EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HANDBOOK FOR CYBER STRESS TESTS

MAY 2025

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, use enisa-nis-directive@enisa.europa.eu.
For media enquiries about this paper, use press@enisa.europa.eu.

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2025

COPYRIGHT NOTICE

ISBN: 978-92-9204-700-9, DOI: 10.2824/8248517, Catalogue Number: TP-01-25-009-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Stress tests became well-known in the wake of the global financial crisis of 2007–2009, when banking regulators, under the Basel Committee on Banking Supervision, wanted to supervise the asset portfolios of banks more closely and analyse if they were sufficiently strong to withstand financial shock scenarios.

Stress tests have been recently used to test cybersecurity, offering a new, lightweight and targeted method for assessing cybersecurity and resilience. For example, in 2022 the Bank of England did a cyber stress test of retail payment services in the United Kingdom and, in 2024, the European Central Bank (ECB) carried out a large cyber resilience stress test of EU banks. Last year the European Commission supported the EU Member States in conducting an EU coordinated stress test of the resilience of the EU's energy sector focusing on physical threats in scope of the Critical Entities Resilience (CER) Directive.

In this handbook, we define a cyber stress test as 'a targeted assessment of the resilience of individual organisations and their ability to withstand and recover from significant cybersecurity incidents, ensuring the provision of critical services, in different risk scenarios.' Stress tests focus on resilience, use resilience metrics and can be used to test both preparedness measures and responsive recovery measures.

This handbook contains a simple, five step guide to cyber stress testing (see illustration):

1. defining the test scope and objectives, engaging with stakeholders;
2. designing the test, choosing the methodology, refining the scenarios;
3. execution of the cyber stress test;
4. analysing results and identifying gaps;
5. following up on gaps and issues identified in the stress test.

We also apply this step-by-step guide to a practical example, explaining how a cyber stress test could be done in the health sector. We also explain how cyber stress tests can be carried out at the national, regional and EU levels.

For authorities, cyber stress tests can be a good way to start a dialogue with the sector, about both strategic and systemic risks, as well as more technical issues. Gaps revealed by stress tests can be discussed openly in collaborative and voluntary settings, but can also be followed up in a stricter supervision context.

Considering the current EU policy context – with the European Union focusing more on preparedness and resilience, and with the transposition of the NIS2 Directive[1] concluding – cyber stress tests can become an important new tool in the toolkit of the NIS authorities in the coming years. At ENISA, we look forward to supporting national authorities and agencies, at the national and EU levels, with carrying out national-, regional- and EU-level cyber stress tests.

[1] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

1. INTRODUCTION

While vital to the functioning of modern societies, critical infrastructure's reliance on increasingly sophisticated and interconnected technology is increasing its exposure to systemic failure and disruptive threats. The European Union has intensified its collective efforts to achieve a high level of cybersecurity and strengthen resilience across critical infrastructure sectors.

The Cyber Solidarity Act[2] further supports these efforts by laying down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

Because cyber stress tests are a relatively new concept in the cybersecurity domain, we developed this handbook, mainly aimed at national authorities overseeing cybersecurity and resilience of critical sectors. This handbook is based on desktop research and discussions with cybersecurity experts and other experts from critical sectors, where different types of stress tests have been carried out.

In the cybersecurity domain there is already a wide range of different cybersecurity assessment and testing methods, for example audits, penetration tests, ethical hacking, red-teaming, vulnerability scanning and cyber exercises. Authorities and agencies should find the right methods to use, depending on the setting and their needs. Different methods can also be mixed and combined.

Cyber stress tests thus emerge as new tool in the regulatory toolkit of the national authorities overseeing the cybersecurity and resilience of critical sectors, complementing other more well-known supervision activities.

In this handbook, we provide a definition of cyber stress tests and discuss common characteristics (in Section 2), we provide a step-by-step guide for cyber stress testing (in Section 3), explain how stress tests can be carried out at the EU level (in Section 4), and share a practical example of how to carry out a cyber stress test.

1.1 SCOPE AND TARGET AUDIENCE

The goal of this handbook is to guide authorities with the stress testing of the cybersecurity and resilience of entities in critical sectors, typically operators of critical infrastructure and providers of critical services. We include some case studies of stress tests done outside the cybersecurity domain, but we do not discuss these in much detail.

This handbook is aimed at national or sectorial cybersecurity authorities and national cybersecurity agencies overseeing cybersecurity and resilience of critical sectors, at the national level, regional or EU level, under NIS2, the revised EU NIS Directive. The handbook could also be useful for supervisory authorities under the Digital Operational Resilience Act (DORA), the EU regulation for operational resilience of the EU's finance sector, or national authorities under the CER Directive. The handbook could also be useful for other authorities, agencies and policy makers, at both the national and EU level.

1.2 POLICY CONTEXT

We list several EU policy initiatives relevant for stress tests.

- **NIS2.** The NIS2, the revised NIS directive, aims to improve the cybersecurity and resilience of information and communication technology (ICT) in critical sectors. NIS2 has a broader scope of critical sectors, strengthens risk management and reporting requirements for entities in these critical sectors, and aims to increase the cybersecurity capabilities of Member States and increase collaboration at the EU level. National- and EU-level cyber stress tests can be a new tool for authorities supervising the network and information systems sectors.
- **Union risk evaluations.** The European Commission, the Member States and ENISA have been conducting union risk evaluations, resulting in risk scenarios. See for example, the 5G toolbox, the Nevers risk assessment and the Cyber risk posture report[3].

[2] https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act
[3] https://ec.europa.eu/newsroom/dae/redirection/document/107357

These union risk evaluations have led to the creation of strategic/systemic cyber risk scenarios, which can be used for cyber stress testing.

- **Cyber Solidarity Act (CSoA).** The Cyber Solidarity Act aims to strengthen capabilities in the EU to detect, prepare for and respond to cybersecurity threats and incidents. It introduces the cyber reserve funding mechanism and EU funding for 'coordinated preparedness testing' by Member States, which will be focused on critical sectors and specific risk scenarios, and which include national or regional cyber stress tests.
- **Niinistö report.** The Niinistö report 'Safer Together – Strengthening Europe's civilian and military preparedness and readiness', makes several recommendations on how to enhance Europe's civilian and defence preparedness and readiness, and calls for union risk evaluations, including broad all-hazard, all-sector risk evaluations.
- **DORA.** DORA, the Digital Operational Resilience Act, is *lex specialis* under the NIS2 and aims to strengthen the digital resilience of the EU's financial sector. DORA introduces mechanisms for identifying common cyber vulnerabilities and risks across the financial sector, for example through analysis of major incidents reported by banks.
- **CER.** CER, the Critical Entities Directive, complements NIS2 by focusing on resilience of critical infrastructure in general, in the face of physical attacks and natural hazards. CER requires Member States to adopt a national strategy and perform risk assessments, as part of an all-hazards approach, accounting for both man-made threats and natural disaster risks, to prevent or minimise the effects of disruptions of essential services. Critical entities identified under CER are automatically in scope of NIS2. NIS2 is intended to act as the cybersecurity *lex specialis* for (the broader) CER, meaning that cybersecurity threats and cybersecurity measures to protect ICT systems are in scope of NIS2.

2. STRESS TESTING FOR CYBERSECURITY AND RESILIENCE

2.1 DEFINING CYBER STRESS TESTS

There are different definitions of stress tests ([4]) ([5]) and cyber stress tests ([6]) ([7]), used in different contexts and for different purposes. In this handbook we define a cyber stress test as follows:

> **Cyber stress test:** a cyber stress test is a targeted assessment of the resilience of individual entities and their ability to withstand and recover from significant cybersecurity incidents, ensuring the provision of critical services, in different risk scenarios.

In practice, stress tests are mostly 'desktop-based', relying on a technical questionnaire, centred around one or more risk scenarios, which is filled out independently by the entities/organisations that are being tested. Stress tests can test both preparedness measures and response/recovery measures. The assessment is targeted, because it focuses on specific risk scenarios and specific threats, not on all cybersecurity aspects. Gaps identified in the stress test can be followed up by a national authority, in a more open, collaborative process, during discussions with the different stakeholders or potentially in a stricter supervisory approach. Stress tests can be carried out at the national, regional or EU level.

Characteristics of cyber stress tests

We list the key characteristics of cyber stress tests as follows.

1. **Resilience focus.** Stress tests are designed to evaluate the resilience of an organisation in the face of different cyber threats. Stress tests are not forecasts, but tools to understand failure points, to improve preparedness, response and recovery.
2. **Scenario-based.** Follow a 'what if' approach, building on plausible and as close to the real world as possible risk scenarios.
3. **Stress levels.** Stress test have different stress levels, to understand the organisation's preparedness in different scenarios. At the highest stress level, the stress test scenario includes low-probability–high-impact incidents, also known as 'black swan' events.
4. **Resilience metrics.** Stress tests use resilience metrics to qualitatively and quantitively 'measure' the resilience of the entities. Examples of metrics used in cyber stress tests are 'time-to-detect' and 'time-to-recover'.
5. **Individual and independent.** Stress tests are carried out by organisations individually, independently, that provide the required evidence often through the use of detailed questionnaires.
6. **Systemic risk view.** Stress tests start from a systemic risk view of the sector and are also used to identify cascading effects and interdependencies.

What is not a cyber stress test

A cyber stress test is **not**:

- **a penetration test**, which is a live simulation of an attack, often on the actual live infrastructure, with a tester trying to actually break through defences;
- **conducted in real time**, as this type of test is desktop-based and usually relies on a technical questionnaire for the main assessment;

([4]) ECB stress tests, https://www.bankingsupervision.europa.eu/activities/stresstests/html/index.en.html.
([5]) Joint Research Centre: Institute for the Protection and Security of the Citizen, Galbusera, L., Ward, D. and Giannopoulos, G., *Developing stress tests to improve the resilience of critical infrastructures – A feasibility analysis*, Publications Office of the European Union, Luxembourg, 2014, https://data.europa.eu/doi/10.2788/954065.
([6]) Danish Financial Supervisory Authority (n.d.), 'Cyber stress testing', https://www.dfsa.dk/Media/638665595227077818/Cyber %20stress %20testing_v4.pdf.
([7]) Bank of England (2024), 'The Bank of England's approach to stress testing the UK banking system', https://www.bankofengland.co.uk/stress-testing/2024/boes-approach-to-stress-testing-the-uk-banking-system.

- **a cyber exercise**, as this type of test is individual and carried out independently by entities, and does not test operational collaboration between entities, as in cyber exercises, where players share information and collaborate with other entities.

Advantages of cyber stress tests

Cyber stress tests have several advantages over other cybersecurity assessment methods.

- **Lightweight.** Cyber exercises which focus on operational collaboration require a great amount of preparation and coordination, to ensure everyone is online and ready to play out scenarios and engage with the other players in the cyber exercise at that same moment. Cyber stress tests, however, are individual and independent, which means that there is more flexibility for entities to carry out the stress test, using their own timing and planning. Being paper-based, cyber stress tests do not require complex tools, for example to live-simulate scenarios or attacks.
- **Targeted.** Audits are often broad, covering a wide range of cybersecurity threats and measures. This makes the process of auditing resource-intensive, both for the auditor and the auditee. Cyber stress tests focus on a few very specific risk scenarios, which makes them much more targeted, and also easier.
- **Objective.** Auditing the risk management and security measures of a company, for instance the company's risk list, or the measures they took or didn't take, can be a rather subjective exercise. Cyber stress tests use resilience metrics, which make the overall assessment process more objective.
- **Collaborative.** To build up cybersecurity and resilience in critical sectors, a partnership is needed between the national authorities and the owners/operators of the critical infrastructure. In this context, a compliance-based approach to supervision, based on audits, can be counter-effective, consuming scarce cybersecurity resources with broad compliance checklists of security measures. Cyber stress tests allow to start a dialogue with the sector, about specific risk scenarios, taking a systemic risk view.

Stress test objectives

National cybersecurity authorities and agencies can use cyber stress tests to:

- assess the preparedness of individual entities in the face of significant incidents, even in severely adverse circumstances;
- assess the preparedness of the critical sector overall, and help with understanding systemic risks;
- respond to a national risk assessment pointing to specific risks or risk scenarios;
- prepare for a cyber exercise that tests cross-border and cross-sector operational collaboration between stakeholders, using similar risk scenarios;
- support authorities in setting supervision priorities, singling out systemic issues;
- start a dialogue about key threats, and a collaboration with critical sector entities.

For entities undergoing a cyber stress test, there are also benefits in taking part in a stress test, because it will help the entity understand preparedness and resilience when faced with significant cybersecurity incidents.

2.2 CYBER STRESS TESTS AS PART OF THE SUPERVISION TOOLKIT

Under the NIS2, national authorities and agencies need to supervise the cybersecurity and resilience of entities in the critical sectors. There are many different approaches national authorities can take for this, and cyber stress tests can become a part of their toolkit.

Supervision beyond auditing

After specifying what are the detailed cybersecurity requirements for the sectors, national authorities need to supervise and ensure that these requirements are met. Authorities often audit, or ask a third party to audit, the entities in the sector. Audits can be done *ex ante* or *ex post*, that is, before or after incidents happen. Audits can be paper-based, online or on-site. Historically, audits in the cybersecurity domain have been carried out mainly for compliance reasons, for example for ISO27001 or SOCS compliance, and are usually rather broad, costly and lengthy assessment processes. However, it is important to underline that authorities can

engage with their sectors in many other ways, for example by providing threat intelligence, providing guidance, by organising workshops to raise cybersecurity awareness or discuss common issues, by starting public–private partnerships for common cybersecurity issues or by organising cyber exercises. Cyber stress tests can also be used by authorities to engage with the sector and are well-suited to start a dialogue about specific threats or risk scenarios.

Mixing cyber stress tests with other cybersecurity assessment methods

Besides cyber stress tests, the cybersecurity domain has a wide range of other cybersecurity assessment and testing methods which authorities can use, such as on-site audits, penetration tests, ethical hacking, red-teaming and vulnerability scanning. Authorities and agencies should find the right methods to use, depending on their setting and their needs. A subsea cable is very different from a pacemaker, and therefore the telecom sector may need a very different approach than the health sector Different methods can also be mixed and combined. For example, an audit can be preceded by a vulnerability scan, a cyber stress test can be followed up with a cyber exercise and so on.

Mandatory/stringent versus voluntary/exploratory cyber stress tests

Depending on the cybersecurity maturity of the sector and depending on the needs, authorities can decide to adopt a more mandatory/stringent approach to cyber stress tests, or a more voluntary/exploratory approach. It is important that authorities clarify their intentions towards the entities being stress tested: authorities should clarify upfront what will happen with the stress test results, if gaps will be followed up, etc.

Authorities should weigh the pros and cons of taking a more stringent/mandatory approach versus a more exploratory/voluntary approach when organising a stress test. We list some pros and cons:

More stringent/mandatory cyber stress tests – more formal, often compulsory, backed by strict detailed legal requirements for the sector:

- Gives a new method for ex-ante supervision, which is targeted
- Captures maturity of multiple entities exposed to the same risk scenario
- Better insights into entities capabilities and sector specificities

Cons

- Entities may see the stress test as a compliance exercise
- Entities may refrain from fully stress testing capabilities to avoid sanctions.

More exploratory/voluntary cyber stress tests – collaborative approach between authority and entities, focused on gaining insights, aimed at starting a dialogue and collaboration

Pros:

- Voluntary, non-supervisory approach leads to more collaboration and more open discussions
- Greater buy-in, increased willingness to disclose on capabilities and weaknesses
- More flexibility to address novel topics where authorities and sector still lack knowledge
- More open approach allows to identify and discuss unforeseen dependencies and impact

Cons:

- Voluntary approach may lead to lack of engagement and participation by entities
- Data collected during the stress test may be less accurate or incomplete
- Entities may be unwilling to address the recommendations resulting from the stress test

3. STEP-BY-STEP GUIDE FOR CYBER STRESS TESTING

In this section we provide a step-by-step guide for doing a cyber stress test. We use the following terminology.

- **Authorities.** The authorities carrying out the cyber stress test, for example a cybersecurity agency or a sectorial/national cybersecurity authority.
- **Entities.** The entities undergoing the cyber stress test, meaning the critical infrastructure operators which will be undergoing the stress test, responding to the stress test challenges. Entities is the NIS2 terminology for the companies in the sector.
- **Stakeholders.** Other organisations with an interest in the outcomes of the cyber stress test, or with relevant expertise for the design of the stress test, for example, a sectorial industry association, sectorial experts or a sectorial authority with sectorial expertise but limited cybersecurity mandate. It is good practice to form a stress test working group or committee, with the authorities and the stakeholders, to oversee the stress test process.

The figure below summarises the five steps in organising a cyber stress test.

Below we explain the steps in more detail, and discuss trade-offs and some good practices.

1. Cyber stress test scope and objectives	The scope and objectives of the cyber stress test are defined by choosing the sector, the target entities and infrastructure, and the high-level risk scenarios. In this step, stakeholders are identified, who can support and help design the cyber stress test.

1a. Define sector, entities and infrastructure in scope. Firstly, the sector, the type of entities and the target ICT infrastructure needs to be decided. It is crucial to have a clearly defined scope to ensure that a test is feasible. Stress testing an entire sector may not be feasible, and a subset of entities may need to be chosen, for example, within the telecom sector, stress testing only the large mobile network operators.

It is important to note that with a broader scope, entities will be more diverse, making it harder to design a fitting stress test that works for all later on. The advantage of a broader scope is that more systemic risks can be assessed, but it may require the design of several versions of the stress test for the different entities in scope. For example, if the scope is set to the telecoms and electricity subsector, then inter-dependencies can also be evaluated (telecoms depending on the grid, and the grid depending on the networks), but in this case two versions of the stress test will certainly be needed, to be appropriate for both telecom operators and electricity

producers. If the scope of the stress test is limited to only telecom operators, then the telecom dependency on the power grid could be assessed, perhaps revealing a single point of failure, but not the electricity sector's own dependency on the telecom networks.

One of the most important aspects of stress test design is deciding how many and which entities will be tested. There is a trade-off between breadth and depth. If more entities are involved, then the stress test will produce a broader picture of the sector, but diversity will make it more difficult to go into specifics. The collection of results will likely be more focused on statistics, and it will be more difficult to identify specific gaps and issues. The advantage of involving a larger set of entities is that the stress test may show single points of failures, which would otherwise not be seen. For example, when stress testing a large number of companies, it may become clear that too many companies are relying on the same supplier. Such dependencies may remain hidden with fewer entities.

1b. Define test objectives and high-level risk scenarios. Secondly, the objective of the stress test needs to be decided and formulated, and the risk scenarios need to be chosen. Cyber stress tests can cover preventive cybersecurity measures as well as incident response and recovery measures. Depending on the needs, the focus of the stress test may be more on prevention and preparedness, or more on response and recovery. For example, the objective of a stress test could be to assess the preparedness and resilience of large hospitals with respect to targeted cyber-attacks by ransomware groups, and their ability to continue providing care.

A cyber stress test could focus on ransomware readiness, or on large-scale espionage attacks, on physical sabotage of network infrastructure, or on redundancy and failover, and so on. In general, when choosing the risk scenarios for the stress test, it is a good idea to address multiple cyber threats and threat types. But by making the risk scenarios too complex, for example by adding too many different threats, the stress test may become too broad. There is a risk of losing focus and turning the cyber stress test into a generic information security management system audit questionnaire.

1c. Engage relevant stakeholders. Thirdly, once the sector, the targeted ICT infrastructure, the objectives and the risk scenarios are determined, it is important to engage other stakeholders who can support the stress tests, for example with valuable domain knowledge, or who can benefit from the stress test.

Stakeholders may be non-cyber authorities, sectorial agencies, sector-specific experts or working groups, national computer security incident response (CSIRT) teams, law enforcement, civil contingency agencies, etc. It depends both on the choice of sector and the choice of risk scenarios. For example, when stress testing the energy sector, and ICT infrastructure underpinning electricity production in particular, then the relevant stakeholders could be grid operators (transmission system operators, distribution system operators). If, for example, the high-level risk scenario involves a cyber-attack by organised crime groups, then it could be useful to involve a law enforcement agency, to provide input on past cybercrime cases.

Good practice for stakeholders: 'Establish an oversight committee composed of different subject matter experts, on cybersecurity and on sectorial matters'

It is a good idea to also involve the stakeholders in the rest of the cyber stress test, and particularly for the design of the test, the refinement of the scenario, the definition of the right metrics and the follow-up in the conclusion phase. The stakeholder group can also act as a steering board or oversight committee.

2. Cyber stress test design	The authority designs the stress test, choosing the methodology, refining the scenario and developing the resilience metrics that are linked to the stress test objectives.

2a. Testing methodology. Choosing a stress testing methodology is key to ensuring alignment with the objectives and the scope previously identified. As mentioned already, although there are variations, stress tests are mostly 'desktop-based', relying on a technical questionnaire, centred around one or more risk scenarios, which is filled out independently by the organisations that are being tested. We provide a simplified example of such a stress test questionnaire below. A stress test could also be done via an on-site visit or with a scheduled and structured interview.

Stress test questionnaire – EU health sector example

Stress level 1

What if a phishing email with malware targets back-office staff?

- Which measures do you have to prevent it? (choose from awareness training, endpoint detection, email phishing filter, etc)

What if these preventive measures have failed or were circumvented, and the malware is downloaded and installed?

- Rate the risk for patient data and health records (very low – very high).

Stress level 2

What if the attackers attempt to infect other PCs?

- Which measures do you have to prevent lateral movement?

What if these measures have failed or were circumvented?

- Rate the risk for patient care and safety (1–10).
- How fast is it detected, and when does response start?
- How fast can you restore and recover?

Stress level 3

What if the attackers attempt to move laterally to medical / operational technology (OT) devices?

- Which prevention measures do you have (choose from airgap, zero-trust, firewalls, etc.)?

What if …

- Rate the risk for patient care and safety (very low–very high).
- Rate the risk for your critical care operations (extended care unit, intensive care unit, etc.).
- …

2b. Scenario refinement. In this step the high-level risk scenarios need to be refined, choosing the specific infrastructure, business processes, information technology (IT) architecture and ICT systems in scope. It is important to focus stress tests on the most relevant infrastructure and the main risks, ensuring a targeted and effective assessment.

Good practice for scenario refinement: 'Identify key business processes and/or categories of critical cyber and physical systems'

Escalation in scenario development is key to realistically assessing resilience under increasing pressure. A gradual escalation of severity can be delivered either by scaling the impact of a single scenario or layering multiple scenarios together for each variation (by means of injects with additional information after the first responses are obtained, or by using 'what if' questions in the data collection template).

The level of detail needed depends on the number and variety of entities in scope and whether the test has a stringent or exploratory supervision approach. If the test focuses on specific failure points, there needs to be sufficient detail. In a more exploratory approach, the risk scenario may be more generic, asking entities to provide feedback on a broader range of potential impacts and mitigation strategies.

Good practice for risk scenarios: 'Include sector-specific elements based on sectorial threat landscapes, sectorial dependencies sectorial supply chain risks'

A good stress test scenario should have several sub-scenarios, addressing different impacts and different types of threats, allowing to stress test different aspects. In the case of the (all-hazard) NIS2 Directive, and specifically when it comes to stress testing the resilience of critical infrastructure entities, it is a good idea to stress test against a mix of cyber and cyber-physical threats. However, if too many threats are included in scope, and the scenario is very complex, with many sub-scenarios, then the stress test itself will become lengthy and time-consuming.

2c. Resilience metrics. Stemming from the stress objectives, the right resilience metrics should be chosen, which will measure the level of preparedness, resilience and the impact of the scenario. In the Belgium stress test case study (see Annex B), for instance, entities were evaluated using resilience indicators across three main areas: preparedness, incident response and recovery.

Good practice for metrics: 'Evaluation criteria should focus on assessing the performance and resilience of the entities being tested'

Resilience metrics can be qualitative or quantitative and should be framed within the scope, and be linked to the objectives of the stress test. For example, resilience metrics could be the time to detect an incident, the time to recover or the level of sophistication of preventative measures.

2d. Planning and timeline for the stress test. After the cyber stress test methodology has been defined, a more detailed planning and timeline can be set, deciding on the deadlines for the entities being stress tested, planning the collection and analysis of stress test results, and the follow-up phase. It is good practice to explain to the stress tested entities, up front, when they will need to complete the stress test, what the follow-up will be and how they will be involved.

3. Cyber stress test execution	The authority engages with the entities to execute the cyber stress test, providing guidance and explanation about the objectives of the test, the overall timeline and planning, and how results will be analysed and gaps followed up.

3a. Engagement with entities. In this step, the authority engages with the entities to execute the cyber stress test, providing the overall objectives and timeline, as well as guidance and explanations. Several aspects are important to address.

- Explaining the stress test objectives and the main risk scenarios.
- Explaining which experts are expected to carry out the tests on the side of the entity.
- Providing a contact point for questions and concerns, and asking for a single point of contact on the side of the entity.
- Clarifying confidentiality and usage is crucial: test results are often sensitive and should be handled with great care. It is important to explain how responses will be processed, who will have access, etc. Building trust between the entities and the authorities is important, not only for the sake of the upcoming cyber stress test itself but also for future interactions.
- Providing a detailed planning and timeline is important, including response deadlines, and, if foreseen, joint workshops to discuss identified gaps and findings.
- Identifying centralised single points of contact within the entities and establishing dedicated communication channels.

3b. Support and guidance for entities during stress testing. It is important to provide support and guidance for a smooth execution and to improve the quality and consistency of responses. Authorities should consider organising a kick-off workshop with the entities, to explain the stress test and address feedback. Developing a short "Frequently Asked Questions" is a good strategy to ensure that issues and questions are addressed and the answers made

available to all stress tested entities. Offering a helpdesk or support contact (direct email or phone number), during the stress test execution, should be considered.

4. Gap analysis	Data analysis is used to identify gaps, weaknesses and areas for improvement, for the individual entities and/or the sector overall. Stress test results are assessed qualitatively and quantitively against the predefined resilience metrics.

4a. Evaluate stress test findings. An analysis of the overall stress test results gives a good idea of the general baseline of the entities involved. It is a good idea to make use of data analysis tools to assess against the predefined metrics. Confidentiality and anonymisation is important in this step. Test results of a single entity may be very sensitive and should not be disclosed to other entities or to a general audience. Anonymised, aggregated findings may be interesting to share with a broader audience, but caution is advised, to avoid threat-actors using this information for future cyber-attacks.

4b. Identify gaps, including those of cross-sector or cross-border nature. Gaps and issues can be identified at different levels:

- gaps at an individual entity;
- common issues or gaps across multiple entities;
- dependencies on a specific entity in the sector;
- cross-sector or cross-border dependencies;
- supply chain dependencies;
- shared infrastructure or shared service providers.

While it is important to identify the gaps and the dependencies, it could also be useful to highlight in which area the entities, or the sector overall, are quite mature and well-prepared. This approach helps to build trust and collaboration between the authorities and the entities.

It is important that preliminary findings are discussed first in a closed setting, between the entities and the authority. In some cases, extending such discussions or presenting draft conclusions to both stakeholders and subject matter experts helps to validate the findings and supports further buy-in for the recommendations to be issued. Cybersecurity matters often require time and budget to be resolved. Developing mutual understanding, trust and openness makes the follow-up process easier.

5. Conclusion	In the final step, authorities report the findings from the test. If needed, they issue recommendations for individual entities or sector wide. Authorities oversee that such recommendations are implemented and draw lessons learned.

5a. Recommendations. The main goal of a cyber stress test is to understand what are the gaps and issues, and to follow up with targeted recommendations to address them. These recommendations should focus on immediate remediation and long-term improvements. Establishing a timeline and a plan for addressing the recommendations is crucial for ensuring that the cyber stress test leads to actual improvements.
Recommendations can be made at different levels.

Good practice:
'Provide guidance and frameworks for organisations to integrate stress test results into their risk management procedures'

- **Individual recommendations for individual entities.** Individual gaps and findings, as discussed already, should be handled with care and should be discussed in more detail with the entity in question.
- **Recommendations for the sector as a whole.** Sector-wide issues should be discussed in a broader forum, including stakeholders and the entities who participated in the stress test. Collective action, government funding or public–private partnerships may be needed to address these issues.

- **Cross-sector and cross-border recommendations.** The cyber stress test may even lead to recommendations related to cross-sector or cross-border issues, which should be discussed and followed up with authorities in other sectors or with national authorities in other countries, for instance in the NIS Cooperation Group.

Authorities should follow-up on the recommendations made, and periodically check to ensure that the recommendations are addressed after the cyber stress test. Rather than a stringent enforcement approach, authorities should focus on encouraging entities to submit regular progress reports detailing the status of their remediation actions. Building up cyber resilience is a continuous process of improvement, even in highly mature sectors.

5b. Lessons learned. Upon completion of the stress test, it is important to document the lessons learned about the overall stress test process. In this last step, the organisation and execution of the stress test itself, the effectiveness and efficiency of the test, and the adequacy of the testing method is analysed. It may be a good idea to collect feedback from the stress tested entities, but also from the other stakeholders. In this phase, a repetition of the stress test can be discussed, for example, if the next stress test should be based on a similar same stress test scenario, or if a different set of risks should be stress tested against.

4. NATIONAL, REGIONAL AND UNION CYBER STRESS TESTS

In this handbook, and in the step-by-step guide, we focus on national cyber stress tests, carried out by a national authority, stress testing entities in a critical sector, within a country. Of course, cyber stress tests can also be carried out at the regional level, involving multiple authorities, or even at the union level, involving all national authorities. In this section we briefly discuss these different possible variations of cyber stress tests.

National cyber stress tests

Probably the easiest way of carrying out a cyber stress test is to do it at the national level. A national authority with a cybersecurity mandate for a specific sector can engage with key entities in the sector, and execute a cyber stress test with these entities.

As we mentioned already, there is a trade-off in selecting entities to test. Stress testing a large group of entities means that more entities are reached, but the stress test questionnaire may have to be more generic, with mostly quantitative questions, and the stress test outcomes may be mostly statistics. With a smaller group, the stress test can be more tailored, and the follow-up can be more in-depth.

We give three simple examples:

- **5 entities within 1 sector.** A national telecom authority decides to do a stress test of the large mobile network operators, focusing on resilience of emergency communication during large scale crises and large-scale network outages. The stress test is mandatory, and the results are only analysed and followed up individually.
- **50 entities within 1 sector.** A national health authority decides to do a stress test of a wide range of entities in the health sector, including hospitals, clinics and laboratories. The stress test is mandatory but generic, and the main focus is to collect statistics about the overall maturity of the sector.
- **20 entities from 2 sectors.** National authorities for the energy and telecom sector collaborate to do a stress test of 10 big telecom operators and 10 big energy providers, to understand general preparedness but also specific inter-sector dependencies. The main goal of the stress test is to strengthen collaboration between the two sectors and discuss cross-sector issues.

We encourage national cybersecurity authorities to engage with authorities for other sectors at the national level, who may have experience in conducting other types of stress tests, for instance in the area of finance, or in the area of physical/natural threats and resilience. These other authorities may have useful knowledge to share. For instance, in the finance sector, stress testing has been done to assess solvency at different levels of financial/economic risk scenarios.

Regional cyber stress test

Although it complicates planning and coordination, there may be value in working with other countries in the region, especially when the economies are closely linked and there is shared infrastructure.

We give a simple example:

- **2 authorities from 2 countries, 5 entities from each country.** The electricity grids of two countries are closely linked, and two authorities from neighbouring countries decide to stress test several key entities in a regional stress test. The focus is on strengthening collaboration across the border, at the level of the authorities but also at the level of the entities. The kick off workshop is held in one country, and the concluding workshop is held in the other country.

It is important to note that the recently adopted Cyber Solidarity Act encourages Member States to carry out coordinated preparedness testing activities, and that the Commission has reserved dedicated funding (digital Europe programme) for these activities, which will be made available in funding calls launched by the European Cybersecurity Competence Centre. Preparedness testing

can include different assessment methodologies, and could also include national or regional cyber stress tests.

Union cyber stress test

As discussed already, for instance in the introduction and in the case studies in the annex, the ECB recently conducted an union cyber stress test of the EU's finance sector. Similarly, the Commission, together with the Member States, has recently conducted a union stress test of the energy sector, focusing on physical threats and natural disasters.

Taking an EU approach to stress tests can be very beneficial and effective. It can help national authorities with conducting stress tests at the national level, without burdening them with the details of organising the entire process, developing the questionnaire, collecting the data, analysing the results, etc. A union stress tests can start an EU-wide dialogue about key threats.

We give a simple example:

- **20–30 authorities, 2–5 entities from each country.** Several national authorities agree at the EU level to do a cyber stress test to assess the ransomware readiness of liquefied natural gas terminals across the EU. Each authority involved selects the 2–5 largest entities in scope of the cyber stress test. The main focus of the stress test is to understand EU-wide issues. During evaluation of the stress, good practices are shared by entities and authorities. The stress test itself and the findings trigger an union-wide dialogue about common issues, increasing the awareness about certain threats and informing authorities and policy makers about supervision priorities and policy priorities.

5. CONCLUSIONS

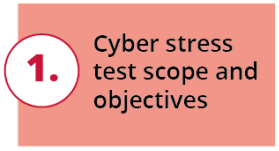
In this handbook we introduced and explained the concept of cyber stress testing, provided a step-by-step guide for stress testing and referenced various case studies and good practices.

Although stress tests are a relatively new concept in the cybersecurity domain, they are increasingly being used in other domains. Cyber stress tests can be a new tool in the regulatory toolkit of the national NIS authorities overseeing the cybersecurity and resilience of critical sectors. Experience from mature sectors, like the finance sector, where financial/economic and cyber stress tests have been carried out, shows that cyber stress tests are well suited for the supervision of complex interconnected systems, that they help to assess systemic risks, and that they can help to build up resilience together.

Cyber stress tests are becoming a new lightweight and targeted mechanism for assessing critical sector resilience, which can help understand where are the cybersecurity gaps. At ENISA, we look forward to supporting national authorities and agencies, both at national and EU level, with carrying out national or EU-level cyber stress tests.

ANNEX A: HEALTH SECTOR EXAMPLE

In this section we give a practical example of how a national authority could do a cyber stress test in the health sector, using the step-by-step guide detailed in Section 4.



In this example, the stress test will be conducted in the health sector.

- Entities in scope:
  - hospitals and large clinics;
  - health authorities, bodies and agencies nationally and in the EU;
- Critical infrastructure in scope:
  - IT assets – including workstations & laptops, network infrastructure, electronic health records systems (EHR), hospital management systems, medical imaging & picture archiving and communication systems, telemedicine & remote access platforms, cloud-based healthcare platforms,
  - OT assets – typically connected medical devices ([8]), internet of things devices ([9]), building infrastructure and utilities (e.g. heating, ventilation, and air conditioning, main power and backup systems ([10])), and emergency systems, ambulance and emergency communications.

In this example, the objectives of the stress test are defined as:

- evaluate protective measures in place to detect and prevent incidents;
- evaluate response and recovery measures, particularly the ability to maintain continuity of care and minimise the impact on patient safety;
- use findings to guide upcoming sector-specific regulations and funding priorities to strengthen the health sector cyber resilience.

In this example, the stakeholders take into account published EU health sector threat landscape reports ([11]), which indicate that the top threats in this sector are:

- ransomware affecting the IT and OT environments of hospitals;
- data-related threats, affecting patient data;
- Network intrusions, into the IT and OT environments of hospitals;
- supply chain attacks (via service providers, equipment suppliers, and managed service providers).

In this example, the national health authority decides to focus the stress test on ransomware.

The national health authority also identifies the following stakeholders for the stress test:

- the national health authority;
- the national CSIRT;
- the national cybercrime unit;
- the national public–private partnership for cybersecurity;
- the national health CSIRT;
- medical device suppliers and hospital ICT solution providers.

([8]) For example: infusion pumps, pacemakers, magnetic resonance imaging machines.
([9]) For example: smart sensors, wearables, patient monitoring systems.
([10]) For example: heating, ventilation and air conditioning units, power units.
([11]) *ENISA Threat Landscape Report – Health sector*. https://enisa.europa.eu/publications/health-threat-landscape

2. Cyber stress test design

In this example the risk scenario could be written as follows:

A ransomware attack on a hospital locks the IT network and encrypts the electronic health record. The attacker also exfiltrates sensitive patient data (protected health information, financial details) and threatens to leak it publicly unless the ransom is paid.

The first level of escalation is the compromise of connected medical devices. Using the ransomware foothold, the attacker locks down the access to multiple networked medical devices, but is still able to manage them ([12]).

The second level of escalation is a distributed denial of service attack on the hospital's external network and emergency response, disrupting online patient portals, scheduling systems and telehealth services. Emergency response systems (ambulance coordination, remote monitoring) experience severe delays.

In Section 3, we provided a detailed example of a stress test questionnaire that could be used in this setting. In the table below we give some examples of possible resilience metrics.

Assets in scope	Resilience metrics
– hospital IT network – security monitoring and logging systems (SIEM, IDS / IPS) – firewalls, routers, switches – connected medical devices	– percentage of systems covered by network security policies – average response time to detected threats – number of security events flagged per month – number of networked medical devices
– hospital and medical staff	– percentage of employees trained in phishing awareness – percentage of phishing simulations successfully detected – click rate on phishing emails in simulations
– identity and access management system – EHR system – workstations and laptops	– percentage of accounts using multi-factor authentication – number of unauthorised access attempts per month – time taken to revoke access for terminated employees
– workstations and laptops – servers hosting EHR and critical applications – storage systems	– percentage of systems updated with latest security patches – average time to apply critical security patches - endpoint security compliance rate
– security monitoring and logging systems (security information and event management, intrusion detection system / intrusion prevention system)	– mean time to detect (MTTD) security incidents – mean time to respond (MTTR) to a security incident – percentage of incidents successfully mitigated
– backup and disaster recovery systems – storage systems	– recovery time objective (RTO) – recovery point objective (RPO) – percentage of critical data successfully restored in test scenarios – does the hospital have an established ransomware response plan? – are there manual procedures for medical treatments if devices fail?

([12]) For example: infusion pumps are disabled or set to administer incorrect dosages, ventilators and heart monitors shut down or display false readings, magnetic resonance imaging and radiology equipment become inoperable, delaying diagnosis.

	– how often does the hospital test disaster recovery procedures?

3. Cyber stress test execution

In this example, the authority engages with the hospitals up front, organising a kick-off workshop with the hospital chief information security officers. The authority also prepares a 'questions and answers' webpage and, after the workshop, sends formal letters of invitation to all the targeted entities.

During the test, the authority provides additional support and guidance in the form of a real-time helpdesk / support line, and by updating the FAQ page when new questions coming in. The questions and answers page includes questions such as:

- what is the purpose of the test?
- which staff should be involved in the test?
- will our individual performance be evaluated?
- can I opt out of participating?

4. Gap analysis

In this example, the stress test is followed by identification and analysis of gaps. We give some examples of potential stress test findings for the wider sector:

- awareness vs protection: awareness is high in most hospitals, but technical measures are lacking and often insufficient. There is too much reliance on non-technical measures, on the skills of users, which are lacking in this environment.
- From IT to OT: Ransomware often starts in the office IT environment and from there can easily spread to the medical device environment, where particularly legacy ICT is at high risk.
- Weakest link: Staff and systems at the different large hospitals are closely interconnected, and a ransomware attack in one hospital can easily spread to other hospitals. Often systems are shared and staff at different hospitals use similar systems.

5. Conclusion

In this example, the stress test results in specific recommendations for hospitals. The recommendations are captured in a follow-up action plan. As a response to the stress test results, the government also triggers a national funding program, specifically for hospitals to a) implement mitigation measures against ransomware, and b) to phase out legacy ICT systems.

In this example the stakeholders also draw up lessons about the overall stress test process. The findings could be that the stress test was useful and successful and that entities want to run the stress test around a similar or different scenario in the short term.

ANNEX B: CASE STUDIES – FINANCE AND ENERGY

In this section we include two case studies of previous stress tests:

- A union stress test focusing cyber threats for the banking sector
- A union stress test focusing on hybrid threats for the energy sector.

FINANCIAL SECTOR – ECB'S 2024 CYBER RESILIENCE STRESS TEST

In 2024, 109 banks directly supervised by the ECB (109 in total) were tested to on their ability to cope with a scenario, under which all preventive measures have failed and the main core system of the bank is compromised. The set of stress tested banks covered different sizes, business models and geographical locations to capture euro- area system wide financial stability and ensure sufficient coordination with other supervisory activities.

From the 109 banks, a subset of 28 banks was chosen to undergo more extensive testing, namely to perform an actual IT recovery test and provide evidence that it had been successful. In addition, they were subject to on site audits by supervisors. The test delivered a report per tested entity describing the main gaps and weaknesses identified and proposing actions for its mitigation.

All participating banks were asked to provide feedback on ([13]).

1. The impact of the scenario:
    a. impact on key economic functions,
    b. estimated operational losses, including indirect losses;
2. The banks' response to the scenario, showing their ability to:
    a. activate their crisis response plans, including internal crisis management procedures and business continuity plans,
    b. communicate with all external stakeholders such as customers, service providers and law enforcement agents,
    c. run an analysis to identify what services would be affected and how,
    d. implement mitigation measures, including workarounds that would help the bank to operate during the time needed to fully recover IT systems;
3. The banks' ability to recover from the scenario, showing they were able to:
    a. activate their recovery plans, including restoring backed-up data and aligning with critical third-party service providers on how to respond to the incident,
    b. ensure that affected areas were recovered and up and running,
    c. implement lessons learnt, for example by reviewing their response and recovery plans.

ENERGY SECTOR – 2024 HYBRID THREAT STRESS TEST

In this case study we look in more detail at the stress test run by the Belgium SPF Economie – DG Energie ([14]) on critical infrastructure in the energy sector. The stress test aimed to evaluate how well operators respond to significant disruptions and measure their capacity to restore operations quickly and coordinate across borders effectively. The goal of the stress test was to stress test protection from both cyber and physical threats, including:

- adequacy of physical protection;
- adequacy of security management;
- ability to mitigate and resist an attack;
- ability to recover from an attack (business continuity);
- ability to continue to deliver an essential service;

([13]) Extracted from https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html.
([14]) SPF Economie – DG Energie – Haute Surveillance du Marché et Infrastructures Critiques.

- ability to communicate to authorities.

Belgium's implementation of the stress test followed the methodology proposed by the European Commission, adapted to the specific characteristics of energy networks in Belgium focusing on three resilience areas: **preparedness**, **incident response** and **recovery**. The key steps included the following elements.

Threats and scenarios: The cyber and hybrid threats in scope of the stress test included:

- Sabotage of transmission lines,
- Cyber-attacks on critical infrastructure like SCADA systems,
- Physical insider threats
- Social and political unrest

The stress test used 3 scenarios at different escalation levels: full cyber, full physical and hybrid.

- Scenario A: The current state in Europe with baseline threats, meaning low threat level, not complex, mostly physical, e.g. an attack with small firearms.
- Scenario B: Heightened threat level, with more intense cyber and physical threats, sabotage, combined with spare part shortages, some social unrest.
- Scenario C: Very high threat level, geopolitical instability, coordinated physical and cyber-attacks, large scale disruption of networks and communication, energy supply shortages, widespread social unrest.

The stress test method, and the main data collection method, was a structured open-ended stress test questionnaire, sent to the operators. The questions were divided equally into three main areas/phases: preparedness, incident management and recovery. Questionnaires were tailored for the type of entity, for example different questions for electricity and gas companies, but the resilience metrics were kept the same. Responses were evaluated quantitatively using resilience metrics, yielding an average resilience score for the entity, allowing for a comparison across the operators.

Key findings and lessons learned from the stress test: Based on the results of the stress test, the Belgian authority made several key findings:

- To mitigate extreme risk scenarios close private-public cooperation is needed.
- Cross-border and cross-sector dependencies need to be discussed and analysed better, to mitigate cascading failures effectively.
- New threats, such as drones, require that critical infrastructure operators take new specific mitigation measures.
- Re-supply and repair are key to mitigate impact in extreme scenarios, and supply chain issues need to be tackled in incident response and business continuity plans.

Belgium's stress test also resulted in several good practices and lessons learned about the stress test itself:

- Incorporating both cyber and physical threats create a more realistic and comprehensive test environment.
- Statistical comparison was not always possible because no all operators had the infrastructure being stress tested.
- Customizing questionnaires for specific infrastructures while maintaining a more generic and standard resilience indicator ensured relevant and actionable insights.
- Regular consultations and collaborative feedback improved the quality of responses and encouraged transparency.
- Operators were sometimes reluctant to share detailed security plans, impacting the depth of data collection.

REFERENCES

1. AXIOMA. Stress Testing Best Practices. available at: https://www.hvst.com/posts/stress-testing-best-practices-X7QTObdl
2. Bank of England, 2024. The Bank of England's approach to stress testing the UK banking system. Available at: https://www.bankofengland.co.uk/stress-testing/2024/boes-approach-to-stress-testing-the-uk-banking-system
3. Basel Committee on Banking Supervision, 2018. Cyber-Resilience: Range of Practices. Available at: https://www.bis.org/bcbs/qis/biiiimplmoninstr_oct18.pdf
4. Board of Governors of The Federal Reserve System, 2021. Dodd-Frank Act Stress Test 2021: Supervisory Stress Test Methodology. Available at: https://www.federalreserve.gov/publications/files/2021-april-supervisory-stress-test-methodology.pdf
5. Centraal Planbureau, 2020. A Stress Test of Dutch SMEs. Available at: https://www.cpb.nl/sites/default/files/omnidownload/CPB-Background-Document-June2020-A-stress-test-of-Dutch-SMEs.pdf
6. Cybersecurity and Infrastructure Security Agency (CISA), 2024. Infrastructure Resilience Planning Framework (IRPF) Available at: https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf
7. Danish Financial Supervisory Authority, 2024. Cyber stress testing strengthens the operational resilience of the financial sector. Available at: https://www.dfsa.dk/news/2024/nov/cyber-stress-testing
8. Department of Defense, 2018. Cybersecurity Test and Evaluation Guidebook. Available at: https://daytonaero.com/wp-content/uploads/DOD_Cybersecurity-Test-Evaluation-Guidebook-ver-2.0_25-APR-2018.pdf
9. ESMA – European Security and Markets Authority, 2017. Methodological Framework – 2017 EU-Wide CCP Stress Test Exercise. Available at: https://www.esma.europa.eu/document/methodological-framework-2017-ccp-stress-test-exercise
10. Esposito, S., Stojadinovic, B., Babic, A., Dolsek, M., Iqbal, S., Selva, J., Broccardo, M., Mignan, A., Giardini, D., 2018. A Risk-Based Multi-Level Methodology to Stress Test Critical Infrastructure Systems. Available at: https://www.earth-prints.org/server/api/core/bitstreams/b5ca3c77-578d-4a2d-a70f-030765db93fb/content
11. European Banking Authority, 2020. 2023 EU-Wide Stress Test. Available at: https://www.eba.europa.eu/risk-and-data-analysis/risk-analysis/eu-wide-stress-testing
12. European Central Bank (ECB), 2024. "ECB to Stress Test Banks' Ability to Recover from Cyberattack" – press release. Available at: https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930b0.en.html
13. European Central Bank (ECB), 2023. 2023 Stress Test of Euro Area Banks – Final Results. Available at: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.Report_2023_Stress_Test~96bb5a3af8.en.pdf
14. European Central Bank (ECB), 2023. Supervisory Review and Evaluation Process (SREP) available at: https://www.bankingsupervision.europa.eu/banking/srep/2023/html/ssm.srep202302_supervisorymethodology2023.en.html
15. European Central Bank (ECB), 2021. Macroprudential Stress Test of the Euro Area Banking System amid the Coronavirus (COVID-19) Pandemic. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4112397
16. European Central Bank (ECB), 2021. ECB Economy-Wide Climate Stress Test. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op281~05a7735b1c.en.pdf
17. European Central Bank, 2018. TIBER-EU Framework. Available at: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
18. European Central Bank (ECB), 2015. Comprehensive Assessment Stress Test Manual. Available at: https://www.ecb.europa.eu/pub/pdf/other/castmanual201408en.pdf
19. European Commission Joint Research Centre (JRC), 2016. Harmonized approach to stress tests for critical infrastructures Available at:

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC104663/jrc104663_online_05_01_ipo.pdf
20. European Commission, 2016. Harmonized Approach to Stress Tests for Critical Infrastructures Against Natural Hazards. Available at: https://op.europa.eu/en/publication-detail/-/publication/aa009c90-d6ff-11e6-ad7c-01aa75ed71a1/language-en
21. European Commission, 2014. Developing Stress Tests to Improve the Resilience of Critical Infrastructures: A Feasibility Analysis. Available at: https://ec.europa.eu/jrc/en/publication/developing-stress-tests-improve-resilience-critical-infrastructures-feasibility-analysis
22. European Insurance and Occupational Pensions Authority, 2019. 2019 Occupational Pensions Stress Test. Available at: https://www.eiopa.europa.eu/browse/financial-stability/occupational-pensions-stress-test/occupational-pensions-stress-test-2019_en
23. European Nuclear Safety Regulators Group (ENSREG), 2011. EU 'Stress Test' Specifications. Available at: https://www.ensreg.eu/sites/default/files/EU %20Stress %20Test %20Peer %20Review %20Final %20Report_0.pdf
24. European Systemic Risk Board, 2025. Handbook on cyber resilience scenario testing in the financial sector.
25. European Union (EU), 2019. Regulation on Security of Intelligent Transport Systems (C-ITS). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM %3AC %282019 %291789
26. European Union (EU), 2022. Digital Services Act (DSA). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32022R2065
27. European Union (EU), 2019. Cybersecurity Act (CSA). Available at: https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html
28. Financial Stability Board, 2020. Cyber Incident Response and Recovery Toolkit. Available at: https://www.fsb.org/2020/10/cyber-incident-response-and-recovery-toolkit/
29. International Monetary Fund (IMF), 2023. Macro-Prudential Stress Test Models: A Survey. Available at: https://www.imf.org/en/Publications/WP/Issues/2023/08/25/Macro-Prudential-Stress-Test-Models-A-Survey-537990
30. KPMG, 2024. Cyber Resilience Stress Test (CRST). Available at: https://kpmg.com/xx/en/our-insights/ecb-office/hacking-the-2024-ecb-cyber-stress-test.html
31. Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., Panda, A., 2022. Resilience Stress Testing for Critical Infrastructure. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2212420922005428?via %3Dihub https://doi.org/10.1016/j.ijdrr.2022.103323
32. National Institute of Standards and Technology, 2020. Security and Privacy Controls for Information Systems and Organizations. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
33. Pendleton, J., Levite, A., Kolasky, B., 2024. Cloud Reassurance: A Framework to Enhance Resilience and Trust. Available at: https://carnegieendowment.org/research/2024/01/cloud-reassurance-a-framework-to-enhance-resilience-and-trust?lang=en
34. Risk Business, 2024. Staying Prepared: Developments in the World of Stress Testing. Available at: https://riskbusiness.com/wp-content/uploads/2024/01/Stress-Testing-Report-Jan-2024.pdf
35. Seðlabanki Íslands, 2023. TIBER-IS Implementation Guide. Available at: https://www.sedlabanki.is/library/Skraarsafn/Fjarmalainnvidir/TIBER-IS-Implementation-Guide.pdf
36. State Bank of Pakistan, 2020. Guidelines on Stress Testing 2020 (Annexure A of FSD Circular No 01 of 2020). Available at: https://www.sbp.org.pk/fsd/2020/Annex-A.pdf
37. Tan, M., Sung Jae, P., Hazarudin, H. A., 2021. LSE SU Central Banking Society – An Introduction to Stress Testing. Available at: https://lsecentralbanking.medium.com/an-introduction-to-stress-testing-15d7e933dfc1
38. De, R., Taft, J. P., Webster, M. S., Forrester, J. P., Bisanz, M., 2020. Sound Practices for Operational Resilience Released by US Banking Regulators. Available at: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf
39. The Investment Association, 2021. Scenario Testing: Severe but Plausible. Available at: https://www.theia.org/node/32166

TP-01-25-009-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-700-9
doi: 10.2824/8248517