The NIST Cybersecurity Framework

& its role in Cyber Risk Management and Cyber Insurance

Thursday, May 28th at 10 AM Eastern

ZURICH®

Advisen
Transforming • Insurance℠

Today's webinar is sponsored by:

ZURICH®

The NIST Cybersecurity Framework

& its role in Cyber Risk Management and Cyber Insurance

Visit www.advisenltd.com at the end of this webinar to download:

- Copy of these slides
- Recording of today's webinar

Mark your Calendars!

Determining Appropriate Cyber Limits

LIVE WEBINAR
June 2 @ 11 AM ET

Advisen Transforming • Insurance

REGISTER NOW

LIVE WEBINAR

Decreasing Cyber Risk through Compliance in the Enterprise

Wednesday, June 3 | 10 AM ET

REGISTER NOW ✓

OneTrust GRC
INTEGRATED RISK MANAGEMENT

Advisen Transforming • Insurance

Technology-based Active Security Management

LIVE WEBINAR
June 9 @ 11 AM ET

REGISTER NOW

Advisen Transforming • Insurance

ZURICH

Register for all upcoming webinars at
www.advisenltd.com/media/webinars

Advisen Transforming • Insurance

ARE YOU A RISK MANAGER?

We have something just for you

Risk Managers and Insurance Buyers now get FPN Pro FREE

Today's Moderator

Erin Ayers

Editor of Cyber Front Page News

Advisen

Email at eayers@advisen.com

Today's Panelists

Philipp Hurni

Cyber Risk Engineering Global Practice Leader

Zurich Insurance Group

John Petersen

Chief Information Security Officer

Nestlé

The NIST Framework and its role in Cyber risk management and for Zurich Cyber insurance

Philipp Hurni, Cyber Risk Engineering Global Practice Leader at Zurich Insurance Group

What is the NIST Framework?

Cybersecurity framework

Version 1.1

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

https://www.nist.gov

Cyber risk is a rather young, but **complex risk**. Many organizations struggle to **properly manage cyber risk.**

The **NIST Cybersecurity Framework** helps organizations to learn from **best practices**. It provides standards, guidelines and practices to better **manage and reduce cybersecurity risk.**

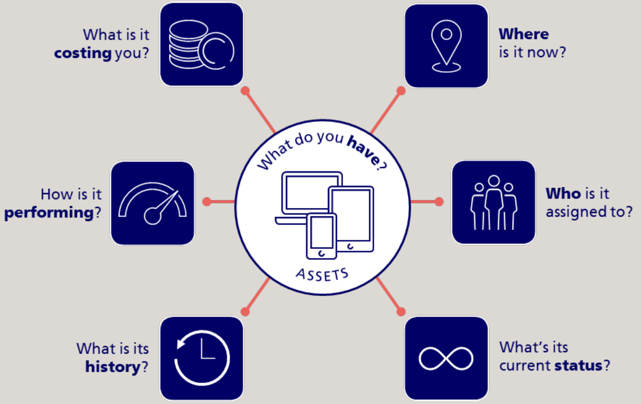
Key attributes:

- **Common** and **accessible language** – also for non-experts
- **Adaptable to sectors** and their **needs**
- **Risk-based** approach
- Continuously **updated** as **technology and threats change**

NIST is embraced by cyber risk professionals in **many companies across the world.**

Identify – what assets need to be protected?

Identify is about developing the **organizational understanding** to manage cybersecurity risks to systems, assets, data and capabilities.


What is it **costing** you?
Where is it now?
What do you **have**?
ASSETS
How is it **performing**?
Who is it assigned to?
What is its **history**?
What's its current **status**?

IMPACT	LOW	MEDIUM	HIGH
HIGH	Medium	High	High
MEDIUM	Low	Medium	High
LOW	Low	Low	Medium

LIKELIHOOD

Selected controls in 'Identify':

- Identify **critical business processes**
- Maintain **hardware, software and data** inventory
- Establish **roles and responsibilities**
- Establish **risk assessment** and **risk management processes**
- Document **information flows**
- Manage risk with respect to **external partners**

Protect – protect your most valuable assets

Protect is developing and implementing the **appropriate safeguards** to protect business assets and ensure delivery of services.

Selected controls in ‘Protect’:

- **Manage access** to **systems and information**
- Protect **your network**
- Protect **sensitive data** (i.e. encryption)
- Patch **operating systems** and **applications**
- Train your **employees**

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Detect – identify attacks to your assets at an early stage

Detect is about implementing the appropriate activities to **detect occurrences** of cybersecurity events.

Selected controls in ‘Detect’:

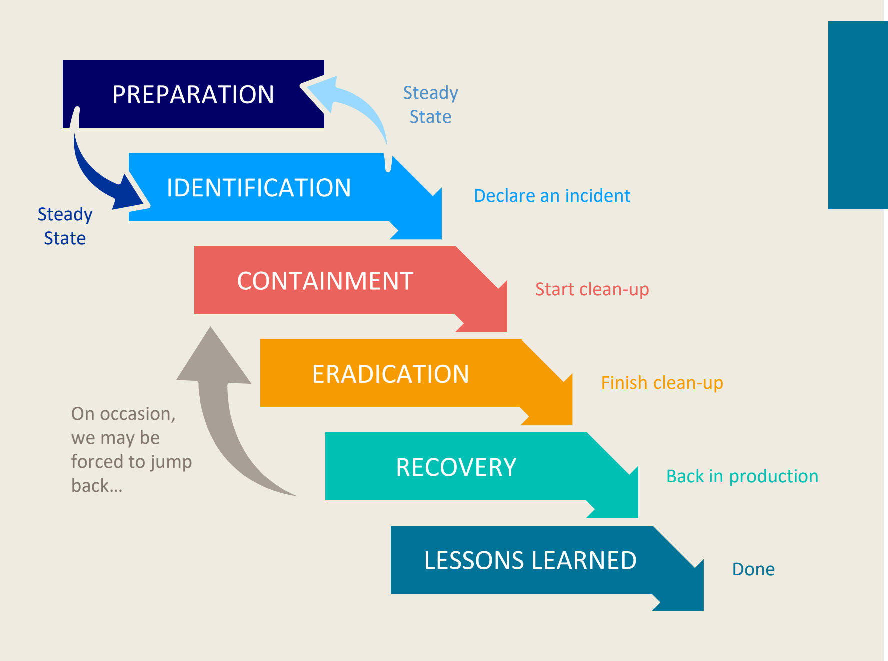
- **Understand expected/usual data flows** of the business (baseline)
- Collect **logfiles of IT assets**, **network traffic** and **correlate** the information
- **Antivirus/anti-malware detection** software on all IT assets
- Continuously **monitor** IT assets

© Zurich

Respond – swiftly react to cyber attacks to reduce impact

ZURICH

Respond is about **implementing the appropriate activities** to take action regarding a detected cybersecurity event.



Selected controls in ‘Respond’:

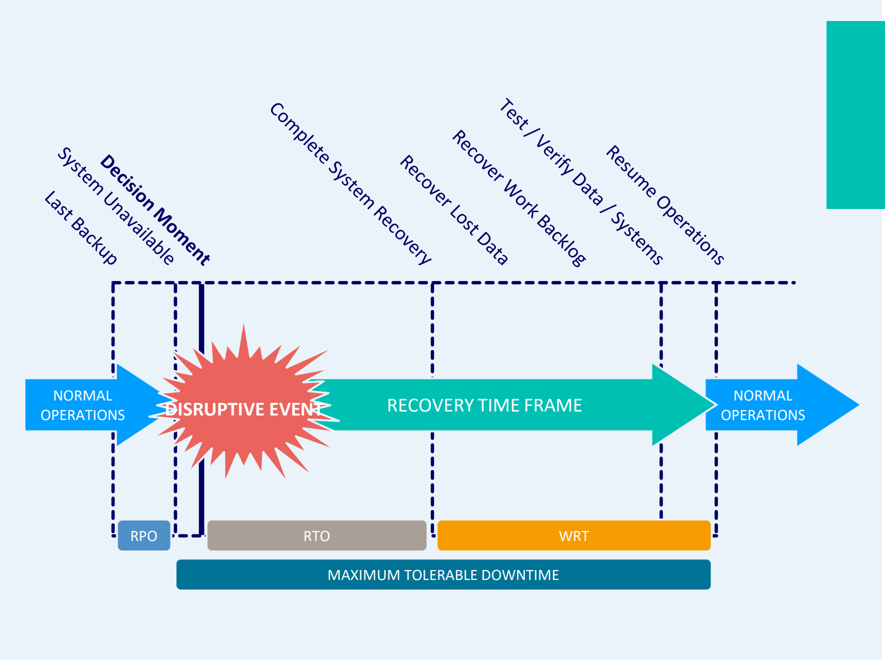
- Develop **incident response plans**
- Define **roles and responsibilities**
- Coordinate with **internal** and **external stakeholders**
- Ensure response plans are **tested**
- Ensure response plans are **updated**

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Recover – recover from cyber attacks and restore operations

ZURICH

Recover is about **implementing the appropriate activities** to maintain **plans for resilience** and to restore any capabilities or services that were impaired due to a cybersecurity event.



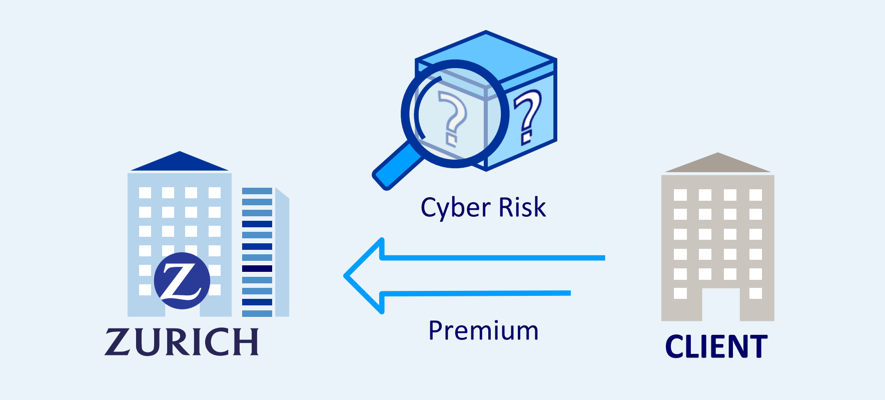
Selected controls in ‘Recover’:

- Prioritize **systems** and **applications** (define recovery time objectives, recovery point objectives)
- Build **resilience** – consider **alternate data center facilities**
- Develop **business continuity plans** with IT emergency scenarios
- Develop **IT disaster recovery plans**
- **Test** plans regularly, incorporate learnings

How can the NIST Framework support Cyber Insurance?

Cyber risk is **nontangible** and **nontrivial to assess**

Cyber insurance struggles with significant inherent **information asymmetry**



Assessment along the **5 NIST Framework dimensions** helps Zurich Underwriters and Risk Engineers to **assess cyber risk**, by

- identifying the client’s cyber risk **exposures**
- identifying **strengths** and **weaknesses** in the client’s cyber defenses
- deriving an **overall metric** for the **maturity** of the cyber risk management of the client

Cyber Risk Engineering – Assessment of Cyber Risk Management Maturity

Evaluation based on the NIST Framework

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Risk Quality Level Scale

Excellent: <51

Good: 51-100

Fair: 101-150

Poor: >150

ZURICH

Risk Engineering

Risk Assessment and Risk Improvement

Helping you to understand and mitigate your risks

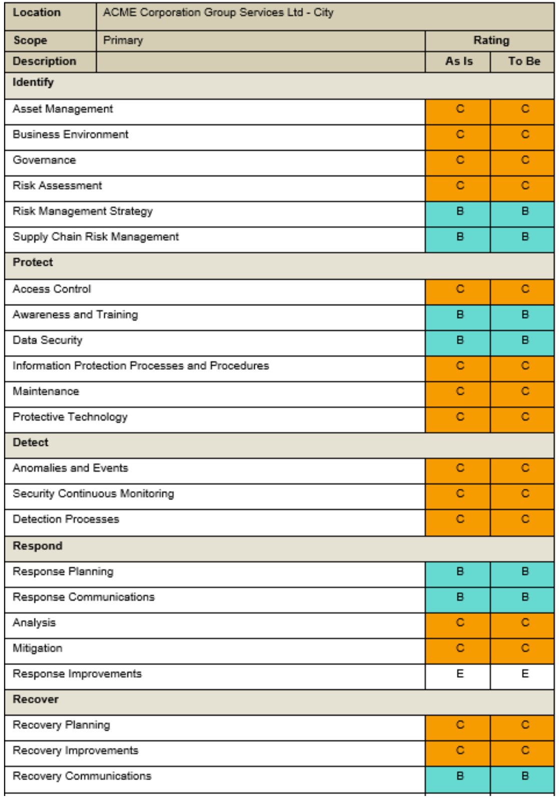
Main Contents

Executive Summary

Risk Overview

Grading

Risk Improvement Actions



Location	ACME Corporation Group Services Ltd - City		
Scope	Primary	**Rating**	
Description		**As Is**	**To Be**
Identify			
Asset Management		C	C
Business Environment		C	C
Governance		C	C
Risk Assessment		C	C
Risk Management Strategy		B	B
Supply Chain Risk Management		B	B
Protect			
Access Control		C	C
Awareness and Training		B	B
Data Security		B	B
Information Protection Processes and Procedures		C	C
Maintenance		C	C
Protective Technology		C	C
Detect			
Anomalies and Events		C	C
Security Continuous Monitoring		C	C
Detection Processes		C	C
Respond			
Response Planning		B	B
Response Communications		B	B
Analysis		C	C
Mitigation		C	C
Response Improvements		E	E
Recover			
Recovery Planning		C	C
Recovery Improvements		C	C
Recovery Communications		B	B

The NIST Cybersecurity Framework

& its role in Cyber Risk Management and Cyber Insurance

Erin Ayers

Advisen

[Moderator]

Philipp Hurni

Zurich Insurance Group

John Petersen

Nestlé

Advisen
Transforming • Insurance

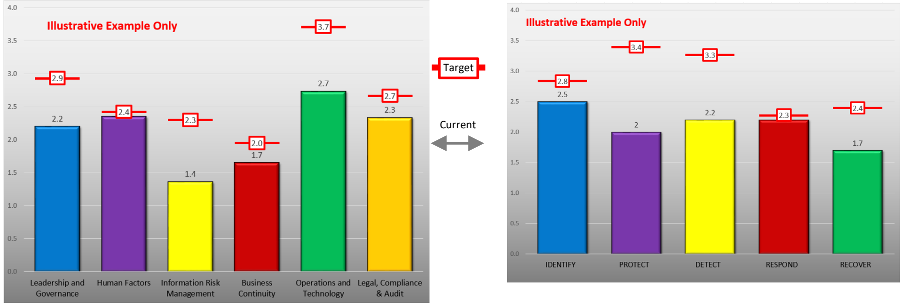
NESTLÉ - CYBER SECURITY DASHBOARD

Information Technology

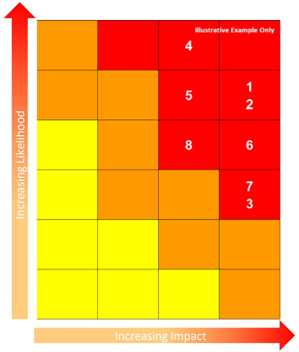
MATURITY LEVELS ASSESSMENT

Governance Maturity Model

Technical Maturity Model (NIST)



RISK HEATMAP



TOP CYBER SECURITY RISKS

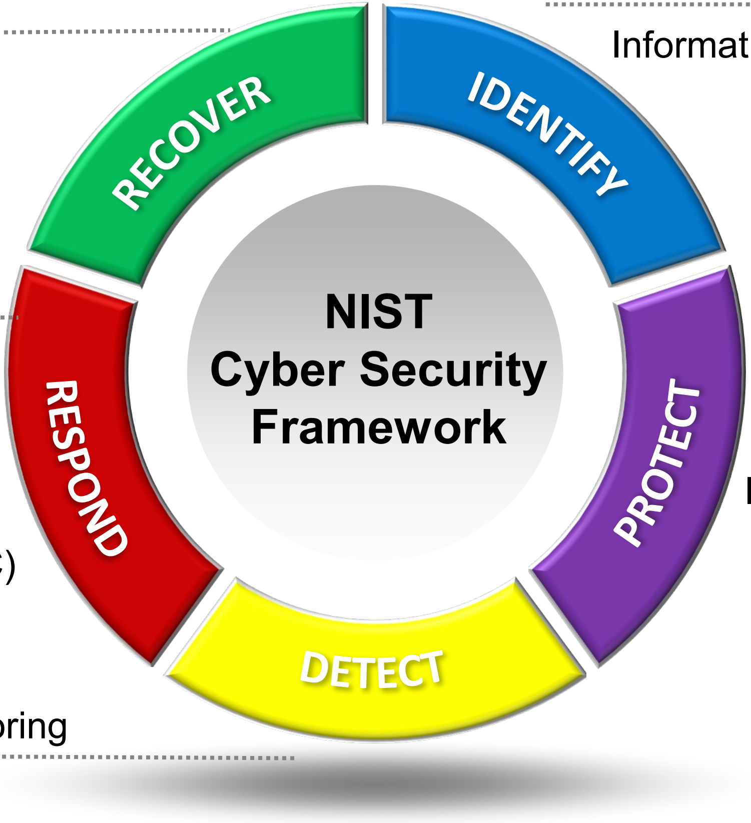
ID	BUSINESS IMPACT	VULNERABILITIES	THREATS	RISK TOPIC
1	Severe **business operations disruption** due to lack of integrated business continuity leading to **financial loss** or missed opportunities	• Inconsistent, non-integrated approach for Business Continuity Management	• Interruption of IS/IT systems supporting critical business processes	BUSINESS CONTINUITY MANAGEMENT
2	3rd Party security incident or breach **impacting business operations** and/or resulting in **reputational damage**	• Inconsistent governance over 3rd Parties operations • Increasing reliance on 3rd Parties for core activities	• 3rd parties not aligned with Nestlé security & compliance culture	3RD PARTY GOVERNANCE
3	Leakage of confidential information due to insecure behavior of untrained employees leads to **reputational damage** or **internal labor issues**.	• Insufficient Security & Compliance training and awareness for employee	• Unaware or untrained employees working with information and systems	SECURITY & COMPLIANCE CULTURE
4	Unauthorized access through exploitation of Identity Governance and Privileged User processes with **operational**, **financial** or **legal** impact.	• Identity Governance and Privileged User processes • Non-automated Joiner-Mover-Leaver process	• Malicious individuals or groups attempting to penetrate Nestlé systems to steal, disclose or modify information	UNAUTHORIZED ACCESS
5	Cyber Attacks resulting in breach of e-Commerce or Consumer Personal Data leads to **loss of confidence** by **consumers** and **key stakeholders**	• Poor awareness of employees on social engineering attacks • IT system design flaws	• Deliberate cyber-criminal activity manipulating Nestlé systems, employees, consumers or customers	CYBER ATTACKS, PHISHING AND RANSOMWARE
6	Reputational impact, costs of remediation and **significant fines** for non-compliance to regulatory requirements.	• Limited insight on compliance or on the effectiveness of implemented controls	• Adherence to changing Regulatory requirements and internal obligations	NON-COMPLIANCE
7	Intentional disclosure of confidential information or **intellectual property** by insiders, damaging **reputation** or **competitive advantage**	• Weak internal controls • Lack of standardized background checks	• Malicious sabotage or fraudulent activity by internal users	INSIDER THREAT
8	**System exploitation** leading to **data breach** and **reputational damage**	• Lack of infrastructure maintenance or patching allowing system access	• External individuals or groups gaining unauthorized access or system interruption	SYSTEM VULNERABILITIES

ACTIONS

Action	Program
• Update Business Continuity Policy to reflect business changes	Information Security Management System
• Expand scope of Vendor Management Policy	Information Security Management System
• Implement Digital Rights Management to enable effective collaboration with highly sensitive information	Information Protection
• Increase automation in Identity & Access Management processes	Identity Management
• Increase impact of awareness programme with Phishing simulations	Security Awareness
• Mandate GDPR and Pharma Risk Assesment across ISMS Scopes	Information Security Management System
• Behavioural Analytics for sensitive and highly privileged roles	Security Operations Center
• Drive risk based improvements in vulnerability management • Publish Nestlé Internet of Things Standard	Security Operations Center

Ilustrative Example

Use NIST to prioritize and drive improvements in security controls and programs



Information Security Mgmt System (ISMS)
Data Privacy Program

Access Mgmt & Identity Gov.
Cloud and Digital Security
Infra. and Application Security
IoT/OT for Facilities and Factories
Multi Factor Authentication
Cont. Employee Education

24/7 Sec. Operations (SOC)
Penetration Testing
Threat Monitoring
3rd Party Cyber Risk Monitoring

Incident Response
Red Teaming

Cyber Resilience across IT
ISMS program

Thank you to Today's Panelists

Philipp Hurni

Cyber Risk Engineering Global Practice Leader

Zurich Insurance Group

John Petersen

Chief Information Security Officer

Nestlé

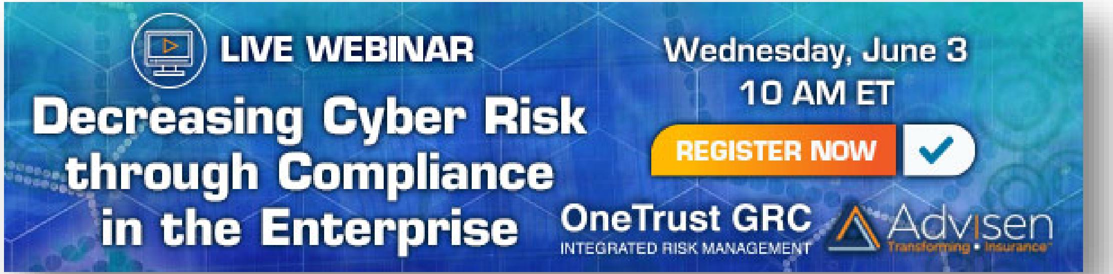
The NIST Cybersecurity Framework

& its role in Cyber Risk Management and Cyber Insurance

Visit www.advisenltd.com at the end of this webinar to download:

- Copy of these slides
- Recording of today’s webinar

For more on Advisen, visit at www.advisenltd.com or email us at webinars@advisen.com



LIVE WEBINAR

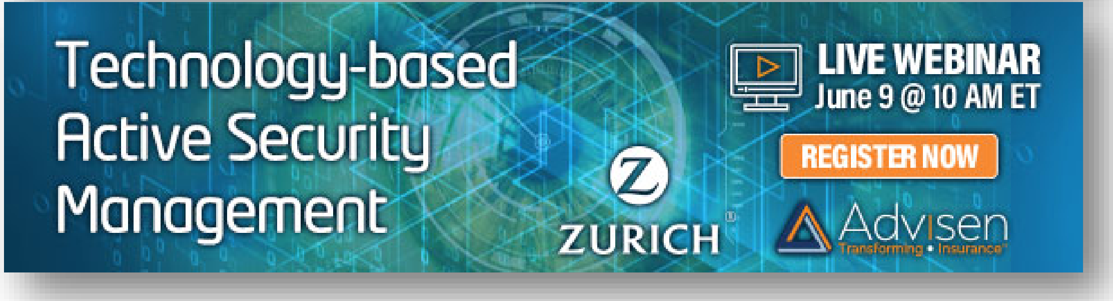
Decreasing Cyber Risk through Compliance in the Enterprise

Wednesday, June 3
10 AM ET

REGISTER NOW ✓

OneTrust GRC
INTEGRATED RISK MANAGEMENT

Advisen
Transforming • Insurance



Technology-based Active Security Management

LIVE WEBINAR
June 9 @ 10 AM ET

REGISTER NOW

ZURICH

Advisen
Transforming • Insurance

Advisen
Transforming • Insurance

Leading the way to **smarter**
and more **efficient**
risk and insurance **communities**.

Advisen delivers:
the ***right information*** into
the ***right hands*** at
the ***right time***
to ***power performance***.

About Advisen Ltd.
Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets and applications focus on large, specialty risks. Through Web Connectivity Ltd., Advisen provides messaging services, business consulting, and technical solutions to streamline and automate insurance transactions. Advisen connects a community of more than 200,000 professionals through daily newsletters, conferences, and webinars. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

+1 (212) 897-4800 | info@advisen.com | www.advisenltd.com