

Insurance Stress Test 2022

Flashing light provision & Cyber Underwriting Stress Test

19 April 2022

Introduction

- ◆ Stress test framework for the insurance sector (communication NBB_2017_06)
- ◆ The NBB's stress test exercises are carried out within this framework.
 - ◇ 2016: EIOPA stress test
 - ◇ 2017: NBB + IMF stress test
 - ◇ 2018: NBB + EIOPA stress test
 - ◇ 2019: NBB stress test
 - ◇ 2021: NBB + EIOPA stress test
 - ◇ 2022: NBB stress test

Insurance Stress test 2022

	Scenarios	Objectives
Cyber Underwriting Stress Test	1. Business Blackout 2. Ransomware Attack	Standalone cyber scenario
	3. Cloud Outage leading to bursting of tech bubble	Cyber + financial With optional reactive management actions (compulsory if SCR ratio falls below the risk appetite)
Low yield	Low for long scenario incl. SII Review SCR IRR (COM Proposal)	Exemption of the flashing light provision

Timing Insurance Stress test 2022

- ◇ 19 April Pre-launch + Stress Test Event (with QAs until 29 April)
- ◇ 16 May Stress test launch
- ◇ Mid June Discussion with undertakings concerning silent cyber
- ◇ 12 August Deadline for the submission of results
- ◇ September Deadline validation meetings & resubmissions
- ◇ End Dec. Publication of NBB stress test results

Low Yield Scenario

Technical specifications - Scenario

Low Yield (LY) scenario

The application of the low yield scenario requests stress test participants to calculate the impact of a stressed risk-free rate curve (see below) on their financial situation.

Same scenario as in 2021

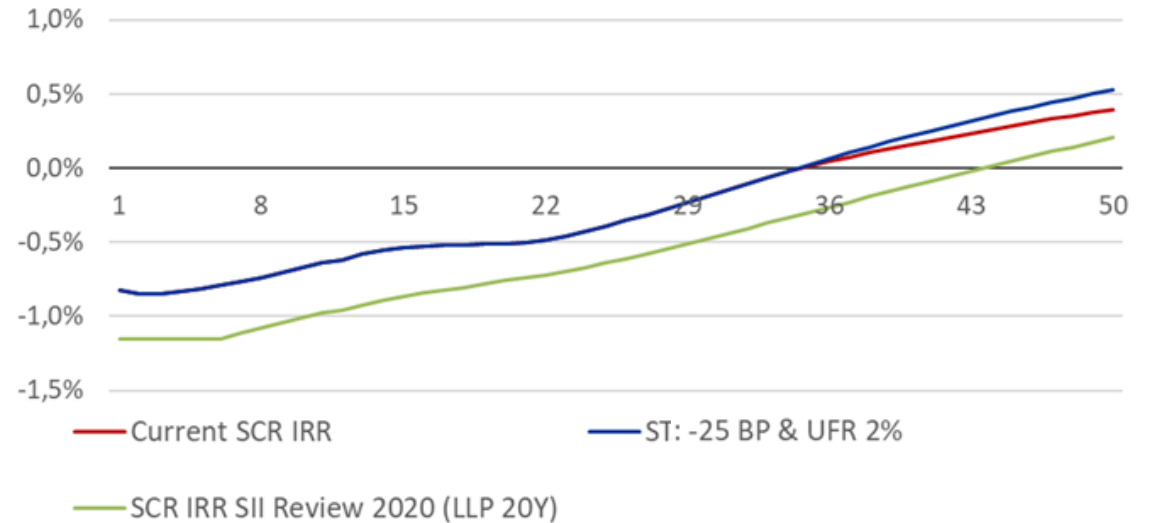
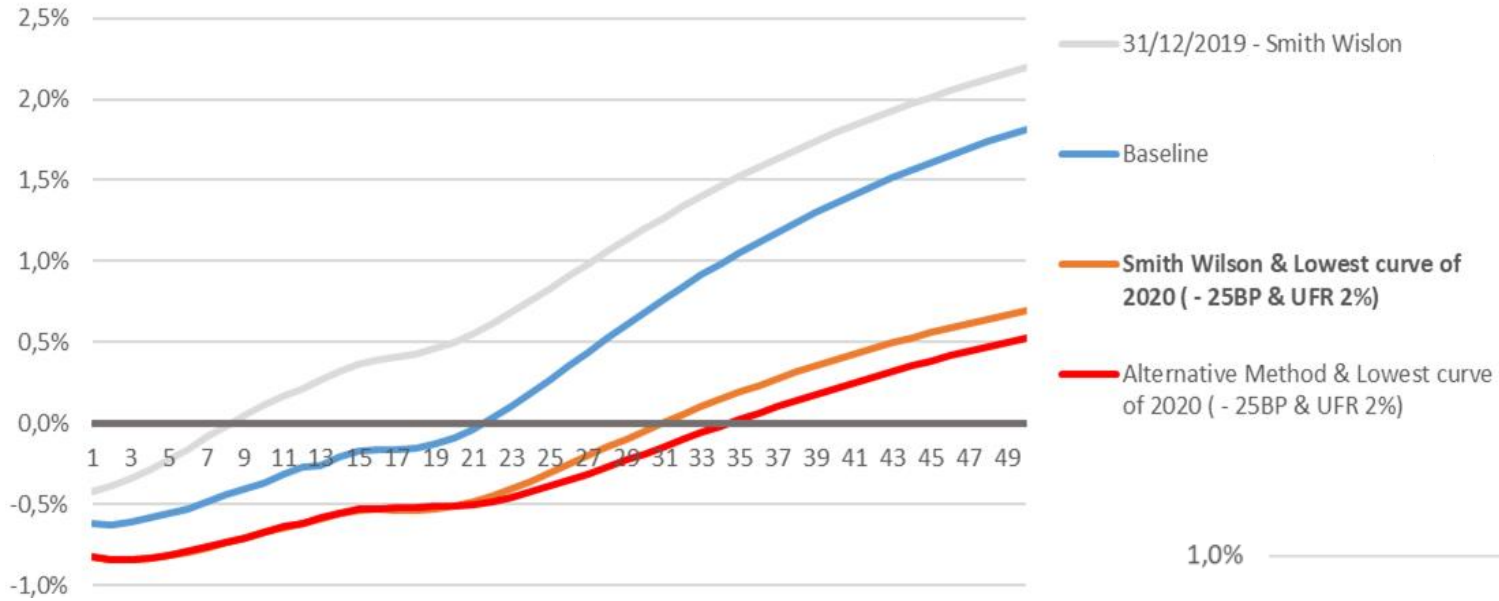
Recalculation of SCR IRR

The second step requires the recalculation of the SCR interest rate risk as proposed in *the Opinion on the 2020 review of Solvency II* (EIOPA-19/451) published by EIOPA on the 11 September 2019.

Low Yield Scenario

Technical information

NBB Stress Test - Scenario



Low Yield Scenario

Technical specifications - Methodology

- The scenario is designed as an **instantaneous** shock
- **All interest rate sensitive assets and liabilities** shall be revalued using the stressed interest rate term structures
- The post-stress figures shall be generated coherently with the models applied for Solvency II valuation purposes
- **Simplifications** in the calculation of the stress test can be used only if they have an insignificant economic impact. Undertakings applying simplifications should inform, via IST@nbb.be, the NBB prior to the submission of results

Exemption contribution to the flashing light provision

Conditions to be exempted from the mandatory contribution to the flashing light provision are outlined in the Royal Decree financial statements (art.34quinquies) and circular letter NBB_2016_39

- ◆ **The exemption file, the assessment of which consists to a large extent of the results of the stress test, shall also be submitted to the Bank by 12 August 2022**
- ◆ SCR ratio > 100% without transitional measures
- ◆ The NBB can impose additional conditions for the recognition or preservation of the exemption, when necessitated by the condition of the undertaking and the market

→ Result of 2021 Stress test will be an important element when assessing the conditions to be exempted from the mandatory contribution to the flashing light provision

Cyber as emerging risk

- Increasing number of cyber events observed
- Geopolitical tensions lead to increase in (state-sponsored) cyber incident
- Ransomware-as-a-Service reduces need for IT skills
- Strong increase in cyber insurance, but still modest in size
 - IAIS expects 400% increase of global market towards 2025
 - BE currently 3rd cyber insurance market in EU after FR and DE

Cyber attack shuts major US pipeline system

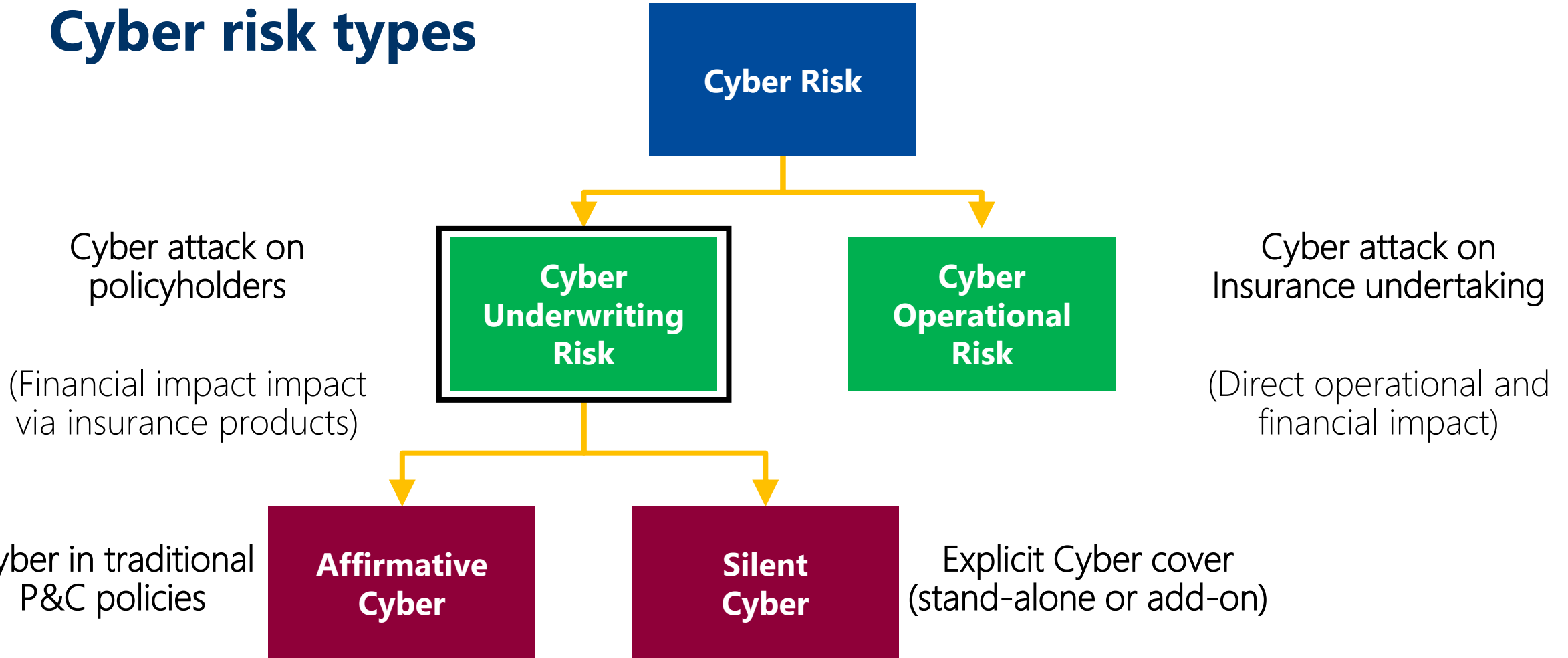
Assault on Colonial Pipeline underscores vulnerabilities in critical US infrastructure

Source: Financial Times, May 8, 2021

Ukraine says it thwarted Russian cyberattack on electricity grid

Source: Reuters, April 12, 2022

Cyber risk types



NBB analyses




- Survey on cyber risk
 - Affirmative cyber: Increasing interest for cyber insurance products
 - Silent cyber: Often still incorporated in traditional policies
- Deep-dive analysis
 - Silent cyber: Mostly in General Liability, Property and Business Interruption
 - Accumulation risk: Concentration of IT service providers used by policyholders
- 2022 Insurance Stress-test
 - First horizontal quantification for cyber underwriting risk
 - Focus on silent cyber and accumulation risk

Assumptions cyber stress-test

	Financial stress-test	Cyber underwriting stress-test
Macro-level assumptions	Stressed financial parameters common to all undertakings	Cyber scenario definition common to all undertakings
Micro-level assumptions	Individual valuation assumptions (e.g. profit sharing in Best Estimate)	<u>Individual or optional default</u> valuation assumptions (e.g. propensity to pay ransom)

- Undertakings have very different claims management and underwriting experience in this recent product line
- Optional micro-level assumptions provided based on historical claims and cyber incident data

Cyber Underwriting Stress Test

	Business Blackout	Ransomware Attack	Cloud Outage																		
																					
Scenario	Cyber attack on electricity infrastructure in largest underwritten country	Ransomware attack like WannaCry across undertakings	Outage of largest cloud service provider across all datacentres																		
Cyber Stress	Blackout with downtime till 24h	Ranswomware attack on 10% portfolio with 300.000 EUR ransom and 17 to 25d interruption	Cloud Outage of 3 days and business up after 14 to 22 days																		
Impacted Lines of Business	<ul style="list-style-type: none"> • Business interruption (BI) • Contingent BI • Property (spoiled goods) • General Liability (D&O, E&O, PI, Med Mal, Product etc.) 	<ul style="list-style-type: none"> • Business Interruption (BI) • Contingent BI • Cyber extortion • Incident Response Cost • Data and Software Loss • General Liability (D&O, E&O, PI, Med Mal, Product etc.) 	<ul style="list-style-type: none"> • Business interruption (BI) • Contingent BI • Incident Response Cost • Data and Software Loss • General Liability (D&O, E&O, PI, Product etc.) 																		
Financial Stress			<p>Tech bubble burst</p> <table border="1"> <thead> <tr> <th></th> <th>Cloud-using sectors</th> <th>Other Sectors</th> </tr> </thead> <tbody> <tr> <td>Sovereign bond yield (OLO)</td> <td colspan="2">-23bps</td> </tr> <tr> <td>Corporate bond yield (AA)</td> <td>+80bps</td> <td>+64bps</td> </tr> <tr> <td>Corporate bond yield (BBB)</td> <td>+105bps</td> <td>+71bps</td> </tr> <tr> <td>Equity (EUR)</td> <td>-56%</td> <td>-38%</td> </tr> <tr> <td>Commercial Real Estate</td> <td colspan="2">-20%</td> </tr> </tbody> </table>		Cloud-using sectors	Other Sectors	Sovereign bond yield (OLO)	-23bps		Corporate bond yield (AA)	+80bps	+64bps	Corporate bond yield (BBB)	+105bps	+71bps	Equity (EUR)	-56%	-38%	Commercial Real Estate	-20%	
	Cloud-using sectors	Other Sectors																			
Sovereign bond yield (OLO)	-23bps																				
Corporate bond yield (AA)	+80bps	+64bps																			
Corporate bond yield (BBB)	+105bps	+71bps																			
Equity (EUR)	-56%	-38%																			
Commercial Real Estate	-20%																				

Business Blackout

- **Definition:**

- A threat actor makes use of vulnerabilities in the electricity sector and grid systems leading to a power outage.
- The electricity load shedding plan (i.e. *afschakelplan voor elektriciteit* or *plan de délestage de l'électricité*) is activated.
- Power is shut down power across the 8 Belgian areas and even the areas outside the plan
- Suspected state-backed threat actor, but not proven so no war clauses triggered

- **General, required assumptions:**

- **Power outage in largest country underwritten:**
 - First phase: Gradual load shedding and shutting down power during 14h
 - Second phase: Gradual restoring of power starting during 24h
 - After 4 hours, 50% of businesses and families.
 - After 16 hours, 75% of business and families
 - After 24 hours, the entire country has regained power
- On average 17h of power loss of insured businesses, suppliers and critical vendors
- Silent cyber should be captured unless explicitly excluded in insurance policies



Business Blackout

- **Additional, optional assumptions:**
 - Average crisis service costs of 60.000 EUR per business
 - Average recovery expense costs of 40.000 EUR per business
 - Average claims cost per policyholder for impacted products and LoBs

- **Insurance losses from Cyber Insurance, General Liability, Business Interruption and Property damage:**
 - Power Generation and Distribution Companies
 - Defendant companies
 - Companies with energy loss
 - Companies with indirect damage due to suppliers
 - Homeowners
 - Specialty (event cancellation)



Ransomware Attack

- **Definition:**

- Threat actor exploits a vulnerability in a worldwide used mail server to deliver a ransomware attack across the world.
- Encryption of files of the infected enterprises to motivate them to pay the ransom.
- Undertakings with recent back-ups do not pay the ransom and restore data and software.
- Other undertakings pay the ransom, but are forced to restore data and software from a back-up nonetheless.
- Suspected state-backed threat actor, but not proven so no war clauses triggered

- **General, required assumptions:**

- Ransomware spreads around the world and **infects 10% of policyholders and triggers 10% of Contingent Business Interruption policies.**
- On average, victims experience **22 days of system downtime.**
- For businesses with back-up and incident response plans **downtime is lower at 14 days on average.**
- An **average ransom of 300.000 EUR** is paid out by the companies.
- Silent cyber should be captured unless explicitly excluded in insurance policies



Ransomware Attack

- **Additional, optional assumptions:**

- Average crisis service costs of 60.000 EUR per business
- Average recovery expense costs of 40.000 EUR per business
- Businesses choose to pay the ransom in 93% of cases.
- The revenue loss for Business Interruption can be estimated per economic sector as followed:
- Average claims cost per policyholder for impacted products and LoBs

- **Insurance losses from Cyber Insurance, General Liability, Business Interruption and Property damage:**

- Companies directly impacted
- Companies indirectly impacted
- Defendant companies



Economic sector (NACE code)	Revenue loss Ransomware
A - AGRICULTURE, FORESTRY AND FISHING	15%
B - MINING AND QUARRYING	
D - ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY	
J - INFORMATION AND COMMUNICATION	
O - PUBLIC ADMINISTRATION AND DEFENCE; COMPULSORY SOCIAL SECURITY	
S - OTHER SERVICE ACTIVITIES	20%
E - WATER SUPPLY; SEWERAGE, WASTE MANAGEMENT AND REMEDIATION ACTIVITIES	
F - CONSTRUCTION	
N - ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES	
T - ACTIVITIES OF HOUSEHOLDS AS EMPLOYERS	
U - ACTIVITIES OF EXTRATERRITORIAL ORGANISATIONS AND BODIES	25%
C - MANUFACTURING	
G - WHOLESALE AND RETAIL TRADE; REPAIR OF MOTOR VEHICLES AND MOTORCYCLES	
H - TRANSPORTATION AND STORAGE	
I - ACCOMMODATION AND FOOD SERVICE ACTIVITIES	
K - FINANCIAL AND INSURANCE ACTIVITIES	
L - REAL ESTATE ACTIVITIES	
M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	
P - EDUCATION	
Q - HUMAN HEALTH AND SOCIAL WORK ACTIVITIES	
R - ARTS, ENTERTAINMENT AND RECREATION	

Cloud Outage



- **Definition:**

- Misconfiguration in global cloud service provider goes undetected and is followed by a cyber attack which leads to a failure across all datacenters.
- Platform and Software providers also observe an outage.
- Enterprises making use of the cloud services have business interrupted.
- Due to the longer-term cloud outage, the financial markets loose confidence in this global IT service provider leading to burst of the bubble for technology and cloud dependent sectors.
- This financial downturn also impacts other economic sectors albeit to a lesser extent.

- **General, required assumptions:**

- **Largest cloud service provider in the portfolio goes down for 3 days**
- On average, PaaS & SaaS providers and companies experience **8 days of downtime**
- Businesses experience on **average 25 days of business interruption.**
- **Average business interruption is lower at 17 days** for businesses with back-up and incident response plans.
- **Combined with market stress** triggered by loss of confidence in technology sector (IR down and Equity shocks)
- Silent cyber should be captured unless explicitly excluded in insurance policies

Cloud Outage



- **Additional, optional assumptions:**

- Average crisis service costs of 60.000 EUR per business
- Average recovery expense costs of 40.000 EUR per business
- If no detailed data on the cloud service providers of their policyholders is available, it can be assumed that 32% of its policyholders are impacted and 32% of the coverages for Contingent Business Interruption are triggered.
- The revenue loss for Business Interruption can be estimated per economic sector as followed:

- **Insurance losses from Cyber Insurance, General Liability, Business Interruption and Property damage:**

- Companies directly impacted
- Companies indirectly impacted
- Defendant companies

Economic sector (NACE code)	Revenue loss Cloud outage
A - AGRICULTURE, FORESTRY AND FISHING	5%
B - MINING AND QUARRYING	
D - ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY	
C - MANUFACTURING	15%
H - TRANSPORTATION AND STORAGE	
I - ACCOMMODATION AND FOOD SERVICE ACTIVITIES	
J - INFORMATION AND COMMUNICATION	
O - PUBLIC ADMINISTRATION AND DEFENCE; COMPULSORY SOCIAL SECURITY	
R - ARTS, ENTERTAINMENT AND RECREATION	
S - OTHER SERVICE ACTIVITIES	
E - WATER SUPPLY; SEWERAGE, WASTE MANAGEMENT AND REMEDIATION ACTIVITIES	25%
F - CONSTRUCTION	
N - ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES	
T - ACTIVITIES OF HOUSEHOLDS AS EMPLOYERS	
U - ACTIVITIES OF EXTRATERRITORIAL ORGANISATIONS AND BODIES	35%
G - WHOLESALE AND RETAIL TRADE; REPAIR OF MOTOR VEHICLES AND MOTORCYCLES	
L - REAL ESTATE ACTIVITIES	
M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	45%
P - EDUCATION	
K - FINANCIAL AND INSURANCE ACTIVITIES	
Q - HUMAN HEALTH AND SOCIAL WORK ACTIVITIES	

Cloud Outage

Bursting of tech bubble and financial downturn

This mixed scenario originates from a cloud outage, with severe repercussions on the financial markets.

Market shocks: Higher shock for sectors sensitive to cloud outage, given by the following NACE Codes (Equity & Corporate bonds):

- K - Financial and insurance activities
- J - Information & Publication
- C21 - Manufacture of basic pharmaceutical products and pharmaceutical preparations
- M - Professional, scientific and technical activities
- C26 - Manufacture of computer, electronic and optical products
- N - Administrative and support service activities
- I - Accommodation and food service activities

Swap rates - The ultimate forward rate (UFR) is set at 3.45% for Euro in line with the current Solvency II regulation.

Bond yields - Based on ratings/countries/Sector

Equity prices (-38% for European Union → 56% for sectors sensitive to cloud outage)

Real estate prices – residential (-7,1% for EU) and office & commercial (-20% for EU)

Reactive management actions are optional:

- However, if the company's SCR ratio falls below its risk appetite, it is expected that reactive management actions will be implemented to eventually restore the situation, at least partially.

Questionnaire – Only for Cyber Stress Test

Participants shall submit the questionnaire via mail to ist@nbb.be

I. Simplifications and approximations: This section focuses on information regarding potential deviations from regular reporting, along with relevant details. On the cyber-specific elements, the undertaking is asked to describe:

- The methodology used to estimate the impact of the scenario on affirmative and silent covers.
- If it used the optional assumptions and if not, what assumptions were made.

II. Reactive management actions (only if applied): Participants are requested to identify the management actions and their triggering shocks as well as on the underlying rationale for participating entities to select them

III. Assessment and impact of the Stress Test: The information requested in this section relates to the impact of the stress on the Assets over liabilities, SCR, Deferred taxes, LTG and transitional measures.

The participating entities are also invited to submit:

- their own overall assessment on the impact of the scenario
- information on the internal process run by participants to produce the results.

Reporting

Results shall be submitted through OneGate.

- For information purposes only, a mock spreadsheet (excel file) containing all reporting templates is provided.
- Low yield Scenario :
 - Basecase (pre-filled)
 - After stress
- Cyber Scenario
 - Basecase (pre-filled)
 - After stress - No management action
 - After stress - Constrained reactive management actions (only if applied)

Reporting: Balance sheet, LTG, OF, SCR (Standard Formula / Partial internal model / Full internal model) + SCR Market (only for low yield scenario) + Cyber impact and Cyber Accumulation

Thank you for your attention

Questions?

Appendix 1

Reporting Template - low yield

Templates				Scenario
Content	Title	Origin	Prefilled	Low Yield
Information				
General information	Information	IST2022 specific	Not prefilled	
Overview of sheets	Index	IST2022 specific	Not prefilled	
Participant information				
Participating entity information	Participant.Basics	IST2022 specific	Not prefilled	X
Base case (pre-stress)				
Balance sheet	0.BS	QRT-based	Prefilled	
Long-term Guarantees	0.LTG	QRT-based	Prefilled	
Own funds	0.OF	QRT-based	Prefilled	
SCR - for undertakings using SF	0.SCR.SF	QRT-based	Prefilled	
SCR - for undertakings using PIM	0.SCR.PIM	QRT-based	Prefilled	
SCR - for undertakings using full IM	0.SCR.IM	QRT-based	Prefilled	
SCR - Market risk	0.SCR.MKT	QRT-based	Prefilled	
Low Yield (LY) scenario				
Balance sheet	LY.BS	QRT-based	Not prefilled	X
Long-term Guarantees	LY.LTG	QRT-based	Not prefilled	X
Own funds	LY.OF	QRT-based	Not prefilled	X
SCR - for undertakings using SF	LY.SCR.SF	QRT-based	Not prefilled	X
SCR - for undertakings using PIM	LY.SCR.PIM	QRT-based	Not prefilled	X
SCR - for undertakings using full IM	LY.SCR.IM	QRT-based	Not prefilled	X
SCR - Market risk	LY.SCR.MKT	QRT-based	Not prefilled	X

Appendix 2

Reporting Template – Cyber Stress Test

Description	Baseline (0)	Scenario without reactive management actions - Fixed Balance Sheet (FBS)	Scenario with reactive management actions - Constrained Balance Sheet (CBS)*
General information	Participant		
Balance sheet reporting template as per QRT data	0.BS	FBS.BS	CBS.BS
Impact of long term guarantees measures and transitionals as per QRT data	0.LTG	FBS.LTG	CBS.LTG
Own funds as per QRT data	0.OF	FBS.OF	CBS.OF
Calculation of Solvency Capital Requirement as per QRT data	0.SCR.SF	FBS.SCR.SF	CBS.SCR.SF
Solvency Capital Requirement - for groups using the standard formula and partial internal model as per QRT data	0.SCR.PIM	FBS.SCR.PIM	CBS.SCR.PIM
Solvency Capital Requirement - for groups on Full Internal Models as per QRT data	0.SCR.FIM	FBS.SCR.FIM	CBS.SCR.FIM
Impact cyber scenarios per product and per economic sector	FBS.CYBER.IMPACT		
Accumulation exposure cyber insurance per IT service provider	FBS.CYBER.ACC		

* CBS only for "Cloud outage leading to bursting of tech bubble"

Appendix 3 - Business black-out

Possible impact Lines of Business

1. Power generation and distribution companies:
 - a. Property damage
 - b. Business Interruption
 - c. Incident Response Cost
 - d. Regulatory Fines
 - e. Professional Indemnity (*RC professionnelle* or *BA beroep*)
 - f. Director's and Officer's Liability (*RC dirigeant* or *Bestuurders-aansprakelijkheid*)
2. Companies which suffer a power loss can possibly have insurance claims for the following products and coverages:
 - a. Property damage (e.g. due to spoiled goods)
 - b. Business interruption (*Bedrijfsschade* of *Pertes d'exploitation*)
 - c. Professional Indemnity (*RC professionnelle* or *BA beroep*)
 - d. Medical Malpractice (*RC médicale* or *Medische aansprakelijkheid*)
 - e. Director's and Officer's Liability (*RC dirigeant* or *Bestuurders-aansprakelijkheid*)
3. Companies which are indirectly impacted can possibly have insurance claims for the following products and coverages:
 - a. Contingent Business interruption
 - b. Third Party Liability (e.g. Director's and Officer's liability)
 - c. Credit insurance (e.g. due to business interruption leading to defaults)
4. Companies delivering inadequate technical services or costs (e.g. which allowed for the vulnerability leading to a cyber attack)
 - a. Professional Indemnity (*RC professionnelle* or *BA beroep*)
 - b. Product Liability (*RC après livraison / produit* or *BA na levering / product*)
 - c. Public Liability (*RC exploitation* or *BA uitbating*)
5. Home owners
 - a. Property damage (e.g. due to spoiled goods)
6. Specialty insurance
 - a. Event cancellation
7. Additional insurance claims might be triggered such as motor, transport, worker's compensation and medical expense claims due to car accidents triggered by not functioning traffic light. However, given the greater complexity and uncertainty at estimating these indirect claims, such claims do not need to be considered by the stress test participants.

Appendix 4 - Ransomware Attack

Possible impact Lines of Business

1. Companies which are directly impacted can possibly have insurance claims for the following products and coverages:
 - a. Business interruption (*Bedrijfsschade* or *Pertes d'exploitation*)
 - b. Cyber extortion
 - c. Data and Software Loss
 - d. Crisis service costs
 - e. Recovery expense costs
 - f. Professional Indemnity (*RC professionnelle* or *BA beroep*)
 - g. Medical Malpractice (*RC médicale* or *Medische aansprakelijkheid*)
 - h. Director's and Officer's Liability (*RC dirigeant* or *Bestuurders-aansprakelijkheid*)
2. Companies which are indirectly impacted can possibly have insurance claims for the following products and coverages:
 - a. Contingent Business interruption
 - b. Third Party Liability (e.g. Director's and Officer's Liability)
 - c. Credit insurance (e.g. due to business interruption leading to defaults)
3. Companies delivering inadequate technical services or costs (e.g. which allowed for the vulnerability leading to a cyber attack)
 - a. Professional Indemnity (*RC professionnelle* or *BA beroep*)
 - b. Product Liability (*RC après livraison / produit* or *BA na levering / product*)
 - c. Public Liability (*RC exploitation* or *BA uitbating*)

Appendix 5 - Cloud Outage

Possible impact Lines of Business

1. Companies which are directly impacted can possibly have insurance claims for the following products and coverages:
 - a. Business interruption (*Bedrijfsschade of Pertes d'exploitation*)
 - b. Data and Software Loss
 - c. Crisis service costs
 - d. Recovery expense costs
 - e. Professional Indemnity (*RC professionnelle or BA beroep*)
 - f. Medical Malpractice (*RC médicale or Medische aansprakelijkheid*)
 - g. Director's and Officer's Liability (*RC dirigeant or Bestuurders-aansprakelijkheid*)
2. Companies which are indirectly impacted can possibly have insurance claims for the following products and coverages:
 - a. Contingent Business interruption
 - b. Third Party Liability (e.g. Director's and Officer's Liability)
 - c. Credit insurance (e.g. due to business interruption leading to defaults)
3. Companies delivering inadequate technical services or costs
 - a. Professional Indemnity (*RC professionnelle or BA beroep*)
 - b. Product Liability (*RC après livraison / produit or BA na levering / product*)
 - c. Public Liability (*RC exploitation or BA uitbating*)

Appendix 5 - Cloud Outage

Financial shocks (1/2)

Shocks to stock prices (%)		
Country/Union	Country/Union	Shock
European Union	Sectors sensitive to cloud outage	-56
	Other	-38
United Kingdom	Sectors sensitive to cloud outage	-71
	Other	-48
United States of America	Sectors sensitive to cloud outage	-68
	Other	-46
Emerging markets	Sectors sensitive to cloud outage	-63
	Other	-43
Other advanced economies	Sectors sensitive to cloud outage	-54
	Other	-37

Shocks to real estate (%)		
Country	Residential	Office & commercial
European Union	-7,1	-20,0
United Kingdom	-11,0	-19,6
United States of America	-11,0	-19,6
Other advanced economies	-11,2	-20,9
Emerging markets	-11,0	-19,6

Shocks to corporate bond yields (bps)								
Country	Type	AAA	AA	A	BBB	BB	B	CCC
European Union	Sectors sensitive to cloud outage	79	94	109	123	172	220	269
	Other	71	75	79	83	88	92	97
United Kingdom	Sectors sensitive to cloud outage	94	109	124	138	187	235	284
	Other	92	94	96	98	103	107	112
United States of America	Sectors sensitive to cloud outage	54	65	87	110	141	173	205
	Other	41	49	66	82	89	96	104
Other advanced economies	Sectors sensitive to cloud outage	83	98	117	136	183	231	278
	Other	75	80	88	96	102	109	104
Emerging markets	Sectors sensitive to cloud outage	131	146	161	175	274	322	321
	Other	119	121	123	125	133	141	149

Appendix 5 - Cloud Outage

Financial shocks (2/2)

Shocks to government bond yields

Country	bps
Austria	6
Belgium	23
Cyprus	49
Estonia	31
Finland	2
France	0
Germany	0
Greece	115
Ireland	13
Italy	69
Latvia	31
Lithuania	32
Luxembourg	1
Malta	36
Netherlands	2
Portugal	88
Slovakia	9
Slovenia	26
Spain	49
EA (weighted averages)	21
Bulgaria	24
Croatia	73
Czech Republic	16
Denmark	4
Hungary	40
Poland	24
Romania	46
Sweden	1
EU (weighted averages)	21
Japan	1
Norway	5
Switzerland	3
United Kingdom	30
United States	19
Other advanced economies	27
Emerging markets	44

Shocks to other assets (%)						
Private Equity		Hedge Funds		REIT		Commodities
EU	Global	EU	Global	EU	Global	
-34	-37	-34	-31	-38	-37	-30

Shocks to covered bond yields (bps)				
Country	AAA	AA	A	BBB
EU	54	60	66	71
North America	30	41	46	51
Asia	69	86	92	97
Others	55	62	68	73

Shocks to RMBS (bps)				
Country	AAA	AA	A	BBB
EU	58	64	72	80
UK	59	66	74	82
US	33	44	51	58
Other advanced economies	50	58	66	74
Emerging markets	94	105	110	116