are subject to NIS2 or DORA.

NIS2, which impacts enterprises that provide their services or conduct activities in the European Union, may apply to some enterprises in the financial sector, but its scope is larger than DORA's. NIS2 applies to entities that are considered essential and important.[6] Sector and enterprise size determine whether an entity is considered essential or important, but these are not the only factors in the decision. Other factors include if an entity is the sole provider of a service or if a disruption to the entity's service could have a significant impact on public order, public security, or public health, among other factors.

**Figure 1** shows which sectors are considered high criticality and which are critical according to the NIS2 directive.[7]

FIGURE 1: NIS2 Sectors


High Criticality
Transport
Energy
Banking
Wastewater
Public administration
Space
Financial market infrastructures
Health
Drinking water
Digital infrastructure
ICT service management (business-to-business)
Other Critical Sectors
Postal and courier services
Waste management
Manufacturing, production, and distribution of chemicals
Production, processing, and distribution of food
Manufacturing
Digital providers
Research

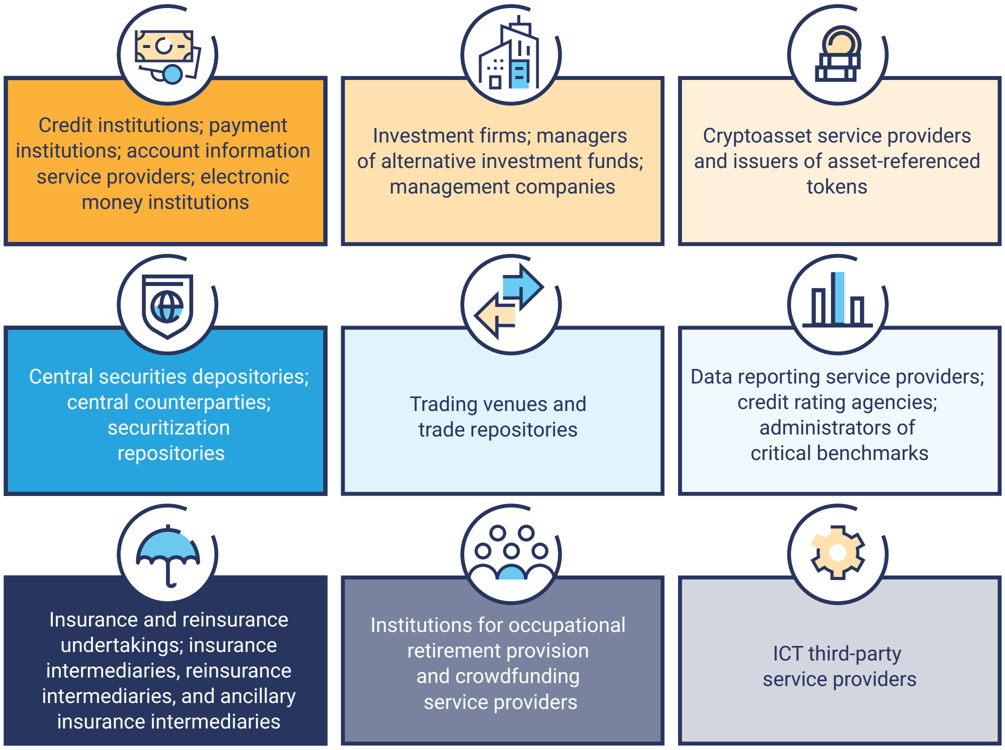
[6] Essential entities are typically large enterprises that operate in one of the 11 critical sectors: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management (business-to-business), public administration, and space. Important entities are all other organizations that are not categorized as essential entities but still fall under the general criteria of location, size, and industry.

[7] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

DORA applies to entities in the financial sector, including credit institutions, payment institutions, and investment firms.[8]

**Figure 2** shows the financial institutions in the scope of DORA. Note that some micro and small- or medium-sized enterprises are not subject to all aspects of DORA or may have different obligations.[9]

FIGURE 2: DORA Scope



Credit institutions; payment institutions; account information service providers; electronic money institutions

Investment firms; managers of alternative investment funds; management companies

Cryptoasset service providers and issuers of asset-referenced tokens

Central securities depositories; central counterparties; securitization repositories

Trading venues and trade repositories

Data reporting service providers; credit rating agencies; administrators of critical benchmarks

Insurance and reinsurance undertakings; insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries

Institutions for occupational retirement provision and crowdfunding service providers

ICT third-party service providers

# Risk Management, Business Continuity, and Disaster Recovery

To promote a harmonized approach to risk management across the European Union, NIS2 and DORA have certain requirements related to risk management. NIS2 calls for putting adequate measures in place to address risk to network and information system security. This includes developing policies related to risk analysis and assessing the efficacy of cybersecurity risk management measures.[10]

[8] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 2, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[9] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[10] European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 21, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

In contrast, DORA has several specific requirements related to establishing and maintaining an ICT risk management framework. This framework must, at a minimum, include strategies, policies, procedures, ICT protocols, and tools needed to protect information and ICT assets. The framework must ensure ICT management, control, and internal audit functions are adequately segregated, and the ICT risk framework must be:[11]

- Documented
- Reviewed at least annually[12] and after major ICT-related incidents
- Subject to internal audit

The ICT risk management framework must incorporate a digital operational resilience strategy that establishes how the framework will be implemented. This strategy must include:[13]

- An explanation of how the framework can support the enterprise's business strategy and objectives
- The ICT risk tolerance level
- Information security objectives, including key performance indicators (KPIs) and key risk indicators (KRIs)
- The ICT reference architecture
- The methods in place to detect, prevent, and protect in the event of an ICT-related incident
- The current state of digital operational resilience
- Digital operational resilience testing
- A strategy for communicating and disclosing ICT-related incidents

Employee training is a vital part of risk management, as humans are often the weakest security link. Tailoring security-related training based on roles and responsibilities is vital to ensure all staff understand how they can support enterprise security. DORA requires organizations to develop ICT security awareness programs and digital operational resilience training as part of the employee training program. All employees and senior management must complete this training, which should contain content appropriate to their roles.[14] NIS2 also requires essential and important entities to offer training related to cybersecurity risk management.[15]

**Tailoring security-related training based on roles and responsibilities is vital to ensure all staff understand how they can support enterprise security.**

DORA calls for continuous monitoring of ICT systems and tools in an effort to minimize ICT risk.[16] It also requires having mechanisms to detect anomalies and ICT-related incidents and that these mechanisms are tested regularly.[17] Business continuity is a key element of operational resilience, and DORA has requirements around response and recovery. ICT business continuity plans and procedures must:[18]

- Provide for the continuity of critical or important functions
- Respond to ICT-related incidents in a timely manner to limit damage and facilitate resumption of activities and recovery
- Activate containment measures, processes, and technologies
- Estimate initial impacts, damages, and losses
- Communicate and conduct crisis management actions

[11] Official Journal of the European Union, "Regulation (Eu) 2022/255 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 6, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[12] Microenterprises only need to review this framework periodically.

[13] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 6, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[14] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 13, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[15] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 20, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[16] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 9, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[17] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 10, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[18] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 11, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Financial entities subject to DORA must establish an ICT business continuity policy and an associated ICT disaster recovery plan. For enterprises that are not microenterprises, this plan is subject to independent audit reviews. To validate ICT efforts, the ICT business continuity policy and ICT disaster recovery plan must be tested.

**Financial entities subject to DORA must establish an ICT business continuity policy and an associated ICT disaster recovery plan.**

DORA also emphasizes the importance of backups, which are critical in the event of an incident. DORA requires financial entities to create a backup policy. This policy should include which data is subject to being backed up as well as the minimum frequency of the backup. This frequency should be determined based on the criticality of the information or the sensitivity of the data. Financial entities must also develop recovery methods.

# Information and Cybersecurity

NIS2 and DORA both contain provisions about the security of network and information systems. Security is vital to ensuring customers can have uninterrupted access to service and have their information protected. To that end, NIS2 and DORA both have security-related obligations.

NIS2 requires enterprises to address security in a way that can prevent or minimize the impact of incidents. Per NIS2, enterprises must have:[19]

- Risk analysis and information system security policies
- Incident handling procedures
- Business continuity measures
- Supply chain security
- Security in network and system acquisition, development, and maintenance
- Assessments of cybersecurity risk management measures
- Cybersecurity training and cyberhygiene
- Encryption and cryptography policies and procedures
- Human resources security
- Multifactor authentication (MFA) or continuous authentication

DORA has multiple requirements related to the security of ICT systems and tools. These systems and tools must be continuously monitored, which can help identify potential service interruptions. Financial entities must define alert thresholds and criteria that would trigger ICT incident detection and response processes. Multiple layers of control must be enabled.

DORA requires that financial entities develop policies and protocols for strong authentication mechanisms. At a minimum, they must annually review the adequacy of classification of information assets as well as any relevant documentation.

## Audits

Audits can help ensure that enacted measures achieve desired outcomes. NIS2 and DORA address audits pertaining to security and third parties. Enterprises that are considered essential entities under NIS2 are subject to regular, targeted, and *ad hoc* security audits. These audits may be conducted by an independent body or competent authority, and results must be made available to the competent authority.[20] Important entities are also subject

[19] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 21, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[20] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 32, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

to targeted security audits by an independent body or competent authority, with results being made available to the competent authority.[21]

DORA allows financial entities and competent authorities to audit ICT third-party service providers.[22] This is critical, as third-party issues could impact the financial entity, which, in turn, impacts their customers. Additionally, the ICT risk management framework is subject to internal audit. There must be a formal follow-up process to act upon any critical ICT audit findings. DORA requires that audit functions have the appropriate knowledge, skills, and expertise in ICT risk and that they are independent. ICT audit frequency and focus will vary based on the enterprise's ICT risk. Note that microenterprises are exempt from many of these internal audit requirements.

**DORA requires that audit functions have the appropriate knowledge, skills, and expertise in ICT risk and that they are independent.**

# Incident Reporting

Reporting an incident to the appropriate authorities and affected people is a core component of operational resilience and supports transparency. Authorities may need to act to protect people and ensure vital services can still be provided, and it is crucial for them to know about incidents in the event of an adversarial state-sponsored attack. Incident details may also help others in the same industry prepare for or address these incidents should they experience them.

NIS2 and DORA both have requirements around incident reporting as well as specific time frames by which certain information must be provided to designated authorities.

The requirements in this directive and regulation help harmonize reporting obligations across the European Union, which could vary considerably from member state to member state.

NIS1 required member states to create one or more computer security incident response teams (CSIRTs). CSIRTs should participate in deploying secure information-sharing tools and, as appropriate, share relevant information with communities of essential and important entities.[23] CSIRTs play a vital role in incident reporting.

If a significant incident occurs, enterprises subject to NIS2 must notify the CSIRT or competent authority of the incident. NIS2 defines a significant incident as one that causes or could cause severe operational disruption of services or financial loss and has affected or could affect natural or legal persons by causing considerable damage (material or nonmaterial).[24]

**Figure 3** contains the significant incident reporting timeline under NIS2.

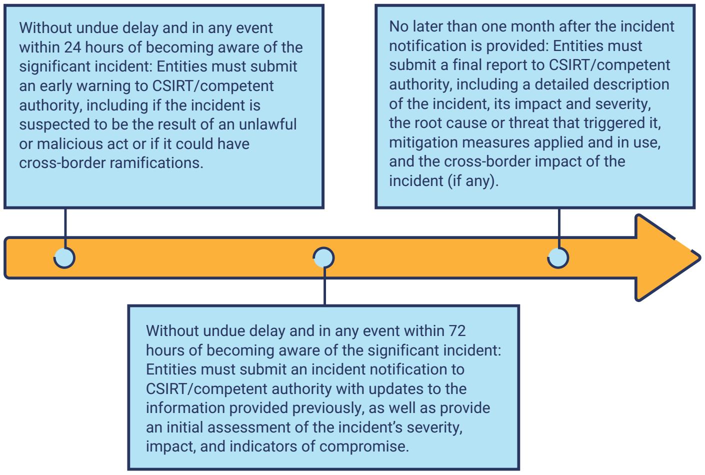
[21] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 33, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[22] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 28, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[23] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 10, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[24] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 23, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

**FIGURE 3:** NIS2 Significant Incident Timeline



Without undue delay and in any event within 24 hours of becoming aware of the significant incident: Entities must submit an early warning to CSIRT/competent authority, including if the incident is suspected to be the result of an unlawful or malicious act or if it could have cross-border ramifications.

Without undue delay and in any event within 72 hours of becoming aware of the significant incident: Entities must submit an incident notification to CSIRT/competent authority with updates to the information provided previously, as well as provide an initial assessment of the incident's severity, impact, and indicators of compromise.

No later than one month after the incident notification is provided: Entities must submit a final report to CSIRT/competent authority, including a detailed description of the incident, its impact and severity, the root cause or threat that triggered it, mitigation measures applied and in use, and the cross-border impact of the incident (if any).

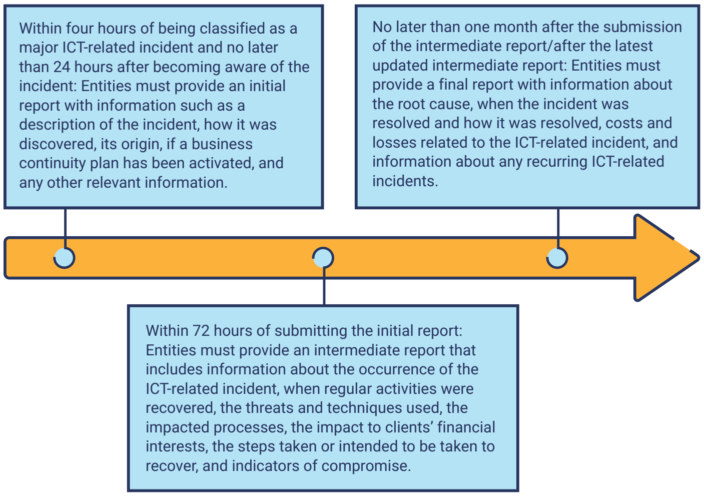
** Entities must provide intermediate reports/status updates if requested by CSIRT/competent authority.*

*** If the incident is ongoing when the final report is due, entities must provide a progress report, and the final report is due within one month of handling the incident.*

DORA defines major ICT-related incidents as those with "a high adverse impact on the network and information systems that support critical or important functions of the financial entity."[25] Financial entities must notify the relevant competent authority of any major ICT-related incidents. To promote resilience across the finance sector, financial entities may share significant cyberthreats with the relevant competent authority.[26]

**Figure 4** contains a DORA incident notification timeline for major ICT-related incidents.[27]

**FIGURE 4:** DORA Notification Timeline



Within four hours of being classified as a major ICT-related incident and no later than 24 hours after becoming aware of the incident: Entities must provide an initial report with information such as a description of the incident, how it was discovered, its origin, if a business continuity plan has been activated, and any other relevant information.

Within 72 hours of submitting the initial report: Entities must provide an intermediate report that includes information about the occurrence of the ICT-related incident, when regular activities were recovered, the threats and techniques used, the impacted processes, the impact to clients' financial interests, the steps taken or intended to be taken to recover, and indicators of compromise.

No later than one month after the submission of the intermediate report/after the latest updated intermediate report: Entities must provide a final report with information about the root cause, when the incident was resolved and how it was resolved, costs and losses related to the ICT-related incident, and information about any recurring ICT-related incidents.

[25] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 3, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[26] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 19, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[27] European Commission, "Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats," 23 October 2024, https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng

A one-day time frame to notify authorities about significant incidents may be challenging for some enterprises. Comprehensive and regularly updated incident response plans are critical for compliance and resilience. Incident response plans must account for reporting obligations, and everyone involved with incident response should be aware of the content to report and reporting deadlines. Incident response testing and simulations can help enterprises identify areas for improvement and gauge their response capabilities.

# Testing Obligations

Because proactive testing can help enterprises identify weaknesses and address them before they are exploited and result in system outages or harm to customers, some regulations include testing requirements. NIS2 does not specify testing measures that should be put in place. In contrast, DORA requires financial entities to conduct threat-led penetration testing (TLPT) every three years, at a minimum, and the scope of this testing may include ICT third-party service providers. This TLPT must cover critical or important functions and must be performed on live production systems.[28]

**NIS2 does not specify testing measures that should be put in place. In contrast, DORA requires financial entities to conduct threat-led penetration testing (TLPT) every three years, at a minimum, and the scope of this testing may include ICT third-party service providers.**

Testing should incorporate criticality, business continuity, disaster recovery, and failover considerations. While three years is the minimum frequency for TLPT per DORA, conducting this testing more frequently can ensure alignment with industry best practice and allow enterprises to have more accurate and up-to-date insights on potential areas for improvement. It is recommended that, given the potential risk associated with testing on live production systems, the scope of such testing be carefully defined and managed to minimize any impact on ongoing operations.

In addition to TLPT, DORA also requires financial entities to test their operational resilience. Pen testing and operational resilience go hand in hand, and pen testing can provide valuable insights into operational resilience. Per DORA, operational testing must be risk-based and led by independent internal or external parties.[29] Testing may include:[30]

- Vulnerability assessments and scans
- Open-source analyses
- Gap analyses
- Reviews of physical security
- Performance testing
- Compatibility testing

NIS2 does not require operational resilience testing, but this testing can help enterprises evaluate how they may respond to an incident, so it is a worthwhile activity even if it is not mandatory.

[28] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 26, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[29] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 24, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[30] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 25, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

# Third-Party Service Provider Requirements

Most enterprises rely on third-party products and services, and third-party outages can have widespread consequences. Contracts with third parties can help address resilience and clearly define risk-related obligations, and enterprises should ensure that service provider requirements are clearly spelled out in contracts and service-level agreements (SLAs).

NIS2 does not outline third-party service provider contractual requirements, but DORA requires that contracts with ICT service providers address risk. Specifically, DORA requires that financial entities have:

- Contractual provisions outlining how the ICT third-party service provider promotes accessibility, availability, integrity, security, and personal data protection
- A method to access, recover, and return data if the service provider discontinues operations
- Assistance in the event of ICT-related incidents related to the services provided

DORA requires that financial entities develop and regularly review their ICT third-party risk strategy, which must include a policy about the use of ICT services supporting critical or important functions provided by ICT third-party service providers.[31] Understanding which services support critical or important functions is imperative to resilience.

NIS2 does not provide enterprises with ICT third-party risk requirements, but addressing third-party risk can support an enterprise's cybersecurity posture. Reviewing the security posture of a third party may include setting specific contractual clauses (e.g., SLAs, right to audit) and requiring providers to provide proof of alignment with specific frameworks, standards, and/or regulations.

NIS2 and DORA align on what is defined as a critical ICT third-party service provider. NIS2 references DORA Article 31 in defining critical ICT third-party service providers. The criteria for determining if a third party is considered a critical ICT third-party service provider are:[32]

- The impact if the service provider experiences a large-scale operational failure
- The importance of the financial entities that rely on the ICT third-party service provider
- The ICT third-party service provider's substitutability

# Governance and Accountability

NIS2 and DORA have certain requirements around governance and accountability, especially related to senior management involvement. NIS2 specifies that management bodies at essential and important entities are responsible for approving cybersecurity measures and overseeing compliance. Additionally, these individuals may be held liable for noncompliance related to cybersecurity risk management.[33]

[31] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 28, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[32] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 31, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[33] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 20, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

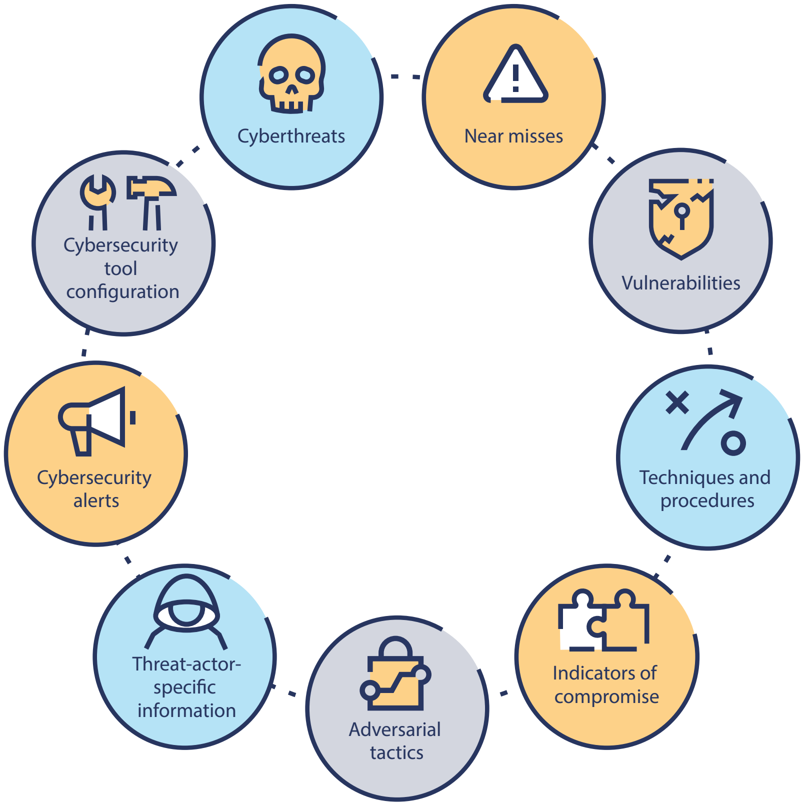
DORA requires management to oversee and be responsible for implementing the ICT risk management framework.[34] As with NIS2, DORA requires that this management body remain knowledgeable on the applicable topics to best perform their oversight and implementation duties.

# Information Sharing

To promote resilience and cybersecurity across an industry, enterprises may wish to share cybersecurity-related information with others in the industry. NIS2 and DORA allow this type of information sharing, but it is voluntary.

NIS2 allows entities in its scope to share information about the categories shown in **figure 5**.

FIGURE 5: Cybersecurity Information to Share



The purpose of information sharing should be to improve cybersecurity, or to prevent, detect, respond to, or recover from incidents or address their impact.[35]

Note that information sharing with other industry enterprises is voluntary, but significant incident reporting to competent authorities is mandatory.

[34] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 5, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[35] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 29, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

# Noncompliance

NIS2 has significant penalties for noncompliance. To complicate matters, the directive left many aspects to be executed by member states. Member states needed to transpose NIS2 into national law by 17 October 2024,[36] but only Belgium, Croatia, Hungary, Italy, Latvia, and Lithuania met the deadline.[37]

Like many member states, enterprises also struggle with NIS2 compliance. A survey conducted in Ireland in October 2024 indicated that 38% of Irish businesses would not be prepared for NIS2 compliance.[38]

NIS2 allows member states to impose fines for infringing on certain parts of the directive.[39]

DORA allows competent authorities to determine penalties and remedial measures for noncompliance.[40] This may include criminal penalties.[41] DORA does not set specific fines or penalties for noncompliance.

**Figure 6** shows the penalties for noncompliance with the NIS2 provisions around cybersecurity risk management measures and reporting obligations, which are outlined in Articles 21 and 23. Member states can set their own penalties for noncompliance with other aspects of NIS2.

FIGURE 6: NIS2 Noncompliance With Articles 21 and 23

| Essential Entities | Important Entities |
|---|---|
| Maximum fines of EUR 10,000,000 or 2% of total worldwide annual turnover, whichever is higher | Maximum fines of EUR 7,000,000 or 1.4% of total worldwide annual turnover, whichever is higher |

# Conclusion

Enterprises must determine whether they are compliant with NIS2 and/or DORA, as noncompliance could lead to large fines and potential reputational damage. It is also important to note that enterprises that provide their products or services to financial entities or essential or important entities in the European Union may have additional obligations under NIS2 and/or DORA, so familiarity with the requirements of the directive and regulation is essential. Performing a gap analysis to evaluate an enterprise's current security posture in relation to DORA and NIS2 requirements can be a crucial step to identifying areas of noncompliance and ensuring alignment with regulatory obligations.

**Figure 7** contains a high-level comparison of NIS2 and DORA.

[36] European Commission, "NIS2 Directive: new rules on cybersecurity of network and information systems," https://digital-strategy.ec.europa.eu/en/policies/NIS2-directive

[37] Pula, V.; "EU countries late in transposing new EU cybersecurity rules (NIS2)," 18 October 2024, https://www.cullen-international.com/news/2024/10/EU-countries-late-in-transposing-new-EU-cybersecurity-rules--NIS2-.html

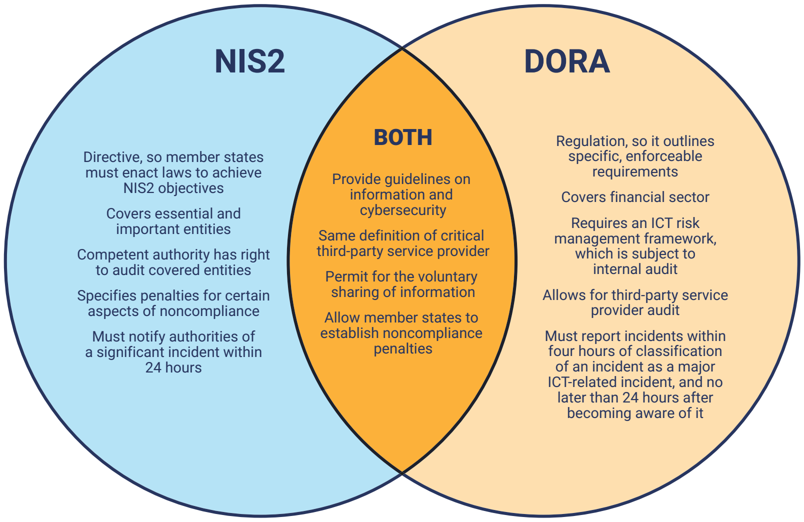
[38] Mason Hayes & Curran, "Four in Ten Irish Businesses Not Ready for New EU Cyber Rules," 15 October 2024, https://www.mhc.ie/latest/news/four-in-ten-irish-businesses-not-ready-for-new-eu-cyber-rules

[39] Official Journal of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)," Article 34, 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[40] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 51, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[41] Official Journal of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Article 52, 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

**FIGURE 7:** NIS2 and DORA Comparison Overview


NIS2
Directive, so member states must enact laws to achieve NIS2 objectives
Covers essential and important entities
Competent authority has right to audit covered entities
Specifies penalties for certain aspects of noncompliance
Must notify authorities of a significant incident within 24 hours
BOTH
Provide guidelines on information and cybersecurity
Same definition of critical third-party service provider
Permit for the voluntary sharing of information
Allow member states to establish noncompliance penalties
DORA
Regulation, so it outlines specific, enforceable requirements
Covers financial sector
Requires an ICT risk management framework, which is subject to internal audit
Allows for third-party service provider audit
Must report incidents within four hours of classification of an incident as a major ICT-related incident, and no later than 24 hours after becoming aware of it

Even for enterprises not subject to NIS2 or DORA compliance, these frameworks provide valuable strategies for enhancing resilience and risk management practices. Regularly reviewing third-party risk, conducting penetration testing, and performing audits are essential practices that can significantly benefit enterprises of all sizes across all jurisdictions and industries.

# Acknowledgments

## Lead Developer

**An ISACA Staff Publication**

## Expert Reviewers

**Aamir Jamil**

CISM, CGEIT

GRC Simplified Limited, United Kingdom

**Suzana Kužnik**

Forvis Mazars IT, Slovenia

**Christian Riley**

CISA, CISM

Royal London Group, United Kingdom

**Stefano Romagnoli**

CRISC

Luxembourg

**Rupinder Pal Singh**

CISA, CRISC, CISSP

NICE Incontact, USA

## Board of Directors

**John De Santis, Chair**

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

**Niel Harper, Vice-Chair**

CISA, CRISC, CDPSE, CISSP, NACD.DC

Chief Information Security Officer and Data Protection Officer, Doodle, Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), Germany

**Stephen Gilfus**

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

**Gabriela Hernandez-Cardoso**

NACD.DC

Former President and CEO, GE Mexico, Independent Board Member, Mexico

**Jason Lau**

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP

Chief Information Security Officer, Crypto.com, Singapore

**Massimo Migliuolo**

Independent Board Member, Malaysia

**Jamie Norton**

CISA, CISM, CGEIT, CIPM, CISSP

Partner, McGrathNicol, Australia

**Maureen O'Connell**

NACD.DC

Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

**Erik Prusch**

Chief Executive Officer, ISACA, USA

**Asaf Weisberg**

CISA, CISM, CGEIT, CRISC, CSX-P, CDPSE

Chief Executive Officer, introSight Ltd., Israel

**Pamela Nigro**

ISACA Board Chair 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Vice President, Security, Medecision, USA

**Tracey Dedrick**

ISACA Board Chair, 2020-2021

Former Executive Vice President and Head of Enterprise Risk Management, Santander Holdings, USA

**Brennan P. Baybeck**

ISACA Board Chair, 2019-2020

CISA, CISM, CRISC, CISSP

Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

## About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 180,000+ members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through the ISACA Foundation, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

### DISCLAIMER

ISACA has designed and created *Resilience and Security in Critical Sectors: Navigating NIS2 and DORA Requirements* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

### RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

**Phone:** +1.847.660.5505

**Fax:** +1.847.253.1755

**Support:** support.isaca.org

**Website:** www.isaca.org

**Participate in the ISACA Online Forums:**
https://engage.isaca.org/onlineforums

**X:** www.x.com/ISACANews

**LinkedIn:**
www.linkedin.com/company/isaca

**Facebook:**
www.facebook.com/ISACAGlobal

**Instagram:**
www.instagram.com/isacanews/