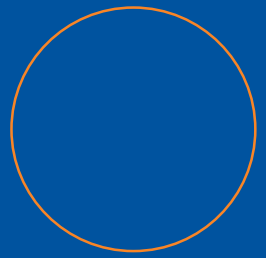
Addressing Challenges to Cloud Security Governance

Redefining Cloud Security Governance in the Digital Era

PRESENTED BY

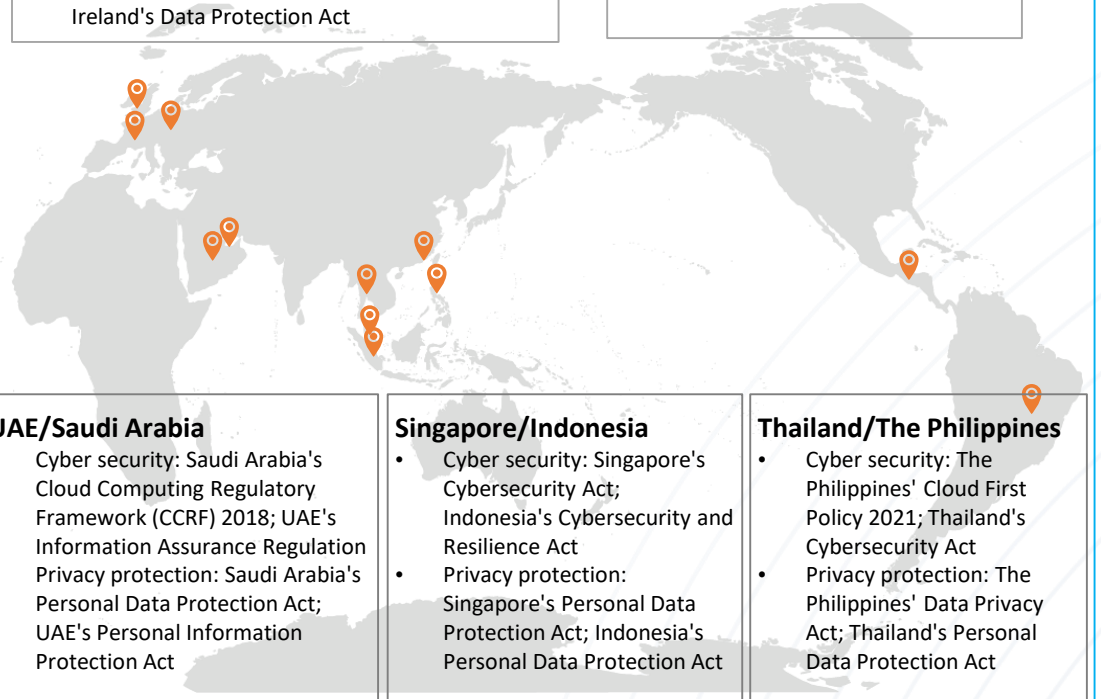


Challenges to Cloud Security Governance — Stricter Supervision over Cyber Security and Privacy Protection Worldwide

Global: Differentiated personal data protection and localization of important data

Ireland/Germany/France
- Cyber security: EU NIS 2 Directive; EUCC Scheme; EU Cybersecurity Act; Germany's IT Security Act 2.0
- Privacy protection: EU General Data Protection Regulation (GDPR); EU ePrivacy Regulation; Ireland's Data Protection Act

Brazil/Mexico
- Cyber security: Brazil's National Cybersecurity Strategy
- Privacy protection: Brazil's General Data Protection Act; Mexico's Data Protection Act



UAE/Saudi Arabia
- Cyber security: Saudi Arabia's Cloud Computing Regulatory Framework (CCRF) 2018; UAE's Information Assurance Regulation
- Privacy protection: Saudi Arabia's Personal Data Protection Act; UAE's Personal Information Protection Act

Singapore/Indonesia
- Cyber security: Singapore's Cybersecurity Act; Indonesia's Cybersecurity and Resilience Act
- Privacy protection: Singapore's Personal Data Protection Act; Indonesia's Personal Data Protection Act

Thailand/The Philippines
- Cyber security: The Philippines' Cloud First Policy 2021; Thailand's Cybersecurity Act
- Privacy protection: The Philippines' Data Privacy Act; Thailand's Personal Data Protection Act

China: Systematic legislation, regular inspection, and precise law enforcement

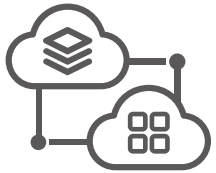
Higher-level legislation (Law)	Cybersecurity Law June 2017	Data Security Law September 2021	Personal Information Protection Law November 2021
	Sector-specific	**Government-specific**	
Lower-level legislation (Regulation)	Network Data Security Management Regulations (Draft for Comments)	xx	
	Measures for Data Security Management in the Industry and Information Technology Sector (for Trial Implementation)	XX	
	Several Provisions on the Management of Automotive Data Security (for Trial Implementation)	Guizhou Big Data Security Assurance Regulations	
	Financial Data Security — Guidelines for Data Security Classification (JR/T 0197-2020)	Measures for Security Management of Chongqing e-Government Cloud Platform (for Trial Implementation)	
	...	...	

Challenges to Cloud Security Governance — Rapid Development of Huawei Cloud Business Leading to Greater Challenges

One of the **top 5** cloud service providers **worldwide** in terms of business scale

Cloud services
220+

Solutions
210+



Marketplace offerings
4500+

Support for numerous services **critical to the national economy and people's livelihood**

Government

Energy

Finance

Manufacturing

Transportation

Education

Healthcare

Media

Internal: Operations security of Huawei as a hyperscaler

Security Challenge

External: Security and compliance assurance for numerous customers

Huawei Cloud's Consideration

"How can we continue implementing **cloud security governance living up to the highest standards** while maintaining such a huge product line and business scale?"

Summary of Challenges to Cloud Security Governance

Excessive security compliance requirements, repeated execution, and low maintainability

Security professional

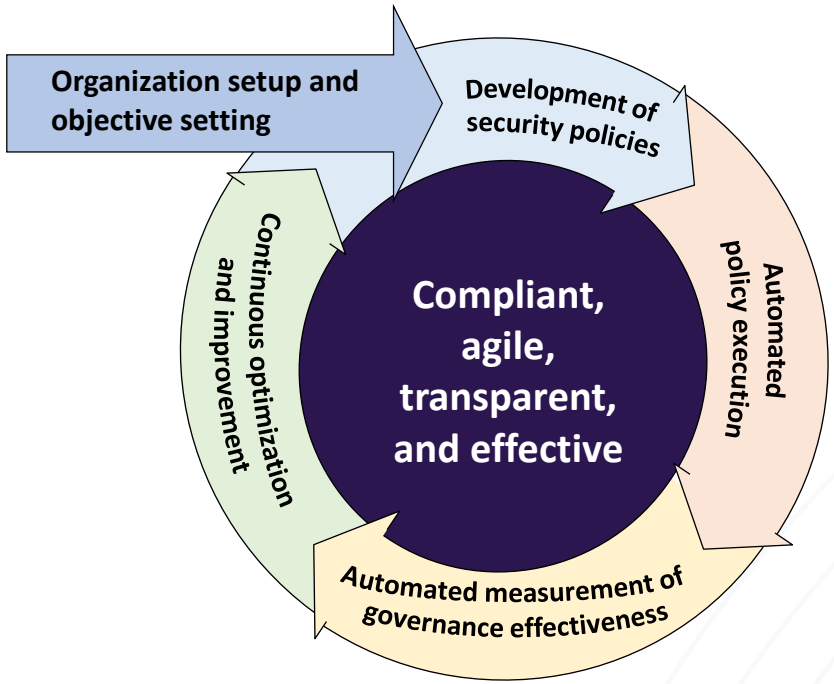
Inefficient security governance and costly ex-post rectification

Business personnel

Invisible governance process and lack of evaluation criteria for governance effectiveness

Senior management

Redefining Cloud Security Governance in the Digital Era



- **Build a unified compliance library (3CS)** that integrates all applicable security requirements and regulations.
- **Implement automated execution of Policy as Code (PaC)** and embed efficient security governance into business processes.
- **Promote improvement via measurement** and implement digital operations of security governance.

3CS as a Unified Compliance Library

Huawei Cloud 3CS Framework

3CS =

CLOUD **S**ERVICE **C**YBER**S**ECURITY & **C**OMPLIANCE

STANDARD

Features:

- Closely integrated with cloud service processes
- Auditable, traceable, measurable, and constantly optimizable
- Built upon the strengths of multiple mainstream security management standards
- Based on Huawei's 30 years of security management experience and technology achievements

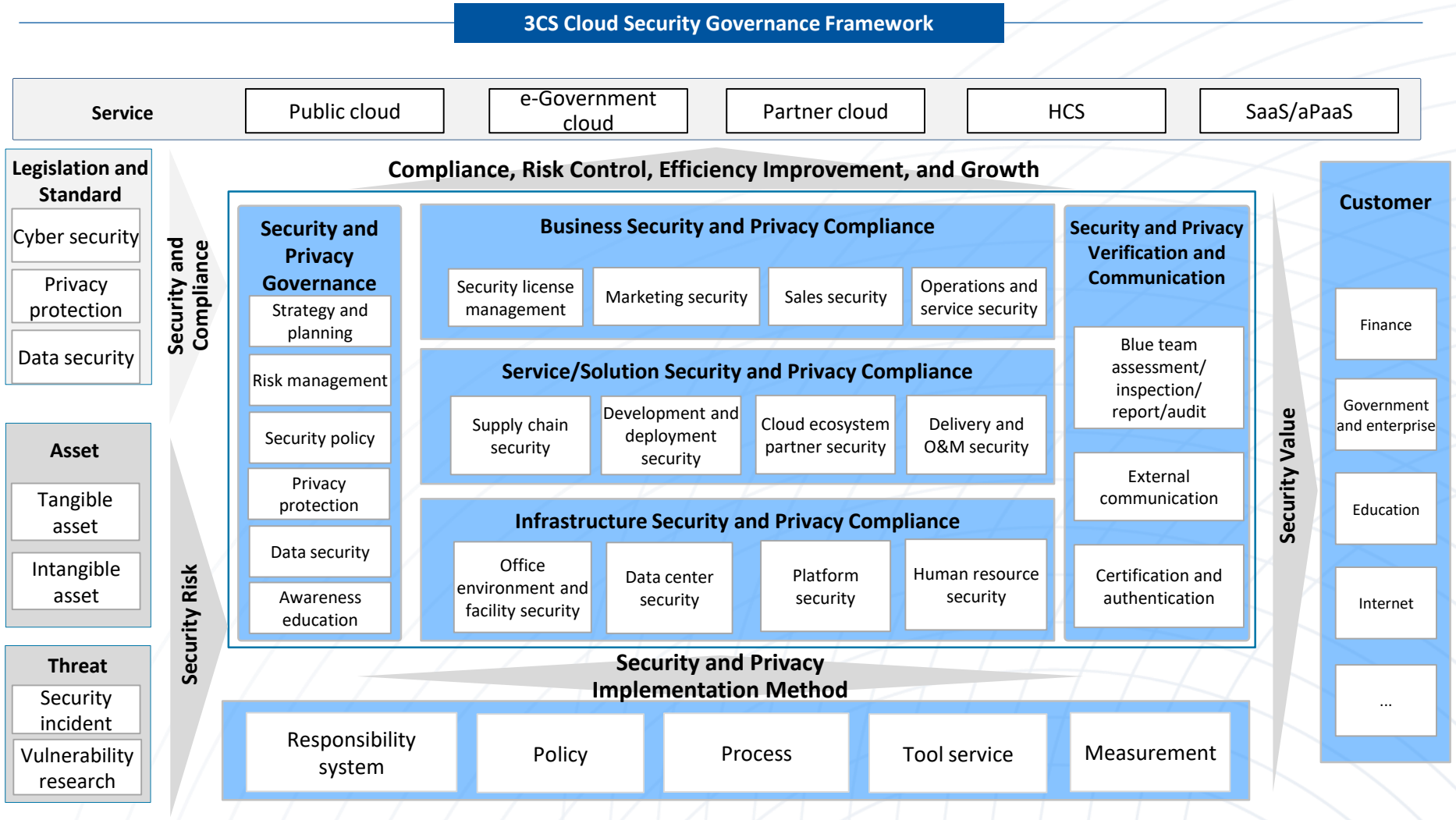
3CS — Overall Framework of Cloud Security Governance

20+ security standards worldwide

- CSA STAR (CCM)
- ISO/IEC 27001
- ISO/IEC 27017
- CSA CoC for GDPR
- ISO/IEC 27018
- ISO/IEC 27701
- AICPA SOC 2
- NIST CSF
- NIST SP 800-53
- COBIT 2019
- CIS Controls
- PCI DSS
- Germany C5
- Singapore SS 584 (MTCS)
- GB/T 22239-2019
- GB/T 31168
- ISO/IEC 27034
- ISO 27799
- ISO/IEC 29151
- PCI 3DS
- OSPAR
- TISAX
- ...

+

Huawei Cloud's practices



3CS — Cloud Security Governance Controls

Gradual breakdown, step-by-step execution, and easy implementation

Level-1 requirements:

- Specify management priorities and objectives.

Level-2 basic requirements:

- Specify countermeasures.

Supplementary requirements:

- Refine key execution points.

Description:

- Provide explanations and remarks.

Guidelines:

- Check the implementation effectiveness.

Example

Level-1 No.	Topic	Level-1 Requirement	Level-2 No.	Level-2 Requirement	Key Elements	Remarks
1.4.6	Data transmission	CSPs should implement technical measures to ensure the security of in-transit data.	1	CSPs should identify scenarios where data must be encrypted for transmission based on data categories and levels.	Such data includes but is not limited to: - Personal information or sensitive data transmitted over the public network - E-commerce and online transaction data transmitted over the public network and data involved in non-console administrative access - Data managed, imported, and exported by interoperability and portability systems (including cloud platforms)	Non-console access refers to access from local/internal networks, as well as access from external/remote networks. In other words, it refers to access to the systems over networks.
			2	CSPs should implement the following technical measures to ensure the authenticity, confidentiality, and integrity of in-transit data in identified scenarios: - Ensure authenticity by authenticating the communicating parties before the communication is established. - Use secure protocols, ensuring that these support secure versions and configurations. - Encrypt sensitive data for transmission or use secure transmission channels or protocols.		Currently, secure protocols include TLS, IPsec, and SSH. However, the following protocol versions have been verified as insecure: SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, SSHv1, IKEv1, etc. The following measures are also available based on data sensitivity: - Block the exchange of restricted data. - Suspend the transmission of data that may be confidential. - Report suspicious data transmission activities to designated personnel.
			3	Cross-border data transfers should comply with local laws and regulations, and be documented.		CSPs should comply with security management regulations related to cross-border data transfers.

Measurement-driven Improvement — Evaluation of Cloud Security Governance Effectiveness Based on 3CS

3CS Compliance Library

- **Cloud service security governance**
- Security strategy and planning
- Security management organization
- Risk management
- Data security
- Privacy protection
- Assessment and audit

Result Indicator

- High risk control rate
- Risk reproduction rate
- Risk treatment rate
- Number of data security incidents

Operations Indicator

- Incident and risk identification rate
- Risk treatment decision-making rate
- Number of data use violations
- Important data monitoring coverage rate

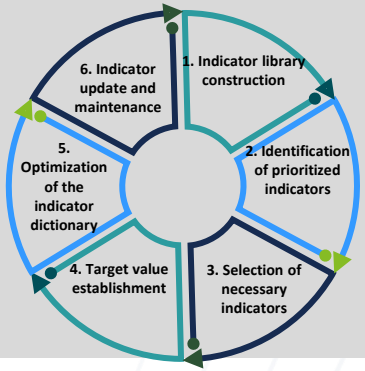
Process Indicator

- Risk grading rate
- Risk assessment coverage rate
- Risk monitoring coverage rate
- Data identification coverage rate
- Data backup coverage rate
- Recovery exercise coverage rate

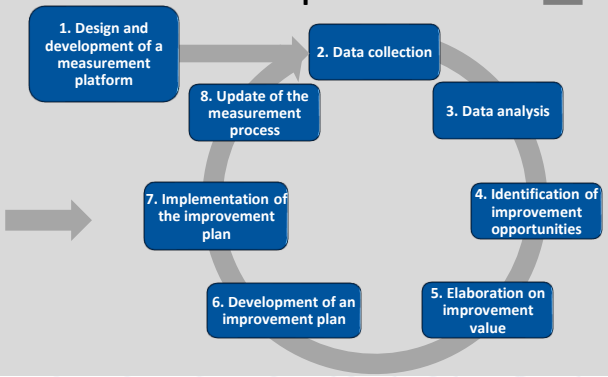
Measurement Planning

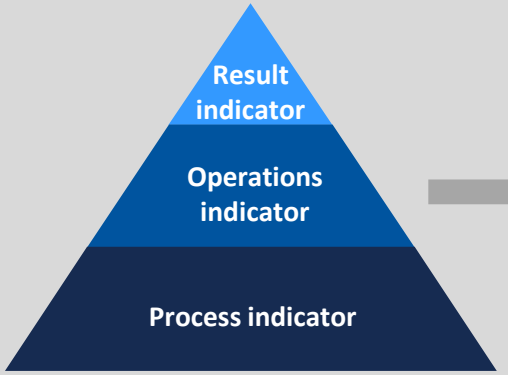
- Organization/Role
- Policy file
- Process cycle
- Technology/Tool

Measurement Design



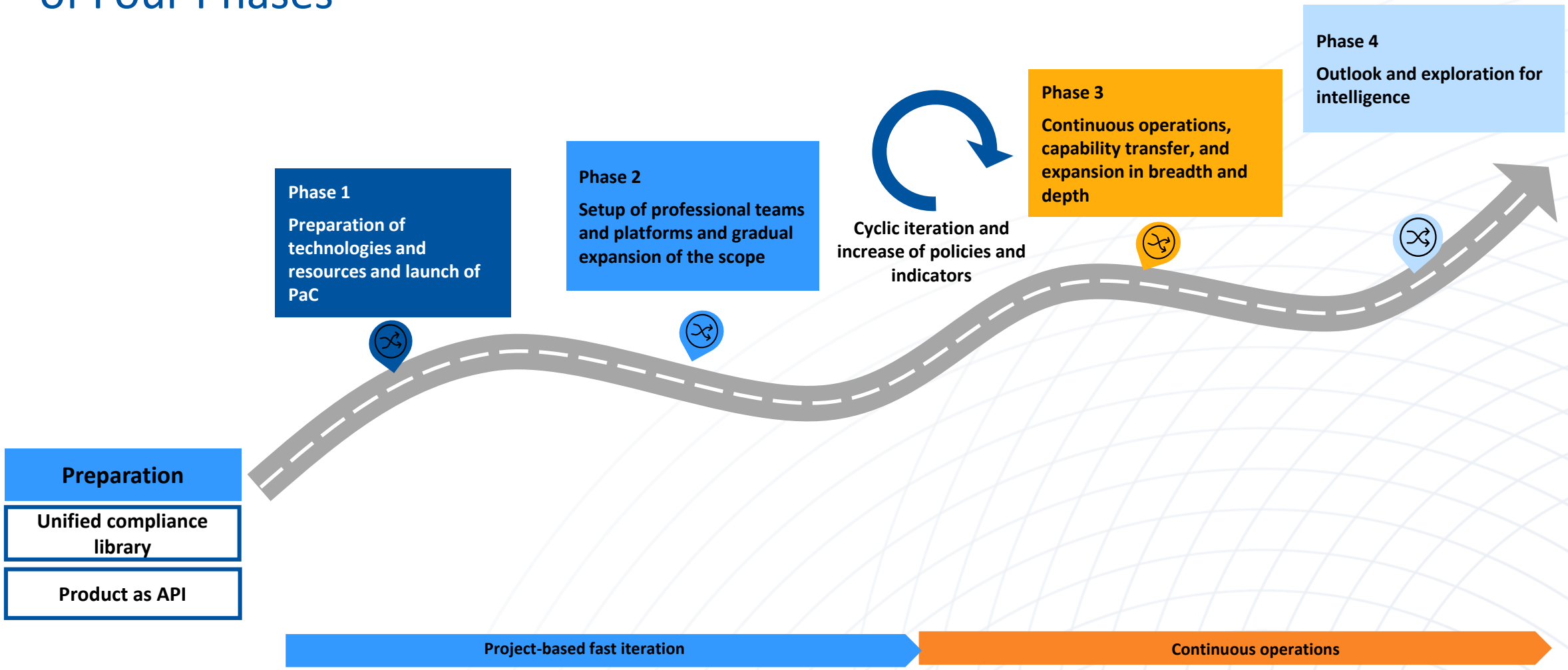
Measurement Implementation





- Effectiveness
- Capability
- Measure

Suggestions on Cloud Security Governance in the Digital Era — Eleven Steps of Four Phases



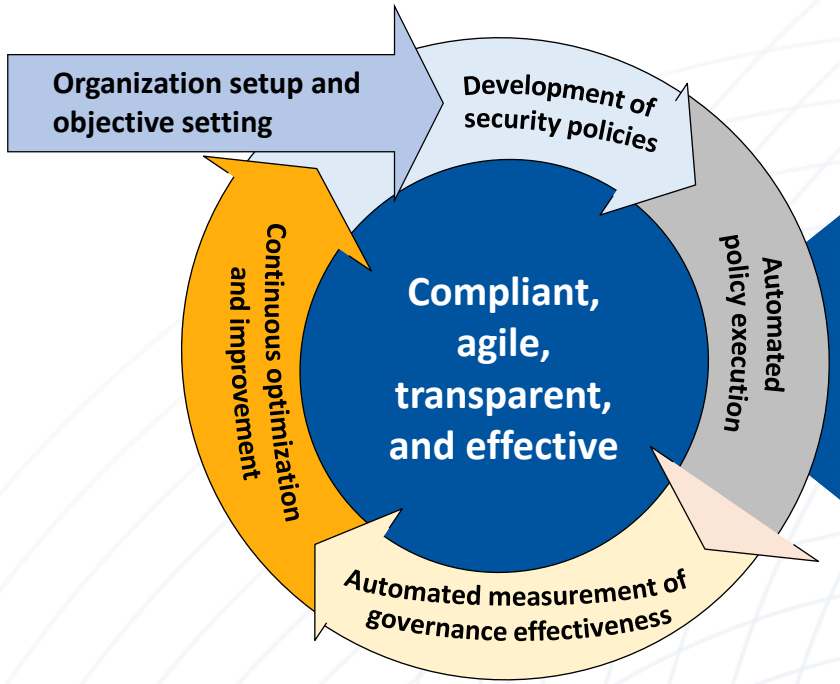
Outlook for Cloud Security Governance in the Next Three to Five Years

Compliant — Intelligent policy generation

Agile — Automated issue correction

Transparent — Real-time evaluation of effectiveness

Effective — Integration with business



AI-powered cloud security governance

Efficient

Proactive

Flexible

Adaptable

Thank You!