Brochure

NIS2 - are you affected and how to comply

WITH secure

The second Network and Information System Directive (NIS2), published by the EU, establishes a minimum standard of cyber security risk and incident management to which organizations that operate services deemed critical to the EU economy must adhere. These services include water, transport, energy, healthcare and digital infrastructure.

Organizations have until October 2024 to comply with NIS2. This document explains what organizations need to do now and how we can help.

Who does it concern?

NIS2 widens the scope of the original NIS Directive which came into force in 2016, reflecting the growing cyber threat to the EU economy.

The following industries are included in the scope of NIS2:

- Electronic communications
- Digital services
- Space
- Food
- Waste management
- Critical product manufacturing (e.g. medicine)
- Postal services
- Public administration.

NIS 2 applies to any organization with more than 50 employees whose annual turnover exceeds €10 million and any organizations included in the original NIS Directive. It may also apply to key suppliers to these organizations.

NIS2 in brief

Organizations must implement technical, operational and organizational measures to manage risks in their networks and systems, and to be more resilient, as depicted below.

Information security strategy and policies
Create an internationally-recognised information security management system (ISMS) that enables: a systematic, proactive approach to risk management; alerting to potential IT vulnerabilities; and annual reviews.

Incident prevention, detection and response
Establish appropriate capabilities to prevent, deter and extinguish cyber security attacks.

Business continuity and crisis management
Have a verifiable plan for how the company will react to an attack and how it can recover as quickly as possible.

Supply chain security
Evaluate and manage the risks posed by vulnerabilities within their supply chain.

Vulnerability disclosure
Vulnerabilities identified within the organization's networks must be disclosed.

Incident reporting
Submit an initial report within 24 hours of becoming aware of any “significant” incident; a full incident report within 72 hours and a final report within one month.

Cooperation between member state authorities
Share EU-level data that enables more efficient responses to cyber incidents.

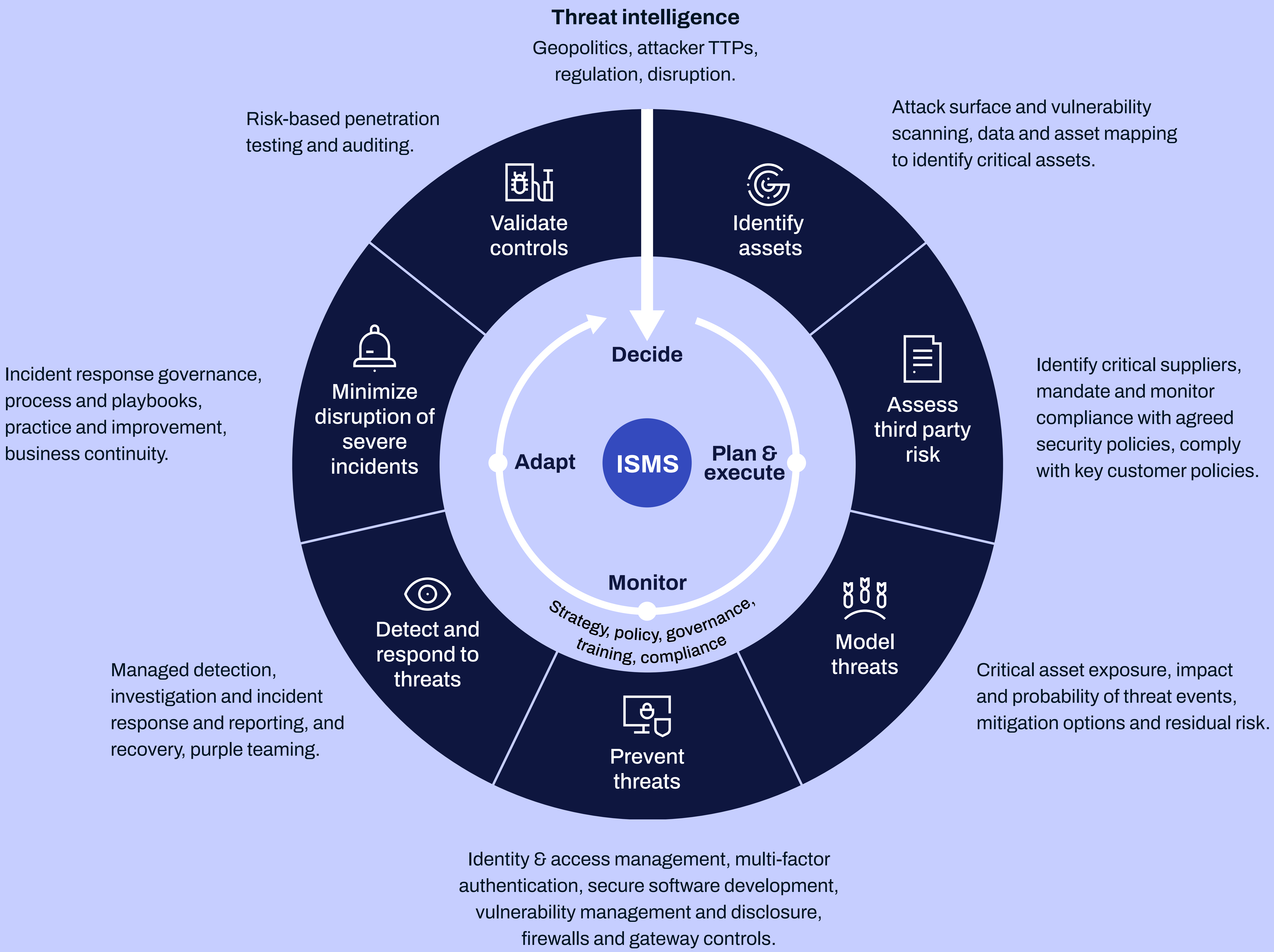
For non-compliance with NIS regulations, companies may be fined up to £17 million in the UK and €10 million or 2% of worldwide turnover in the EU - whichever is higher.

Resilience is the ability to function in some degree when under stress, yet return to normal function when the stress is removed.

What organizations need to do

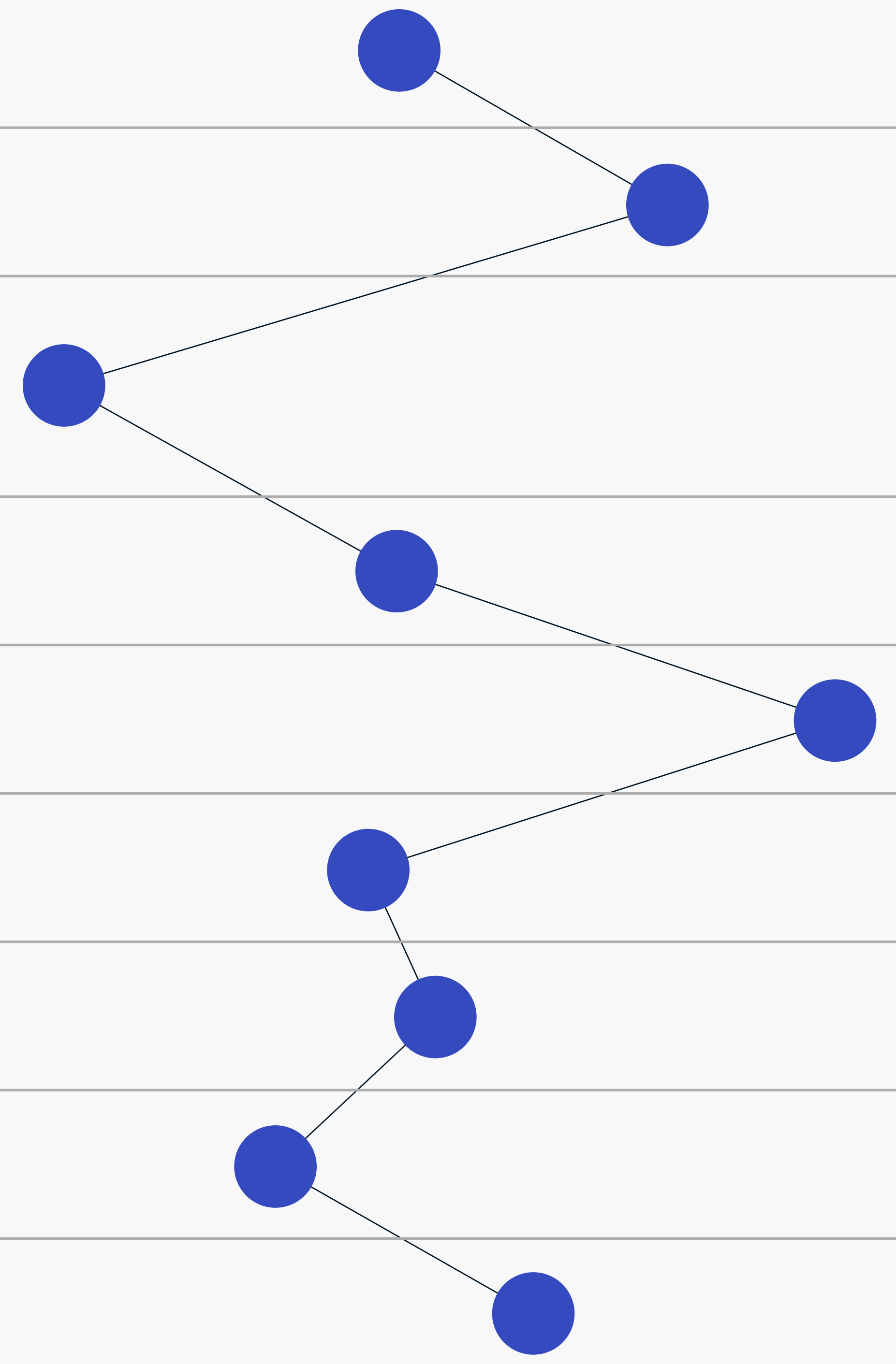
The EU recommends that organizations should set up and maintain an internationally recognised information security management system (ISMS), e.g. ISO27001, that enables them to manage their cyber risk and resilience to cyber attacks.

The scope of the ISMS is depicted in the figure.


Threat intelligence
Geopolitics, attacker TTPs, regulation, disruption.
Risk-based penetration testing and auditing.
Attack surface and vulnerability scanning, data and asset mapping to identify critical assets.
Validate controls
Identify assets
Decide
Minimize disruption of severe incidents
Adapt
ISMS
Plan & execute
Assess third party risk
Incident response governance, process and playbooks, practice and improvement, business continuity.
Identify critical suppliers, mandate and monitor compliance with agreed security policies, comply with key customer policies.
Monitor
Strategy, policy, governance, training, compliance
Detect and respond to threats
Model threats
Prevent threats
Managed detection, investigation and incident response and reporting, and recovery, purple teaming.
Critical asset exposure, impact and probability of threat events, mitigation options and residual risk.
Identity & access management, multi-factor authentication, secure software development, vulnerability management and disclosure, firewalls and gateway controls.

The ISMS sets out how the organization's cyber risk strategy will be implemented: the policies and security controls used to manage cyber risk and the outcome-driven metrics for assessing whether they are adequate and effective, as illustrated below.

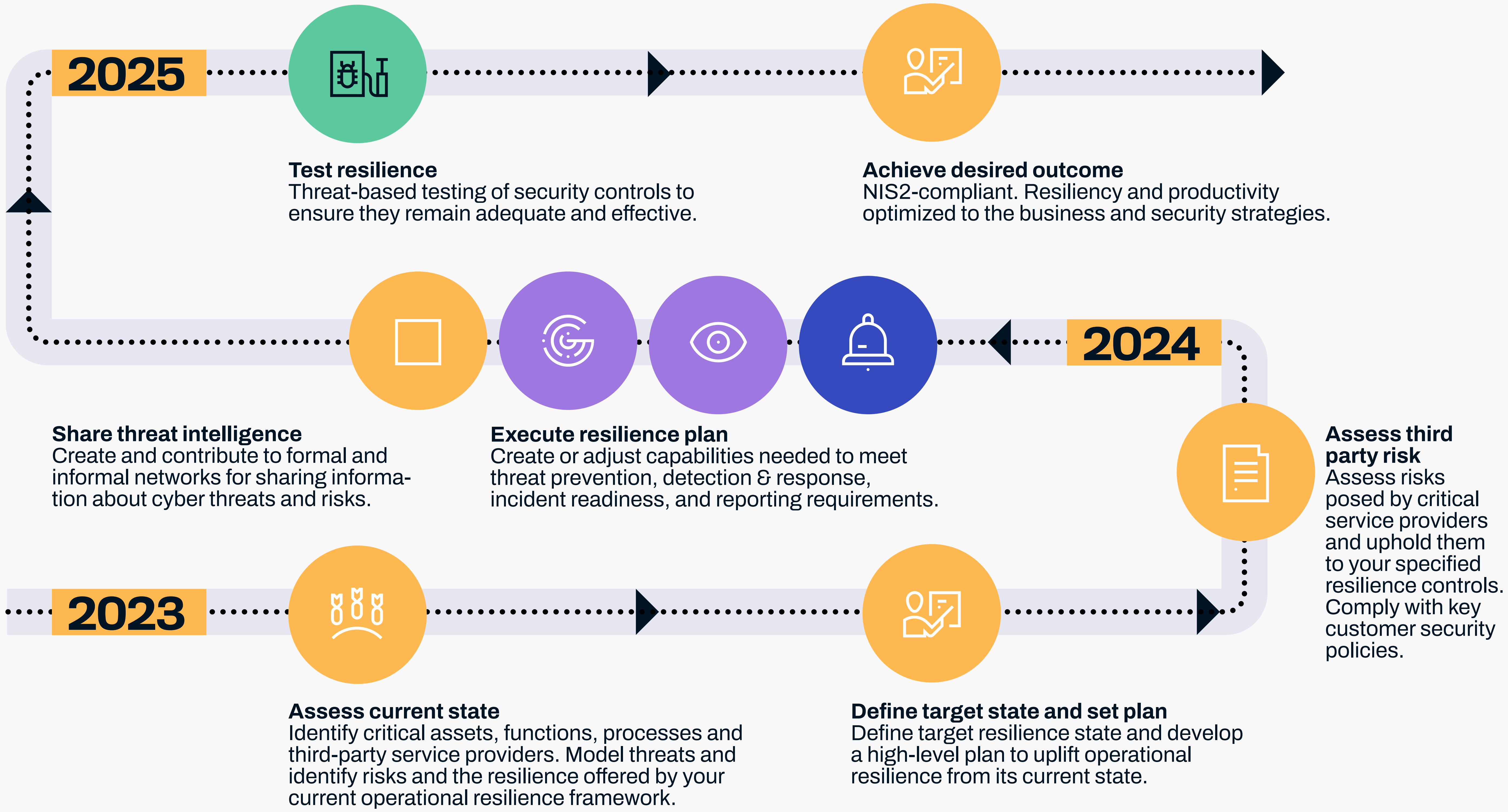
Outcome –driven metric	Variables	Performance level (illustrative)
Variables	Daily, weekly, monthly	
Performance level (illustrative)	Sysadmins only, IT and field staff; all staff	
Acceptable third-party risk threshold	Documented QA system, certified QA system only, adherence to your security policies	
IT backup policy	On or offsite, online or offline, frequency, scope	
Attack surface scanning frequency	Daily, weekly, monthly, scope	
Production software vulnerability rate	One, three or ten per thousand lines of production code	
Crisis management practice	Frequency, exec-level involvement, realism	
Penetration testing scope	Testing method, systems in scope, test objective	
Detection sensitivity and specificity	False positive rate, testing frequency, scenarios tested	



The strategy should be periodically reviewed to ensure that it remains appropriate in a changing threat environment.

How we can help

We help organizations to achieve their chosen level of resilience, as prescribed by NIS2, using the approach depicted below. The first step is a gap analysis to determine the quality of organizations' current capability relative to the minimum standards prescribed by NIS2. This will enable us to plot a path to NIS2 compliance that is optimized to your organization's business and security objectives.



Assess current state
Identify critical assets, functions, processes and third-party service providers. Model threats and identify risks and the resilience offered by your current operational resilience framework.

Define target state and set plan
Define target resilience state and develop a high-level plan to uplift operational resilience from its current state.

Assess third party risk
Assess risks posed by critical service providers and uphold them to your specified resilience controls. Comply with key customer security policies.

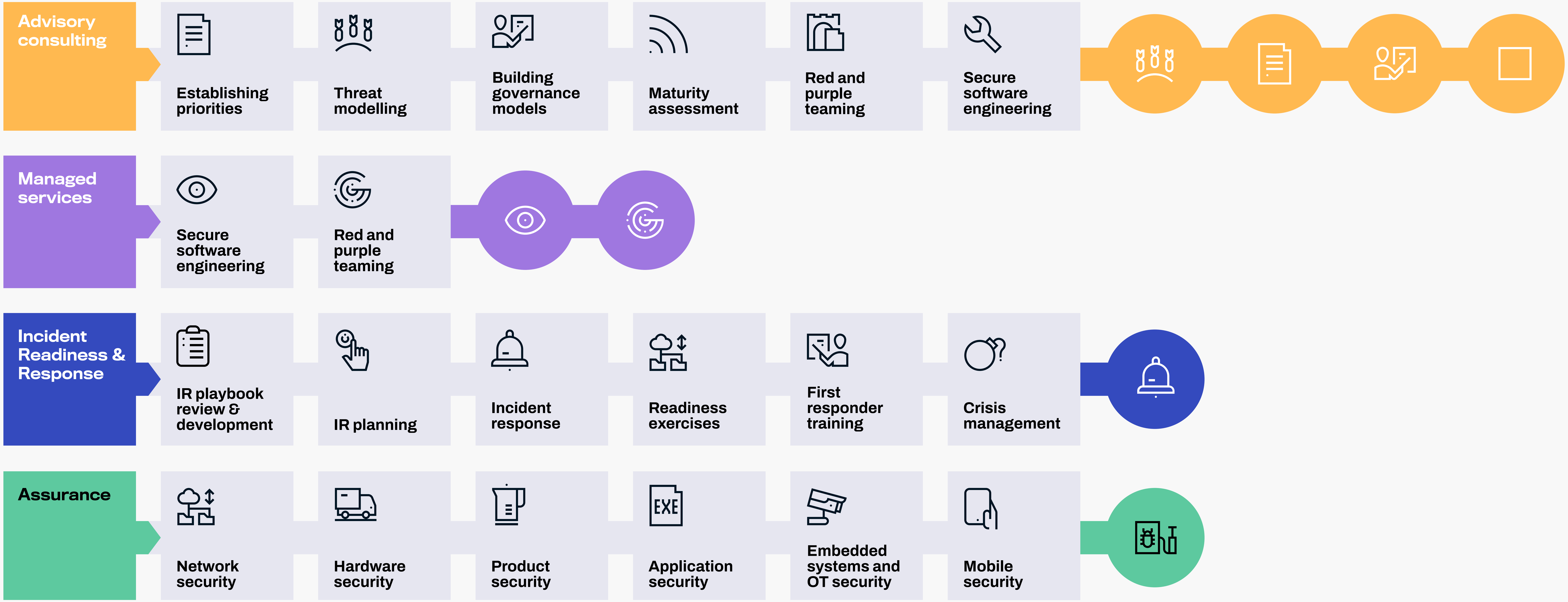
Execute resilience plan
Create or adjust capabilities needed to meet threat prevention, detection & response, incident readiness, and reporting requirements.

Share threat intelligence
Create and contribute to formal and informal networks for sharing information about cyber threats and risks.

Test resilience
Threat-based testing of security controls to ensure they remain adequate and effective.

Achieve desired outcome
NIS2-compliant. Resiliency and productivity optimized to the business and security strategies.

WithSecure™ offers a range of Consulting and Managed Services to support organizations in their journey to NIS2 compliance.



Advisory consulting

- Establishing priorities
- Threat modelling
- Building governance models
- Maturity assessment
- Red and purple teaming
- Secure software engineering

Managed services

- Secure software engineering
- Red and purple teaming

Incident Readiness & Response

- IR playbook review & development
- IR planning
- Incident response
- Readiness exercises
- First responder training
- Crisis management

Assurance

- Network security
- Hardware security
- Product security
- Application security
- Embedded systems and OT security
- Mobile security

The outcomes we deliver

WithSecure™ is a global provider of cyber security services. We are listed on the Nasdaq Helsinki, and we have offices in nearly 30 countries.

We provide consulting and managed services directly to over 700 enterprises. Our clients are members of the FTSE 100 and the Dow Jones. They include 20 of the world's largest financial, manufacturing and technology giants. We excel at solving hard, complex, security problems. Our red team is one of the most formidable offensive units in the world. Our incident responders are government-certified to combat threats from advanced state actors.

Feel free to call us for an initial free-of-charge consultation.

Outcomes we deliver

Resiliency

- Higher service availability during an incident
- Logical, defensible story in the event of a breach

Productivity

- Save money on unnecessary security expense
- Insurance eligibility under better terms
- Lower likelihood of unplanned expenditure
- Reduced annual loss expectancy

Reputation

- Preserve brand value
- Comply with regulations. Avoid fines and legal actions

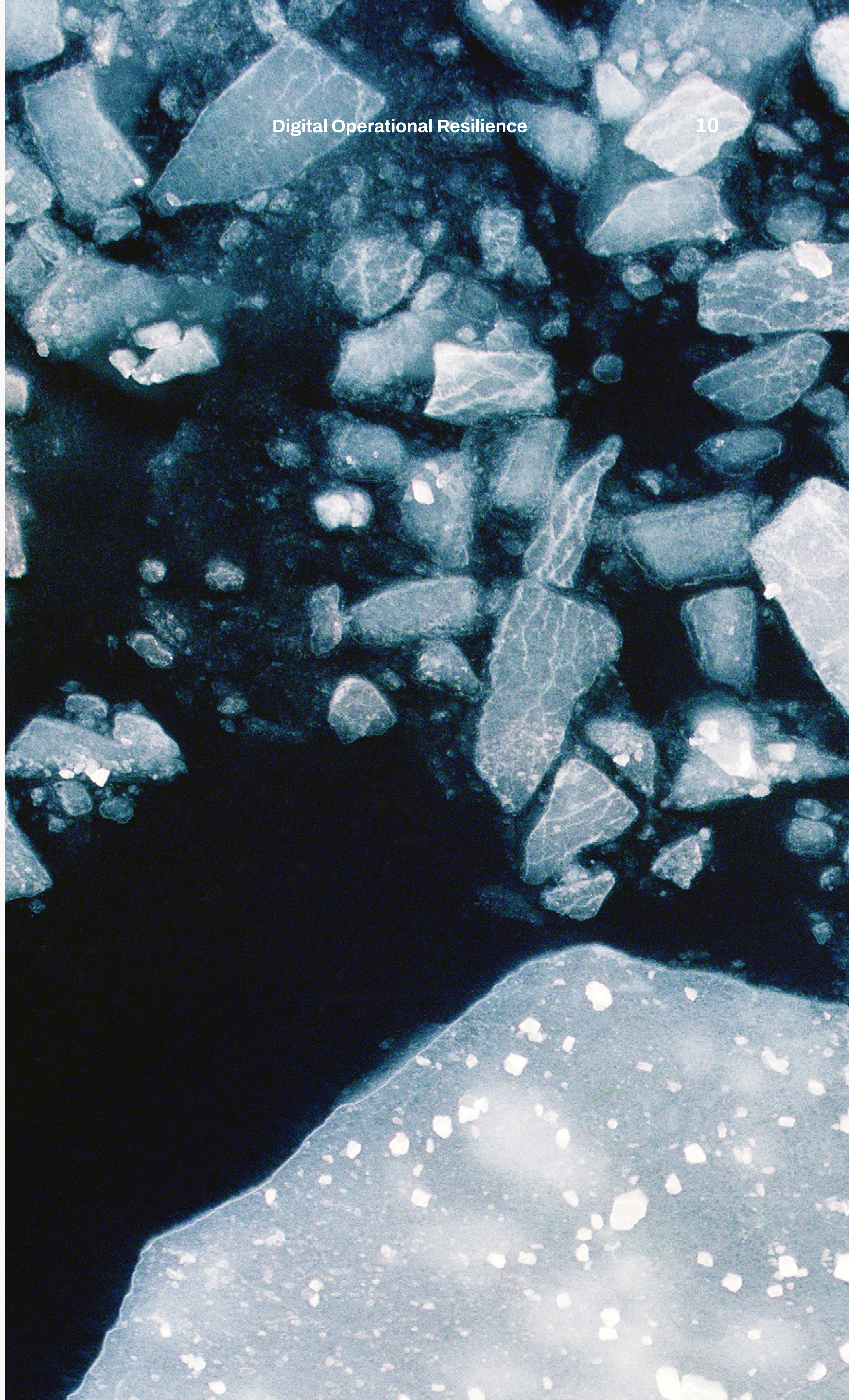
Sources

There are hundreds of summaries of NIS2 published online. Commendations go to Information Security management Systems (ISMS) Online who provide the most clearly written NIS2 summary of all:

https://www.isms.online/cyber-security/nis-2-what-the-proposed-changes-mean-for-your-business/

Other useful sources:

- https://www.ncsc.gov.uk/collection/caf/nis-introduction
- https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/



Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

W/TH®
secure