RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **STR1-T01**

Swiss Re Framework Shortens 800+ Application Multi-Cloud Conversion

Michael Coden
Senior Advisor
Boston Consulting Group
Coden.Michael@advisor.bcg.com

Colin Troha
Managing Director
Boston Consulting Group
Troha.Colin@bcg.com

Philipp Krayenbuehl
Global Chief Security Officer
Swiss Re
Philipp.Krayenbuehl@swissre.com

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The information and opinions contained in the presentation are provided as at the date of the presentation and may change. Although the information used was taken from reliable sources, Swiss Re, Boston Consulting Group, Philipp Krayenbühl, and Michael Coden do not accept any responsibility for its accuracy or comprehensiveness or its updating. All liability for the accuracy and completeness of the information or for any damage or loss resulting from its use is expressly excluded.

RSAConference2022

Introduction & Overview

Swiss Re’s Public Cloud Security Journey

Why Multi-Public Cloud Security

- 80% of organizations will shut down their traditional data centers by 2025.[1]
- 96% of organizations are concerned about their current level of cloud security.[2]
- 70% of organizations hosting data in the public cloud experienced a security incident, while 66% leave back doors open to attackers through misconfigured cloud services.[2]
- Different clouds are required by regulators in different geographies, e.g. Azure, AWS, GCP in Western countries, Alibaba in China
- Different clouds may provide commercial or performance enhancements for different applications

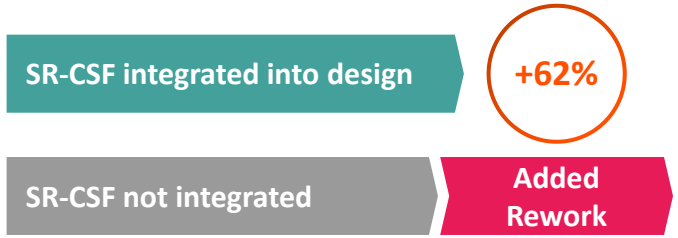
[1] The Data Center Is (Almost) Dead, Gartner
[2] The State of Cloud Security 2020, Sophos

Swiss Re's Public Cloud Security Journey

- Ambition to be "100% Cloud by 2025" to:
  - Support business growth strategies
  - Enable fast innovation
  - Reduce development time and cost
  - Reduce operating costs
  - Increase security of digital services
  - Increase cyber-resilience of digital services
- Timetable could not wait for standards to be developed
- Together with BCG we developed and then implemented the **Swiss Re Cloud Security Framework (SR-CSF)**
- **Open sourced** the SR-CSF through the Cyber Risk Institute - downloadable

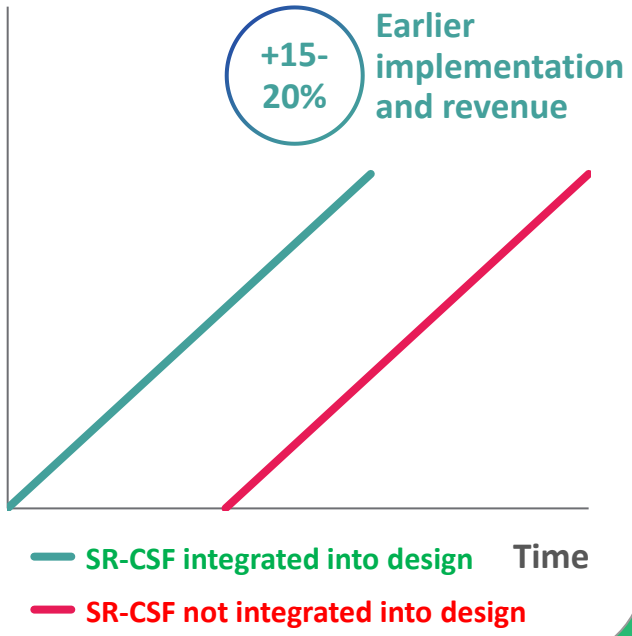
Result: Increased security, reduced time and cost of development & operations, faster time to market, & profits

Designing-in cybersecurity cuts development time/cost …

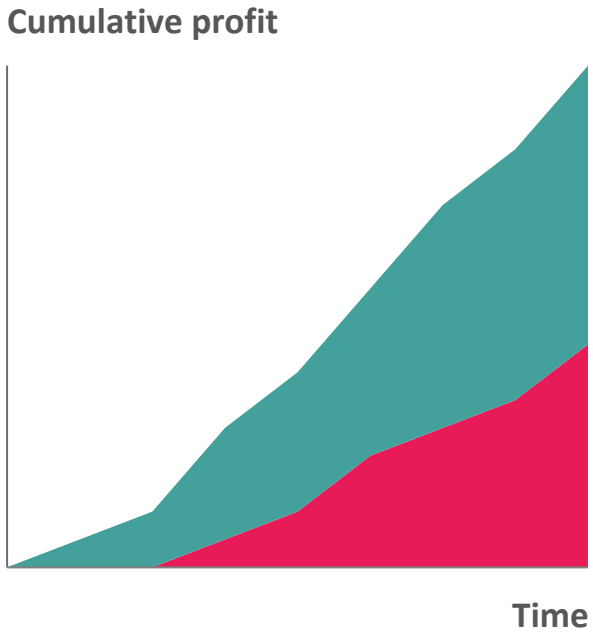


… as well as operating costs…

… accelerating speed to market and revenue generation…



… creating first-mover advantage and increased profitability

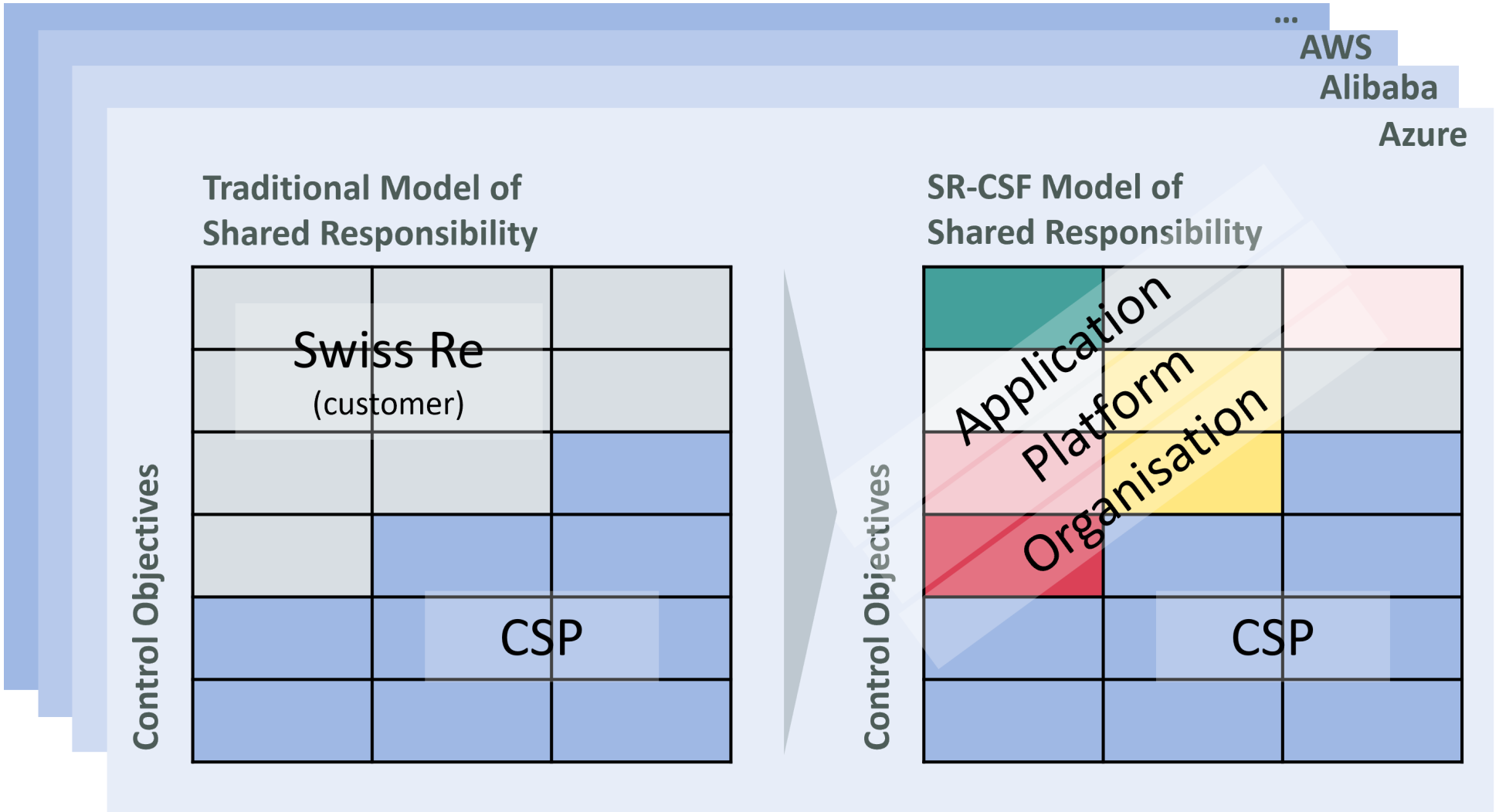


BCG Michael Coden Colin Troha Philipp Krayenbühl Swiss Re

RSAConference2022

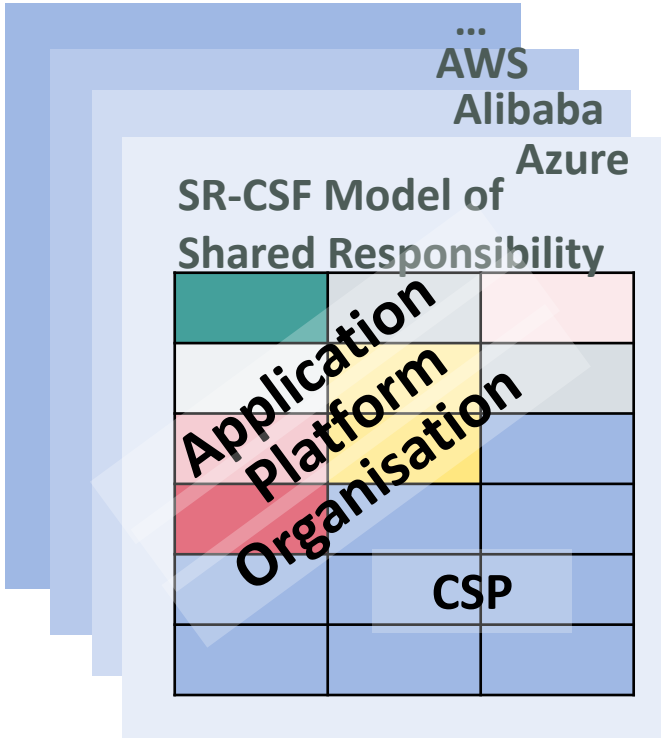
Developing The Swiss Re Cloud Security Framework

We started with a granular definition of our cybersecurity and cyber-resilience requirements



We developed requirements that must be applicable to all CSPs

1. Maintained Cloud agnostic Security Control Objectives
2. Required standardization, consistency, and applicability across CSPs
3. Increased cybersecurity
4. Increased cyber-resilience
5. Reduced development & SecOps costs



Our Swiss Re Cloud Security Framework achieved

- Multi-cloud compatibility and applicability for applications
- Compliance with industry standards and regulations
- Efficiencies in audit, risk, and regulatory reporting
- Increased application and data security and cyber-resilience
- Reduced development time and cost – due to easily reusable security code and procedures
  - **Accelerated time to deployment into production**
  - **Caused developers to adopt willingly**
- Reduced operating costs

Our journey faced 3 challenges

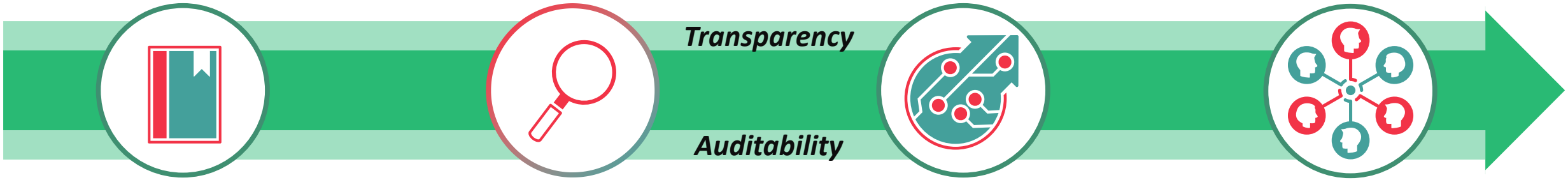
1. Developing a common framework that:
   - Meets the needs of all business unit applications & developers
   - Implements consistent compliance and security controls on every CSP
   - Can be audited on every CSP
     - ➢ Result: **Swiss Re Cloud Security Framework (SR-CSF)**
2. Developing a process facilitating use of the Swiss Re CSF
   - Educate developers to understand benefits of using the CSF
   - Provide self-service approval for developers who use the CSF
   - Provide governance that developers are using the CSF
     - ➢ Result: **Swiss Re Digital Governance Framework (DGF)**
3. Convincing Cloud platform and application developers to embrace

Reusability, compliance, and auditability were critical for acceptance of the SR-CSF and DGF

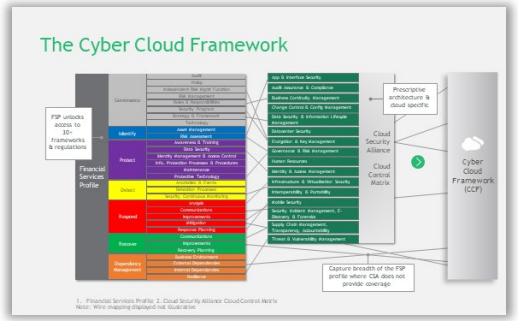
- Security framework for **any digital service** deployed to **any public cloud**
- Based on **CSA/CCM** and Cyber Risk Institute "**Profile**"
- Large one-off effort to establish the framework and map global standards and regulations, but then **reusable**
- Provides a strong foundation for secure & compliant implementation, for consistently staying so, and for **being able to prove it**

1. Cloud Security Alliance / Common Controls Matrix. 2. Cyber Risk Institute Financial Services Sector Cybersecurity Profile – http://cyberriskinstitute.org

Four elements combine to accelerate and reduce cost of secure implementations in the cloud

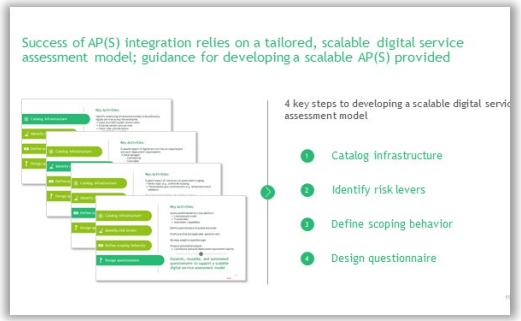


SR Cloud Security Framework



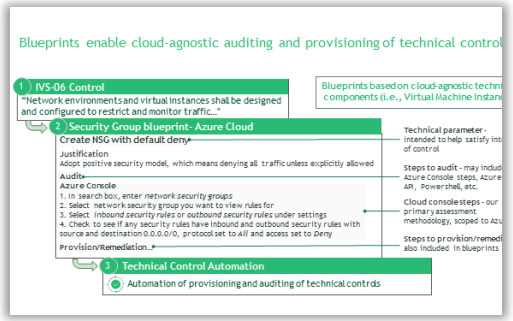
Standardized Cloud Security framework mapped to regulatory requirements

SR-DGF Automated Intake Process / Security Plans



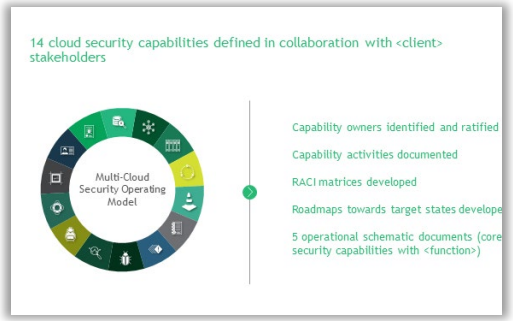
Repeatable process evaluates applications to determine applicable security controls & reusable components

Reusable Security Patterns with automated deployment



Scalable, reusable solutions for securely deploying and auditing across multi-cloud environments

Target Operating Model / Governance / Audit

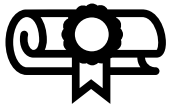


A governance & operating model that efficiently implements cloud security & automates audit functions

BCG Michael Coden Colin Troha Philipp Krayenbühl Swiss Re

SR-CSF required cloud security in: design, during operation, and for continuous improvement

Regulations



SR Internal Policies & Standards

Business need

Industry best practice

Swiss Re Cloud Security Framework (SR-CSF) based on CSA/CMM

Becoming secure

- Swiss Re's assets protected in the public cloud
- Secure migration to the public cloud

Staying secure

- Any changes to cloud services must be assessed and approved
- Situational security awareness across all cloud environments

Proving security

- Providing assurance through controls and audits
- Generating data-driven insights for continuous improvement

Capabilities across Swiss Re

We developed procedural & technical Control Objectives & Safeguards for 16 security capabilities

Becoming secure & compliant

Design and implement procedural capabilities

Design and implement technical capabilities and safeguards

Policies, Standards, & Safeguards

SR-CSF and Capabilities

- Vulnerability Mgmt.
- Logging & Monitoring
- Encryption & Cert Mgmt.
- Threat Management
- Secure Arch & App Dev
- Risk Management
- Identity & Access Mgmt.
- Privacy Mgmt.
- Policy, Stds, & Procedures
- Network Security
- Inc Response & Forensics
- Data Sec & Info Protection
- Business Continuity
- Disaster Recovery
- Supply Chain Management
- Digital Workplace

Control Objectives

Control Objectives (CO) have been defined for the secure use of Public Cloud services and are fulfilled by implemented **Safeguards**, such as

- controls,
- processes,
- technical solutions,
- or other mechanisms employed.

SR-DGF: easy to use, self governing processes enabled developers to work securely and faster

Maintain Security and Compliance

Change management

Assesses risks of new cloud services and application modifications

Continuous monitoring

Assures applications continue to meet Control Objectives

DGF process, DevSecOps, & HAC

DGF (Digital Governance Framework): New or Changing Digital Services

New or changing cloud services are introduced into the DGF by the case owner, and relevant COs assessed within applicable gates

Ongoing Monitoring

COs that are related to maintenance and monitoring, such policy-based or post-deployment COs, are assessed on an ongoing basis via:

HAC (Cloud Hygiene, Assurance and Controls)

Developed to **continuously monitor** digital services wrt **security and compliance.**

Automated auditability ensures continuous security & compliance while greatly reducing costs

Proving security and compliance

Reporting based on Swiss Re's standard internal controls

Developed new easily used cloud security metrics

Control Evidence, Documentation, KPI / KRI

Audit – controls to mitigate risk

Stakeholders: GIA, External Audit, Regulators SOC 2 Type II Report

Client Requests – application security

Stakeholders: Application Owners, BU Leadership

Metrics – for strategic and operational decisions

Stakeholders: CISO Office, Senior Management, Capability Owner

Adaption of internal controls relevant to public cloud security

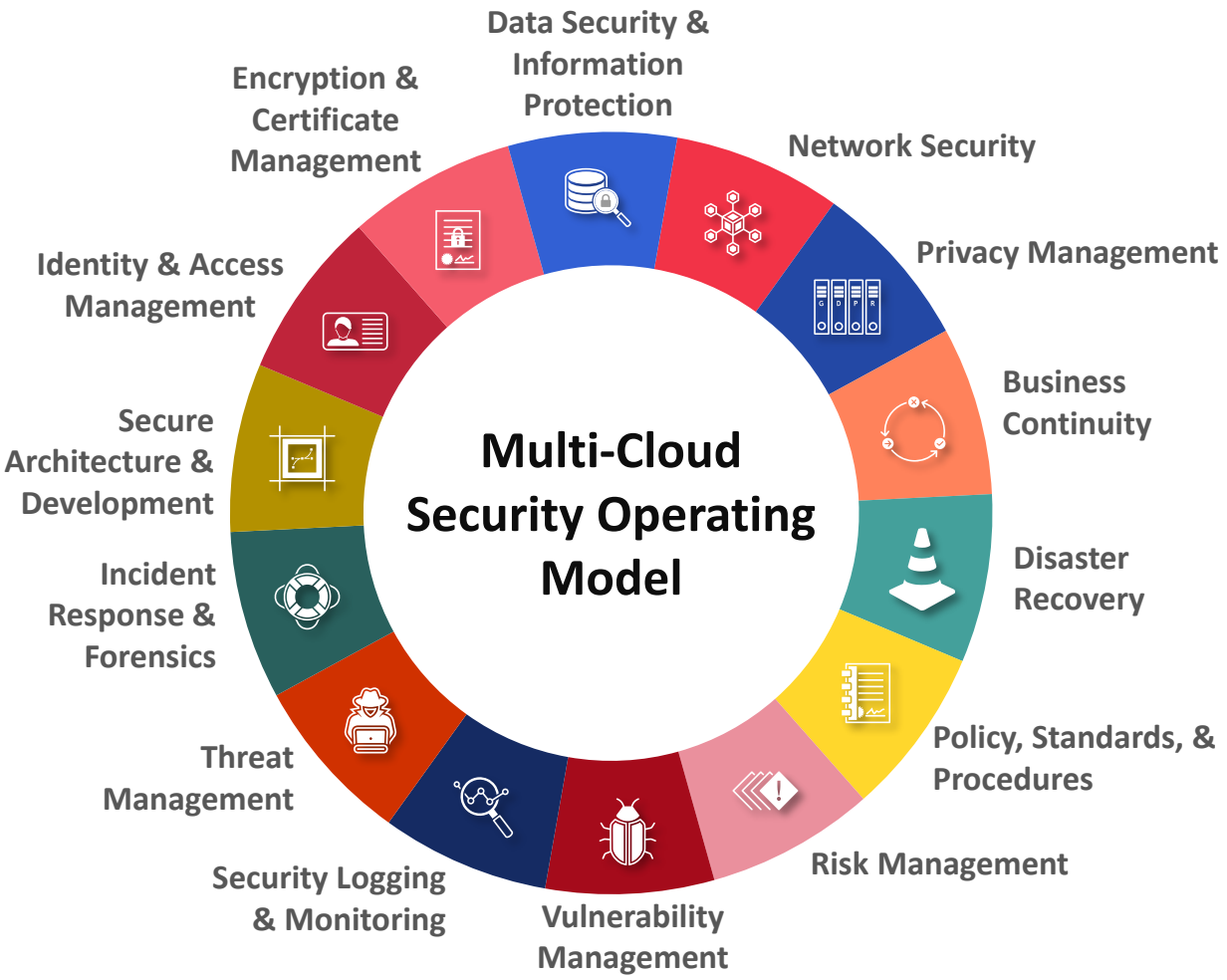
Cloud application self-assessment for individual applications

Cloud security reporting system

Maintaining the Swiss Re Cloud Security Framework

- After design and implementation, maintenance is where the gap between policies and code could fall apart
- We started in excel, moved to a Swiss-based tool
- Developed a data model and tools to support it
- Driving efficiency for:
  - Security reviews
  - Multi-cloud environment deployment
  - Continuous auditing

Operating model has 17 cloud security domains to efficiently implement solutions, streamline governance and automate audit



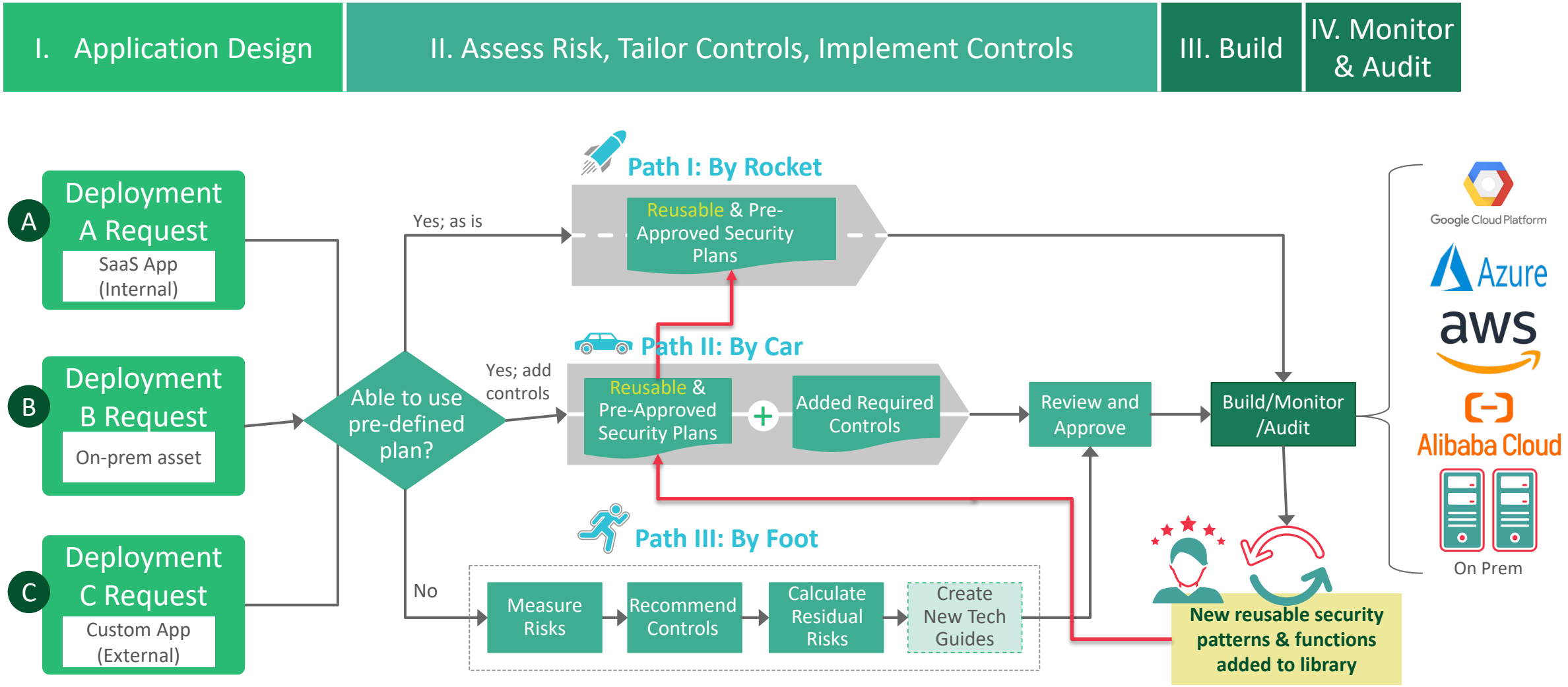
Named capability owners distributed across business units helps enterprise-wide engagement

Capability activities documented

Published RACI matrices
- **show developers who can give guidance**
- **give prestige to capability "owners"**

BCG Michael Coden Colin Troha Philipp Krayenbühl Swiss Re

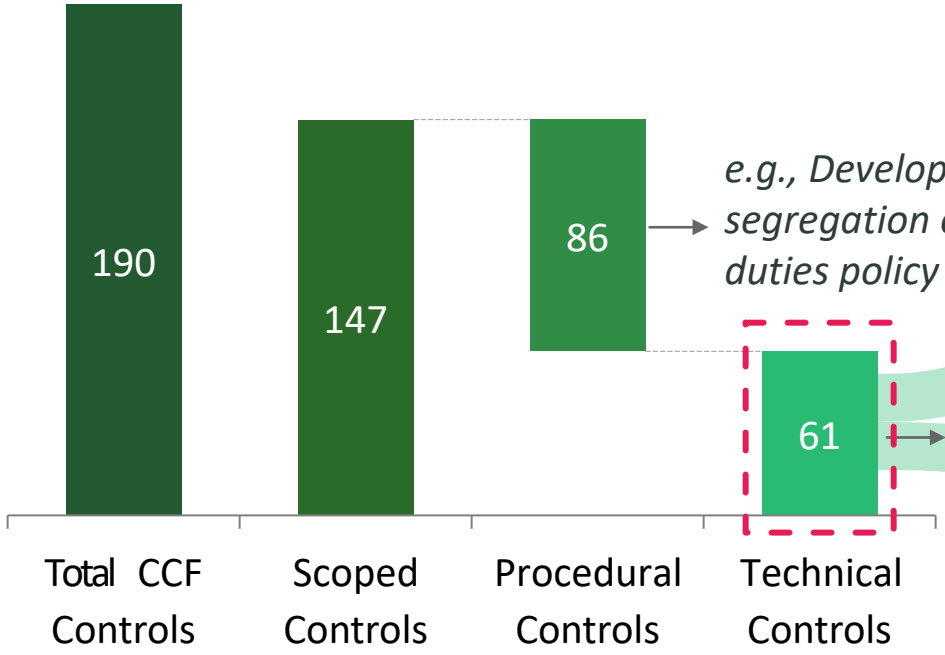
Developers save time by using Pre-Approved Security Plans, & are honored for adding new Plans to the library



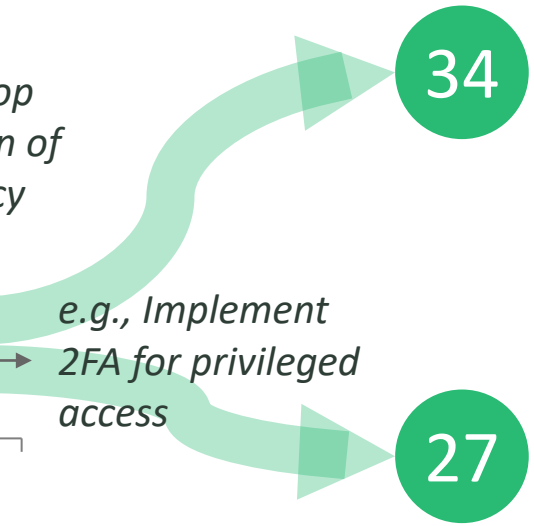
Michael Coden Colin Troha Philipp Krayenbühl

Actual application results: >80% of controls were reusable and 56% of technical controls were automated

Identified 61 scoped technical controls…



… ~60% of which can be automated[1]



Controls are at least partially automatable

- May be set via an API call to cloud service provider
- e.g., log retention set to 180 days

Controls require user action to implement

- Cannot be directly configured via API call
- e.g., configure Role Based Access Security

1. ~16% total control coverage when based on 190 controls

Michael Coden Colin Troha Philipp Krayenbühl

Swiss Re open sourced the SR-CSF through Cyber Risk Institute; BCG has seen excellent results using SR-CSF at numerous clients

Actual client results:

~50%
reduction in developer time implementing security controls due to automation[2]

~67%
Reduction in application approval time due to standardized security guardrails[3]

$48k+
per year per application in operations savings weeks[1]

(~$4.8M annual savings for a company with 100 applications)

Download the SR-CSF at:
cyberriskinstitute.org/the-profile/

1. Due to technical automation of checking controls, time spent by audit team in auditing applications was reduced by 3 weeks. 2. ~60% of security controls were able to be automated, reducing the time spent by developers from 2 weeks to 1 week due to the automated configuration. 3. Previously average application approval time was 6-12 weeks depending on the application complexity, and the standardized guardrails reduced this to 2-5 weeks.

BCG Michael Coden Colin Troha Philipp Krayenbühl Swiss Re

RSAConference2022

Apply

Our lessons learned and how you can apply them to your organization

Key lessons learned

- Involve all stakeholders from the beginning of your cloud security process development
- Be agile – put a project through your process early – evaluate, refine and try again
- Use existing automations of stakeholders as much as possible – it “primes the pump” and gets the community engaged more quickly

Over to you to apply in your organization

- Next week you should:
  - Understand how central cloud will be in your org's strategy and how much you're investing in cloud security
- In the first three months following this presentation you should:
  - Define relevant regulations and standards
  - Transform your applications to take advantage of serverless environments
  - Define reusable security patterns
  - Design resilience into all applications
- Within six months you should:
  - Design your Cloud Security Framework and operationalize it

RSAConference2022

Suggested Next Steps

- **Review and enhance scalability for serverless cloud environments**
- **Review and enhance "Cyber-Resilience by Design"**
  - **Enabling even more rapid cyber event detection**
  - **Enabling even more rapid business continuity/recovery**

Michael Coden: Coden.Michael@advisor.bcg.com

Philipp Krayenbühl: Philipp_Krayenbuehl@swissre.com

Colin Troha: Troha.Colin@bcg.com

Thank you for joining our presentation!

Q&A