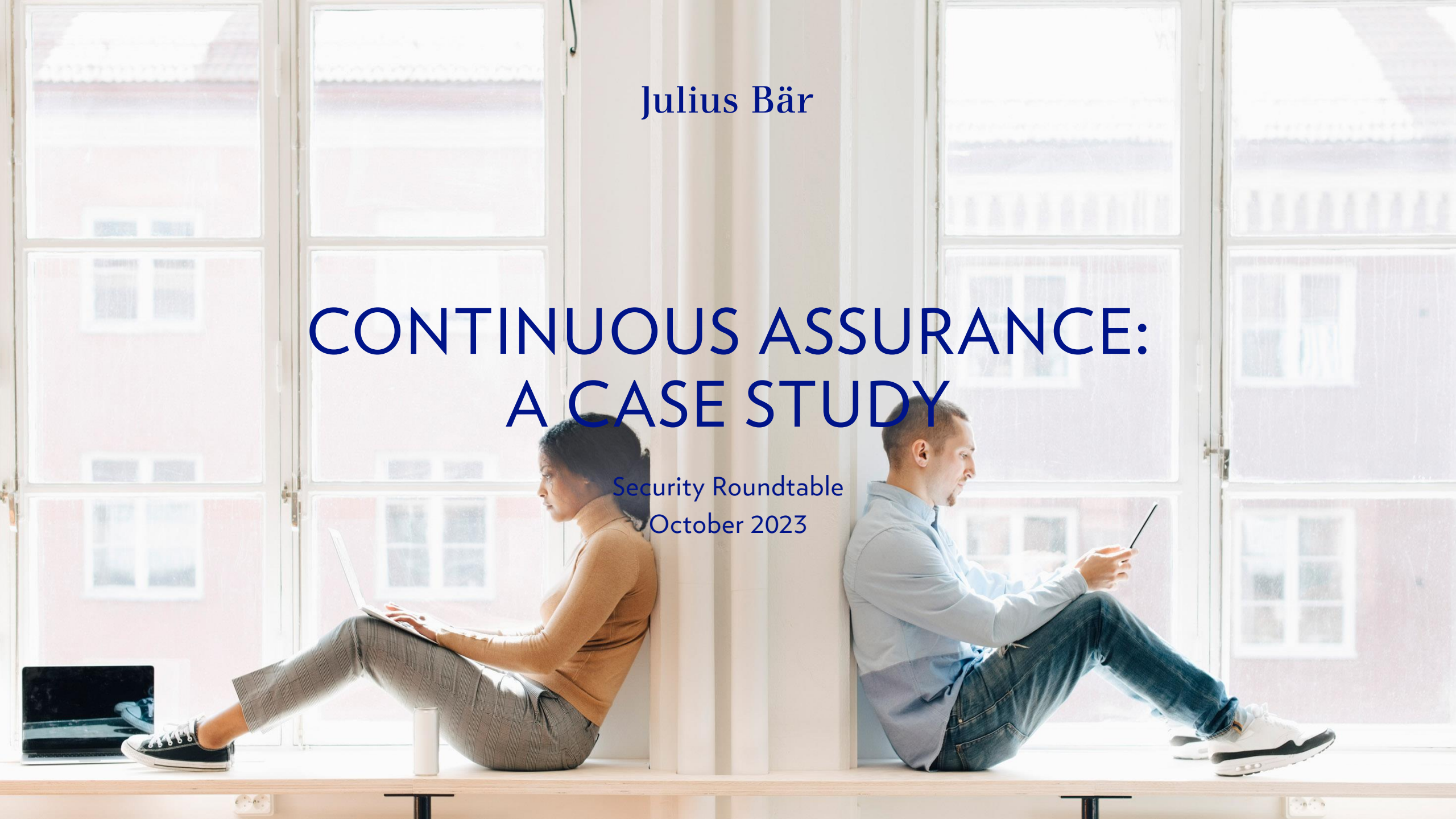
Julius Bär

CONTINUOUS ASSURANCE: A CASE STUDY

Security Roundtable
October 2023



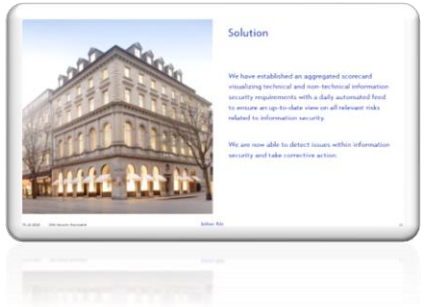
Case Study: Continuous Assurance

Bank Julius Bär

1. PROBLEM

An impossible problem?

Introduction



2. SOLUTION

The Continuous Assurance Dashboard

Concept

3. SUMMARY

Measure Information Security

Takeaways

About Bank Julius Bär

Julius Baer is the leading Swiss wealth management Bank.

We focus on providing holistic and personal advice tailored to the needs of each valued client.

Within Information Security the data of our clients is of most value. Therefore an early onset of threats and risks helps us to stay protected and remain vigilant.

Poll #1

Does your organization have the ability to measure Information Security?

(A) Yes!

(B) Somewhat

(C) Not yet

(D) Don’t know

Scenario

To effectively manage IT and Information Security risks Bank Julius Baer looked for a way to assess the effectiveness of its implemented strategy, risks and processes in order to reach a state of Continuous Assurance.

Continuous assurance gives peace of mind that a state of compliance is ongoing rather than just an expired snapshot.

Simply Put


Information Security Drivers
Need to measure Information Security
Effective Reporting to all Key Stakeholders

Simply Put

Derived Security Requirements	
Technology Neutral	**Technological**
Phishing	Vulnerability and Patch Management
Information Security Training	Baseline Compliance
Security Project Involvement	SIEM Operational Effectiveness
IAM Role Assignment Status	Firewall Rule Recertification
Incident Report	Red Team Exercises Completed
Risks	Transport Layer Security
etc.	etc.

Problem

The challenge with measuring information security is to assess your current state and take a comprehensive approach in bringing together existing measurements into an understandable format.

An impossible challenge?

Key Challenges

1

Understandable

Define relevant Security Controls with associated KRIs

2

Complete

Identify Information Need

3

Automated

Establish a sustainable measurement model

Poll #2

When measuring Information Security what are the most important aspects to consider:

(A) Management Buy In

(B) Easy to understand Reporting

(C) Complete measurability

(D) Automation

Strategy / Approach

Know your Stakeholders

Senior Management, IT, HR, Audience, etc

Create a simple visualization

Test your ideas and involve expert user interface creators

Ensure updated raw data

The underlying data which is sourced needs to be trustworthy

Solution

We have established an aggregated scorecard visualizing technical and non-technical information security requirements with a daily automated feed to ensure an up-to-date view on all relevant risks related to information security.

We are now able to detect issues within information security and take corrective action.

MOCK UP

CONTINUOUS ASSURANCE - OVERVIEW

Continuous Assurance KRI		Mouse over to see more details (L4) and click on a circle or a row to select
SC002	Media Handling	MED
SC003	Security Operations Center	MON
SC004	Security Assessment and Testing	SAS
SC005	Password Management System	CRE
SC006	Information Security Organisation	ISM
SC007	Human Resource Security	HRS SAW
SC008	Information Classification	DAT INV
SC009	Access Control	IAM
SC010	Cryptography	CRY
SC011	Physical Security	PHY
SC012	Operations Security	ABC DBC LOG MAL SBC VPM
SC013	Communications and Network Security	NBD
SC014	System Acquisition, Development and Maintenance	CON SSD
SC016	Information Security Incident Management	IMR
SC017	Cyber Resiliency	CYB
SC018	Compliance	COM

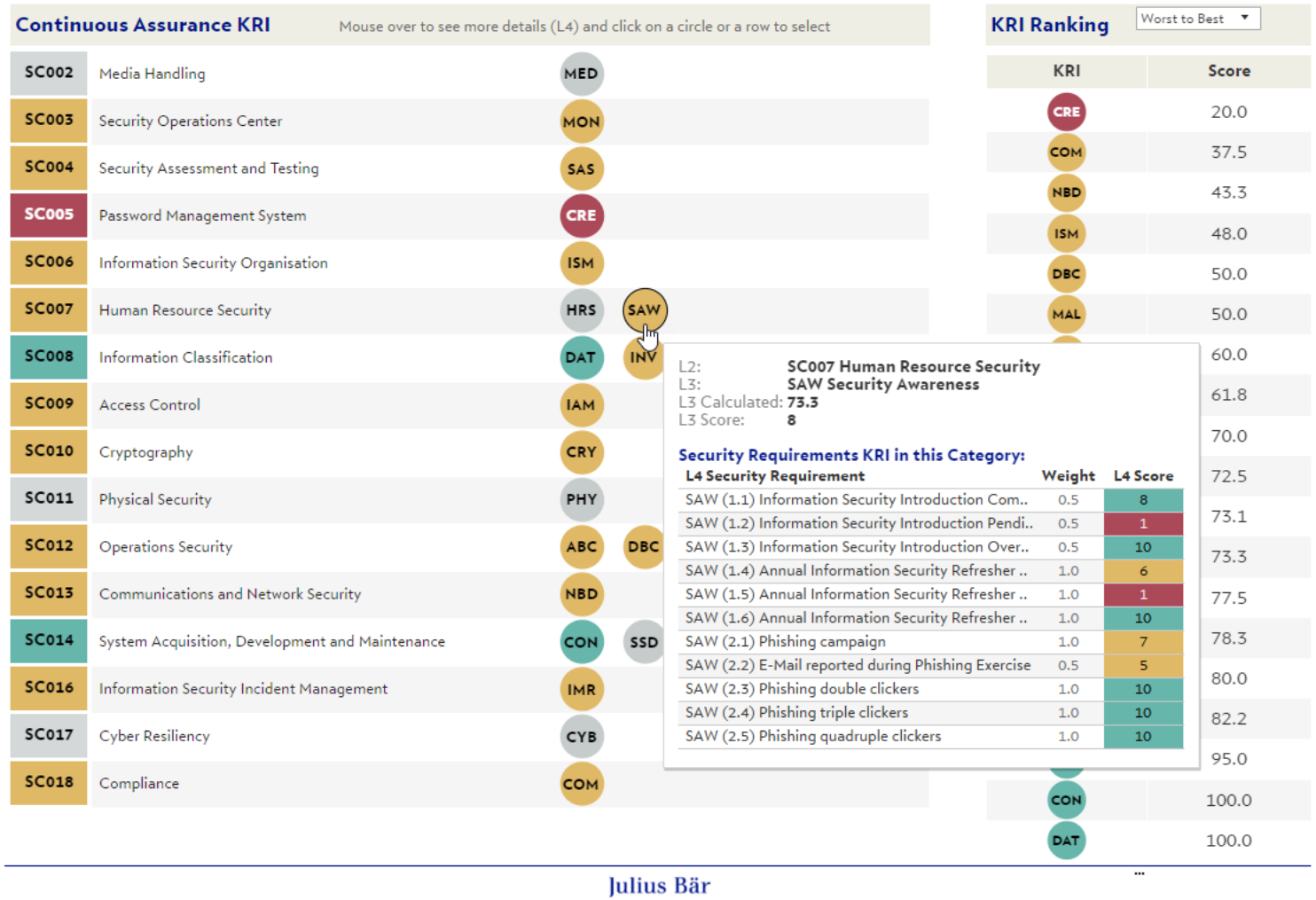
KRI Ranking Worst to Best

KRI	Score
CRE	20.0
COM	37.5
NBD	43.3
ISM	48.0
DBC	50.0
MAL	50.0
ABC	60.0
VPM	61.8
SAS	70.0
INV	72.5
MON	73.1
SAW	73.3
IMR	77.5
IAM	78.3
CRY	80.0
SBC	82.2
LOG	95.0
CON	100.0
DAT	100.0

MOCK UP

MOCK UP

CONTINUOUS ASSURANCE - OVERVIEW



MOCK UP

Business Benefits

1. Increased transparency
2. Evidence of meeting requirements
3. Support decision-making
4. Reduction of attack surface

Key Take Aways

Information Need

What do you want to measure?

Governance

With whom will you discuss your results?

Be patient

Measurability only gets one shot

Key Take Aways

- Measure
- Information
- Security

Julius Bär

Information Security
Bank Julius Baer & Co. Ltd.
--