

Insurance cyber risk stress testing

EIOPA methodological principles summary

General overview

Scenarios

Cyber Underwriting

Cyber Resilience

Why Management Solutions?

Annex



1 | General overview

General Aspects

The EIOPA has published the Methodological principles of insurance stress testing with the aim to set the ground for an assessment of insurers' resilience under severe but plausible cyber incident scenarios, focusing on the financial consequences of such scenarios

Context



- EIOPA published in the last three years two discussion papers enriched by contributions from the insurance industry and generated three methodological papers that were used to design and operationalize the regular EU wide stress test exercises.
- In July 2023, EIOPA published the **Methodological principles of insurance stress testing - Cyber component**. This paper is the fourth of the series and contains the set of rules and guidelines to support the design phase of potential future insurance stress tests on cyber risk. The EIOPA focuses on some scenarios as the common core of events that can affect either directly the insurer, its portfolio or both: **Cloud Outage, Ransomware, Denial of Service (DoS), Data Breach** and **Power Outage**. The choice of scenarios is guided by the discussion of the implications of cyber risk for insurers, as well as a review of work already published by other supervisors.
- This document comes in the context of the **Digital Operational Resilience Regulation (DORA)**, which aims to strengthen resilience in the financial sector by establishing security requirements for network and information systems and comes into force in January 2025.

Next Steps



- EIOPA intends to complete the document in the future, developing three additional scenarios:
- Unauthorised transactions;
 - payment infrastructure hacking;
 - cryptojacking.



Risk Scenarios Applicability

- Cyber risk is the combination of the probability of cyber incidents occurring and their impact. Cyber attacks can vary in terms of motivations, methodologies and impact.
- In a traditional stress test exercise, the reference for selecting the targeted entities is their size, but in cyber stress test exercise, other elements could also be considered depending on the risks to be assessed and the information available:
- For **cyber resilience risk**, it might be useful to consider the exposure of the undertakings to critical ICT third-party service providers, the potential impact of a cyber scenario on non-insurance entities, and the number of employees as a size-based metric.
- For **cyber underwriting**, could consider the cyber insurance market coverage (i.e. affirmative) and the existence of non-affirmative exposures (i.e. silent cyber).



Main content

2 Scenarios

- Scenario selection
- Scenario narratives and specifications
- Other scenarios considered

3 Cyber underwriting

- Shocks
- Metrics
- Applications of shocks

4 Cyber resilience

- Shocks
- Metrics
- Applications of shocks



2 | Scenarios

Impact of cyber attacks against insurers



To define a cyber risk stress test scenario, the entities must consider what kind of cyber incident would be the catalyst and the risk factors. The EIOPA also outlines scenario specifications

Main scenarios (based on main cyber incidents)

Scenario	U	R	Risk factors
Data center/ Infrastructure damage (Cloud Outage)	✓	✓	<ul style="list-style-type: none"> Physical harm Negligent or accidental harmful act Dependency on cloud providers
Ransomware	✓	✓	<ul style="list-style-type: none"> Human factor Internet services Third parties / contractors
Denial of Service (DoS)		✓	<ul style="list-style-type: none"> Internet services Business-to-business platforms Dependency on cloud providers
Data Breach		✓	<ul style="list-style-type: none"> Equipment malfunction / malware Human factor Changes in IT configuration / new services deployment
Power Outage	✓	✓	<ul style="list-style-type: none"> Physical harm (fire, flood, sabotage...) Negligent or accidental harmful act, could be state-backed threat actor

Scenario narratives and Specifications

- Cyber risk scenarios can be specified at **different aggregation levels**.
 - **For cyber underwriting**, the scenario specification and the stress parameters granularity should consider the intensity of the cyber incident, its duration, and the percentage of infected policyholders.
 - **For cyber resilience**, the stress parameters granularity would also depend on the intensity of the cyber incident and its duration, as well as on the percentage of operational units infected.
- There are another important considerations relate to the description of potential scenarios for the various categories of cyber incidents:
 - In the scenario of **Cloud Outage**, loss of part or of the entire IT infrastructure supporting business operations can be caused by natural disaster, misconfiguration affecting service providers, or by sabotage.
 - A **ransomware** attack, encrypts computers and spreads throughout the organization.
 - In the **DoS** scenario, a coordinated attack is launched against the players in the financial sector, which causes the unavailability of entire customer databases, as well as a certain number of hours of system downtime.
 - In **Data Breach** scenario, malicious actors have infiltrated an organization's network and have managed to extract sensitive data.
 - **Power Outage** can be caused by a threat actor exploiting vulnerabilities in the regional/national electricity sector and grid systems, or by a grid failure.

3 Cyber underwriting Shocks



The shocks are based on the EIOPA framework, with respect to the nature, estimation and assessment of impacts, and there are three scenarios applicable on cyber underwriting risk

- **Cyber underwriting** risk is intended as the capability of an insurance undertaking to sustain by a capital and solvency perspective the financial impact of the materialization of an extreme but plausible adverse cyber scenario impacting the insurance coverages contained in the liability portfolios.
- Shocks are the impacts or consequences generated by the cyber events. The consequences of a cyber event can be traced back to an increase in claims deriving by higher frequency and, or higher costs.
- The shocks application and the calculation of the impacts should rely on as much as possible on the **EIOPA framework** for stress testing with respect to the **nature of the shocks, estimation and evaluation of the impacts and the Solvency II framework**. Shocks and specifications are presented for **Cloud Outage, Ransomware & Power Outage scenarios** by product line or guarantee. The DoS and Data Breach scenarios are not discussed due to a lower expected impact in terms of claims.
- Cyber underwriting scenarios are expected to be applied at a **granular level for individual insurance products and policyholders**. For most products, the different shocks will impact frequency and/or severity of the total insurance claims.
- A general distinction can be made between **affirmative cyber and silent cyber**. For affirmative cyber, the insurance undertaking offers an explicit cyber coverage to its policy holder. For silent cyber, the coverage of cyber is implicit due to imprecise policy wording or by not explicitly including or excluding cyber as a covered risk.

Overview of the different product lines or guarantees impacted are presented as well as an overview of the potential shocks for each scenario

PRODUCT LINE OR GUARANTEE	SHOCKS BY SCENARIO		
	Cloud Outage	Ransomware	Power Outage
All products (non-life)	Market share impacted cloud Duration of the outage of the cloud infrastructure	Infection rate	Geographical location risk Duration of the power outage
(Contingent) Business Interruption	Average duration interruption Loss in profit per day	Average duration interruption Loss in profit per day	Average duration interruption Loss in profit per day
Crisis service costs	Average cost IT forensics Average cost Notification	Average cost IT forensics Average cost Notification	Average cost IT forensics Average cost Notification
Recovery expenses	Recovery expenses	Recovery expenses	Recovery expenses
Professional Indemnity	Average cost per claim	Average cost per claim	Average cost per claim

3 Cyber underwriting Metrics



Metrics are used to measure the degree of cyber underwriting and the aim is to provide a comprehensive overview of the major drivers behind the impact of the prescribed scenarios

- Metrics are used to assess and measure the impact of shocks on an insurance undertaking. The metrics provide a comprehensive overview of the major drivers behind the impact of the prescribed scenarios on the Solvency II Balance Sheet and on the Profit and Loss of the participants of stress test.
- The metrics should account for both **silent and affirmative coverages** in terms of baseline and stressed exposures.
- Scenarios will have the common goal of the assessment of the change in **Balance Sheet, Own Funds, SCR, SCR Ratio** as consequences of shocks that were applied.
- The clear **identification of the exposures to affirmative cyber coverages** (both on a standalone basis and with cyber as an add-on coverage) allows a clear estimation of the impacts stemming from a potential increase in frequency and severity of the claims against the prescribed scenarios.

METRIC	DESCRIPTION
Change of gross and net total product for affirmative cyber products	Baseline vs Adverse. Assuming a full reserving of the claims. To be reported separately for: <ul style="list-style-type: none"> • cyber standalone coverages • products with cyber as add-on coverage but main risk being covered • products with cyber as add-on coverage and not as main risk being covered
Change of gross and net claims paid for affirmative cyber products	Baseline vs Adverse. Assuming a full payout of the claims. To be reported separately for: <ul style="list-style-type: none"> • cyber standalone coverages • products with cyber as add-on coverage but main risk being covered • products with cyber as add-on coverage and not as main risk being covered
Change of gross and net total product claims for non-affirmative cyber products	Calculation by participant or estimation. Baseline vs Adverse. Assuming a full reserving of the claims.
Change of gross and net claims paid for non-affirmative cyber products	Baseline vs Adverse. Assuming a full payout of the claims.

4 | Cyber resilience Shocks



The consequences of a cyber event can be related to an increase in operational and other costs associated to business and to detection and recovery costs

- **Cyber resilience** is the capability of an insurance undertaking to sustain the operational and financial effect of an adverse cyber-event. Cyber attacks can cause to the insurer direct financial losses or indirect financial losses due to unavailable systems, restoration and loss of reputation.
- The application of cyber resilience shocks and the calculation of the impacts should rely as much as possible on the EIOPA framework for stress testing with respect to **estimation of the impacts** (fixed balance sheet), **evaluation of the impacts** (Solvency II balance sheet) and to **the Solvency II framework**.
- The costs of cyber-attacks against insurers have an impact on the profit and loss and balance sheet of the affected companies.
- Cyber resilience shocks and their specification are presented for all the five scenarios in the scope of this paper.
- Table lists the possible shocks for all the scenarios considered in the cyber resilience component. Shocks are linked to the downtime of the relevant infrastructures or systems affected by the cyber event and the type of business processes affected.
- In cyber resilience, the shocks are not divided by product lines or guarantees because the impacts of cyber risk are generated in the organization, not in the products or services offered by it.

SHOCKS BY SCENARIO				
Cloud Outage	Ransomware	DoS	Data breach	Power Outage
Outage time	Business processes affected Penalty factor on recovery times	Business processes affected Outage time	Percentage of sensitive data breached	Outage time

4 | Cyber resilience Metrics



The purpose of the operational metrics is to measure the impact of an adverse cyber scenario on the continuity of critical business services

- To assess and measure the degree of cyber resilience, **operational and financial metrics should be used**. The purpose of the **operational metrics** is to measure the impact of an adverse cyber scenario on the continuity of critical business services. **Financial metrics** assess the impact on the insurer profit and loss and balance sheet.
- Contrary to the cyber underwriting, work to assess the impact of cyber resilience scenarios is still incipient and more initiatives are needed to develop common cyber resilience metrics.

	METRIC	DESCRIPTION
Operational	Time elapsed until return to business as usual (time to BAU)	Adverse Average time to restore operations after the shock, i.e. mean time elapsed between initial notification and resuming normal level of operations.
	Business processes affected	Adverse List of business processes that are affected by the attack.
Financial	Operational and other costs (change of)	Baseline vs Adverse Operational and other costs should comprise business interruption costs, including loss of revenue corresponding to lost business during the downtime, and detection and recovery costs.
	Change of total assets	Baseline vs Adverse (in case of payout)
	Change of total liabilities	Baseline vs Adverse (in case of provisioning)

5

Why Management Solutions?

Management Solutions has more than 10 years of experience supporting entities in the development of stress test, including extensive experience in cyber resilience stress testing in financial undertakings

Kind of collaborations in cyber resilience stress testing

- **Survey and definition of calculations, development and architecture of modules and components**, and implementation of the planning and budgeting model.
- **Conducting** (data processing, segmentation, mapping, aggregation and analysis of results) and **coordinating internal capital self-assessment exercises** (e.g. Capital Self-Assessment Report) and **specific supervisory stress tests** (e.g. EBA stress test exercise).
- **Definition** and implementation of a **risk scenario and projection** analysis framework.
- **Design of the governance** to be applied in the generation and use of **macroeconomic scenarios** to be used in capital planning and stress testing exercises.
- **Definition** of the framework and **establishment of a plan** for the **implementation/improvement** of a **robust planning and stress process**, which allows compliance with regulatory and management requirements and meets the established governance.
- **Development of projection models** to be used in capital planning and stress testing exercises in the areas of: balance sheet, income statement, credit losses, operational losses, market risk, ALM and economic capital.
- Support to Internal Validation in the **review of the models** used in the exercise (credit loss, balance sheet, income statement, operational models, etc.) as well as in the **validation of the exercise process**.
- Implementation of a model for **validating the quality** of the data used to carry out the exercise (repositories, information flows).
- Identification of **information needs, design and documentation of procurement processes** for the implementation of planning exercises.
- Development and implementation of **both ad-hoc and proprietary tools** in the field of planning, scenarios, projections and stress.
- **Definition** of the **criteria for coordination** of **Capital Planning exercises** with other types of exercises such as **Risk Assessment, Risk Appetite or business strategy**.
- **Documentation of the complete capital planning** and stress testing process, including the areas responsible, functions, inputs and outputs of the process, methodologies used and controls defined.
- PMO for the **coordination of activities and monitoring of the different areas responsible** for carrying out capital planning and stress testing exercises.

5 | Why Management Solutions?

In this regard, Management Solutions has a multi-sectoral and in-depth knowledge of key stakeholders, as well as strong capabilities to achieve practical results in an agile manner...

Digital
Operational
Resilience
Experience
(DORA)

- **Diagnostic** projects of the **level of adequacy** of different **entities** with respect to the **regulatory requirements** set by **DORA**
- **Normative knowledge** to give understanding to the different stakeholders of the organisation (internal and external) **on Digital Operational Resilience**
- **Detailed knowledge of the regulations** and **analysis of new updates** in the final publication of the document prior to its adoption
- **Detection of gaps and establishment of lines of improvement to comply with regulatory requirements** and development of **master plans**
- **Establishment of PMOs to ensure** the correct implementation of master plans on **DORA compliance**
- **Adjustment of the Master Plan** based on technical standards already published under public consultation (RTSs and ITSs)
- **Accompaniment** in the **inspection process of supervisors** in the field of **Cyber Resilience** (compilation of the CROE questionnaire, collection of evidence, etc.)

Proven
experience in IT
Risk and related
projects

- **Trusted advisor in the implementation of risk & control models** (Info&Data Sec., Physical Sec., Third Party, Technology, Data Mgmt., Processes, Finance, People...)
- **Methodology and framework analysis** (COBIT, ICT, NIST, ITIL, SANS...) Improvements paths identification and control frameworks definition
- **Extensive experience in regulatory compliance projects, evolution and evaluation of compliance models**
- **Supporting organisations in their review of processes, stakeholders, systems, etc. where the main sources of risk are located**
- **In-depth knowledge of IT areas, technology platform (legacy and next gen) and active projects** in the main fields of action

High-value
profiles,
expertise and
cross vision

- Professionals with strong **understanding, communication, challenge/advice skills, expertise in Technology Risks & Cybersecurity, & their relationship with risk & process management (cross vision)**
- **Understanding of business processes, knowledge of risk management methodologies & analytical capabilities**
- **Detailed knowledge of regulations and best practices in market**

Flagship firm
with global
capabilities

- **Global firm, independent and international** (+40 countries), with in-depth knowledge of the businesses in which our clients operate (+1500 global and local), selecting the most appropriate resources for each project, regardless of where they are located
- **Multidisciplinary team** with strong analytical capabilities and specialist knowledge. Organised on a matrix basis (customer, industry, competitor and geography)
- Consultant accredited by **supervisors and supranational bodies** (ECB, FCA, PRA, EIOPA, MEDE/ESM, WB...)
- **Strong corporate culture**: commitment, dedication to service and constant pursuit of excellence
- **Proven track record**: proven delivery capacity, which has been substantiated by significant organic growth (x38 in 20 years)
- **Benchmarking** capability (presence with Top IT customers in all geographies)

Access to
regulatory and
supervisory
criteria

- We accompany **supervisors in their on-site inspections** in organisations
- **We directly support organisations in successfully passing the processes of on-site supervision, internal and external audit**, in terms of ICT risks
- **Office in Frankfurt as Hub for regulatory analysis and liaison with the regulator** for regulatory issues, queries and anticipating requirements

A | Annex

Cyber underwriting: Applications of shocks

The paper includes a set of practical applications of the shocks to the risk of cyber underwriting

SCENARIOS	EXAMPLES OF APPLICATIONS
Cloud Outage	<ul style="list-style-type: none"> • Share of policyholders affected (% of total policyholder per affected business-line. Concentration rate can increase the number of affected policyholders) • Average duration interruption in days • Loss in profit per day (Revenue loss per day in euros) • Recovery expenses
Ransomware	<ul style="list-style-type: none"> • Share of policyholders affected (Infection rate % of total policyholder per affected business-line). • Share of policyholders that opt to pay ransom (% of affected policyholders that have ransom coverage that opt to pay the ransom) • Ransom amount • Average duration interruption • Loss in profit per day (Revenue loss per day in euros) • Recovery expenses
Power Outage	<ul style="list-style-type: none"> • Share of policyholders affected (% of total policyholder per affected business-line. Concentration rate, based on the geographical location of the power outage, can increase the number of affected policyholders) • Average duration interruption • Recovery expenses

A | Annex

Cyber resilience: Applications of shocks

The paper proposes a set of practical applications of the shocks to the risk of cyber resilience

SCENARIOS	EXAMPLES OF APPLICATIONS
Cloud Outage	<ul style="list-style-type: none"> • Outage time dependent on whether: i) the data center is an internal infrastructure operated by the company; or ii) an infrastructure provided by a specialized vendor (Microsoft, Amazon, Google...).
Ransomware	<ul style="list-style-type: none"> • Business processes affected (List of business processes that are disabled and need to be restored). • Penalty factor on recovery times (Factor reflecting the potential longer time of recovery due to encrypted backups and configurations, to be multiplied by the expected time to BAU (factor >1)).
Denial of Service (DoS)	<ul style="list-style-type: none"> • Business processes affected (List of business processes that are disabled and need to be restored). • Outage time (The amount of time in hours until the affected services are available again).
Data breach	<ul style="list-style-type: none"> • Percentage of sensitive data breached (Percentage of sensitive data that are breached after the attack).
Power Outage	<ul style="list-style-type: none"> • Outage time (Period during which the power is out, and the undertaking's operations are interrupted in hours).

A | Annex

Abbreviations

ALM	Assets and Liabilities Management
BAU	Business As Usual
DORA	Digital Operational Resilience Regulation
DoS	Denial of Service
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
IT	Information Technology
PMO	Project Management Office
SCR	Solvency Capital Requirement


MS^o


Management Solutions

Making things happen


International
One Firm


Multiscope
Team


Best practice
know-how


Proven
Experience


Maximum
Commitment

Marcos Fernández Domínguez
Partner at Management Solutions
marcos.fernandez.do1@managementsolutions.com

Jorge Monge Alonso
Partner at Management Solutions
jorge.monge.alonso@managementsolutions.com

Marta Hierro
Partner at Management Solutions
marta.hierro@managementsolutions.com

© Management Solutions, 2023

All rights reserved. Cannot be reproduced, distributed, publicly disclosed or transformed, whether totally or partially, free of charge or at no cost, in any way or by any means, without the express written authorization of Management Solutions.

The information contained in this publication is merely to be used as a guideline, is provided for general information purposes and is not intended to be used in lieu of consulting with our professionals. Management Solutions is not liable for any use that third parties may make of this information. The use of this material is not permitted without the express authorization of Management Solutions.

For more information please visit

www.managementsolutions.com

Or follow us at: 