



Cyber Cloud

Deloitte in Cyber Risk Services

Deloitte continues to drive outstanding performance and strengthen our market-leading position

1 Leader for Security Consulting Services for **the 10th year in a row**, Worldwide, based on market share, in 2021

Source: Gartner, Market Share: Security Consulting Services, Worldwide, 2020, Elizabeth Kim, Shawn Eftink 11 June 2020



9,500+

Cyber Risk engagements in 2020 across all major industries

Deloitte named a leader in Information Security Consulting Services by Forrester for the 5th consecutive wave and a leader in Managed Security Services 2020 Vendor Assessment

Source: The Forester Wave: Global Cybersecurity Consulting Providers, Q2 2019

Source: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment by Martha Vazquez, September 2020.

1,400+

Certified Information Systems Security Specialists (CISSPs)

150+

Certified Information Privacy Professionals (CIPPs)

“Deloitte has a depth of experience, a wide span of managed security services, and a large ecosystem of vendor partnerships.”

Source: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment by Martha Vazquez, September 2020.

Built by our people



30+

Cyber Intelligence Centers

21,000

Risk management and security professionals globally through the Deloitte Touche Tohmatsu Limited (DTTL) network of member firms

7,000+

Global Cyber Risk practitioners **backed by 10,000+** practitioners with a security focus in other supporting areas



5+

Regional Delivery Centers Collaborating with leading government agencies and industry associations on Cybersecurity standards, advanced threat solutions, and cyber resilience practices



EMEA Cybersphere Center



500+ practitioners
28+ nationalities



217+ managed security services engagements

26

countries working collaboratively with the ECC in 2Q FY19 (70% growing rate)



A SOC
(Security Operation Center) with high quality standards:
FIRST® CERT®
ISO 22301®
ISO 27001®

Avoid becoming breaking news

Data Breaches in the Cloud: Who's Responsible?

"Although organizations can mitigate or reduce the risk of a breach by vetting cloud provider security practices and conducting audits of the data stored in the cloud, the majority of companies are not conducting these practices, according to the study. One reason is that the procurement process may be happening outside of IT's purview"

Jessica Hughes, govtech.com, August 26, 2014

- New Threats
- New Attack Surface
- Perimeter Gone
- Reliance on Providers

Apple Not Hacked—Photo Breaches—

usernames, passwords breached, Apple

"It's not surprising second factor of weak password

Kelly Jackson

Dropbox Patches Shared Links Privacy Vulnerability

"Dropbox has acknowledged and disabled a vulnerable shared links feature that exposed documents stored by the service to third parties."

Michael Mimoso, threatpost.com, May 6, 2014

AWS console breach leads to demise of service with "proven" backup plan—Code Spaces closes shop after attackers destroy Amazon-hosted customer data.

"A code-hosting service that boasted having a full recovery plan has abruptly closed after someone gained unauthorized access to its Amazon Web Service account and deleted most of the customer data there."

Dan Goodin, arstechnica.com, June 18, 2014

The time you need for remediation decides very likely if you get into headline news

Who's responsible for our data in the cloud?

Cloud and the security of data are important, but there is government intervention in hacking, politically motivated hacking and error. All these are things raise the

September 4, 2014

cloud?

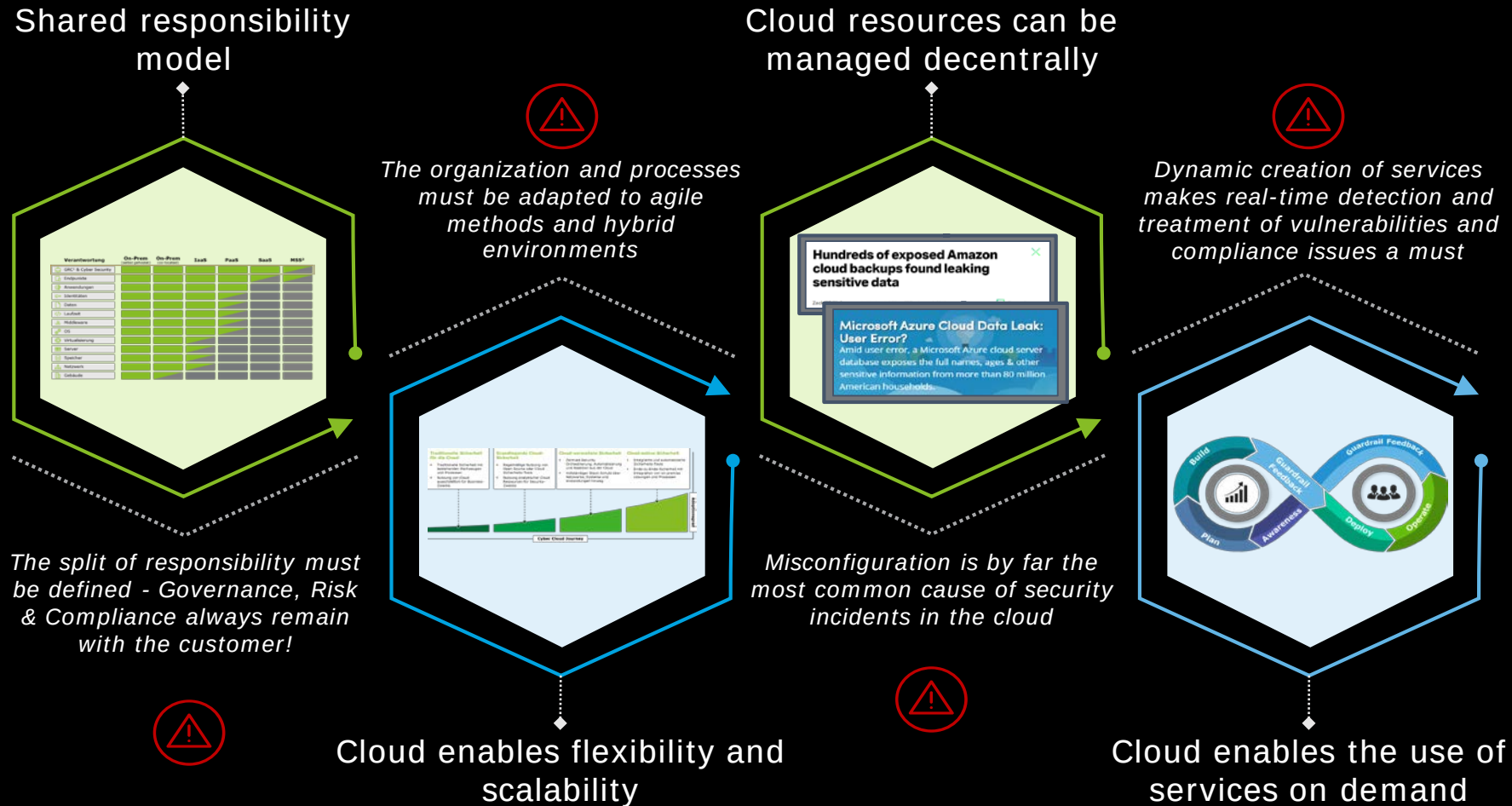
important,

particularly in a world where there is government intervention in personal data, nation state hacking, politically motivated hacking and just straightforward operator error. All these are things raise the stakes."

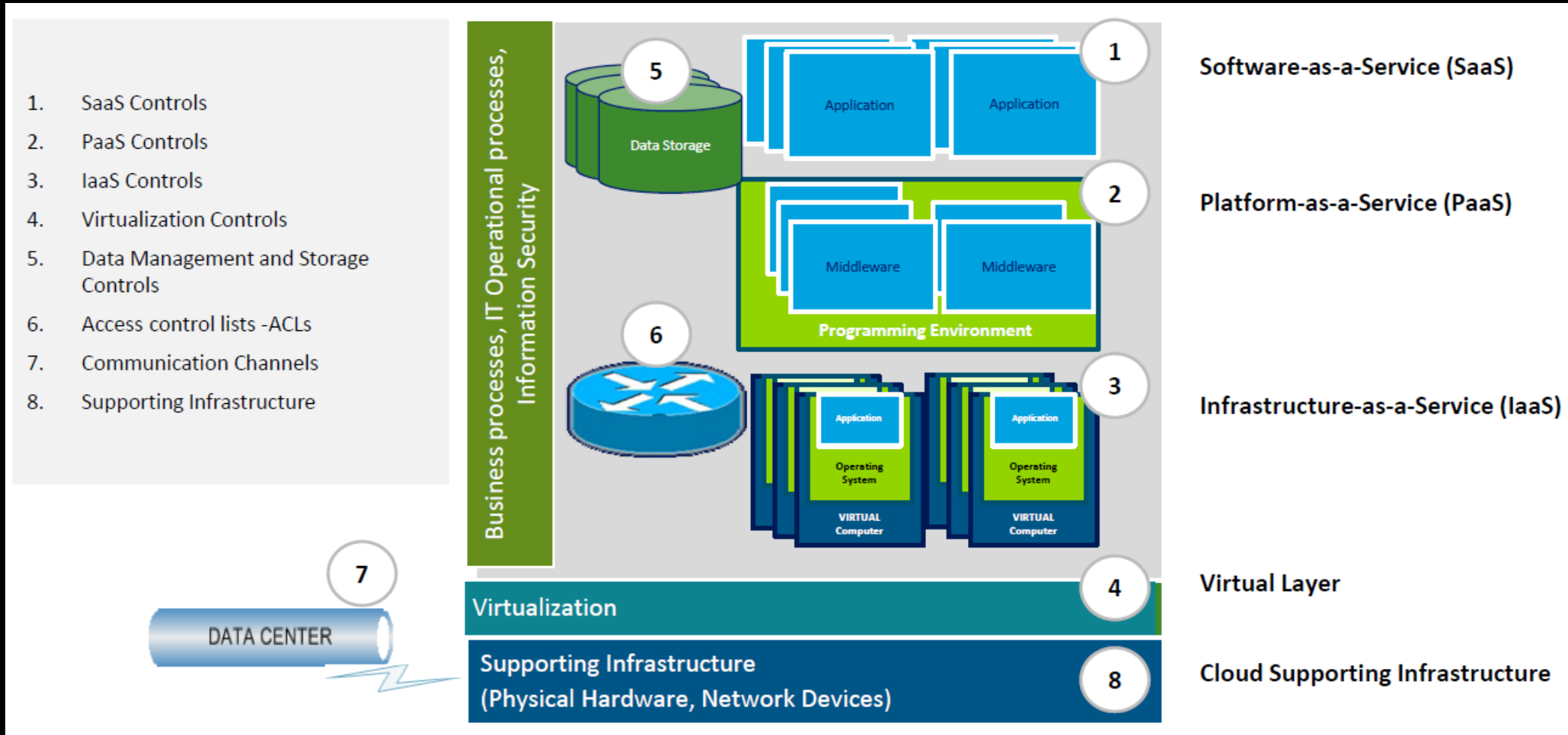
Robert Bond, legalweek.com, December 4, 2014

Challenges of Cloud Security

Cloud is all about **speed** and **dynamic**. Governance, risk, and compliance need to answer at the speed of cloud or is significantly lost.



Are simple controls enough?



Deloitte's Cloud Cyber Risk Framework

Deloitte's Cloud Cyber Risk Framework offers a holistic view of the cloud security capabilities of an organization and helps to identify key strengths and weaknesses.

Input (selected)

Industry Standards

- o ISO¹ 27001/2
- o NIST² Cybersecurity Framework
- o Cloud Controls Matrix CSA³

Leading Practices

- o Existing Cloud Frameworks
- o Relevant Project experience
- o Benchmarks (CIS⁴)
- o Hyperscaler Security Best Practices

Threat intelligence

- o Who are relevant attackers?
- o What are the likely targets?
- o What are the likely attack path?

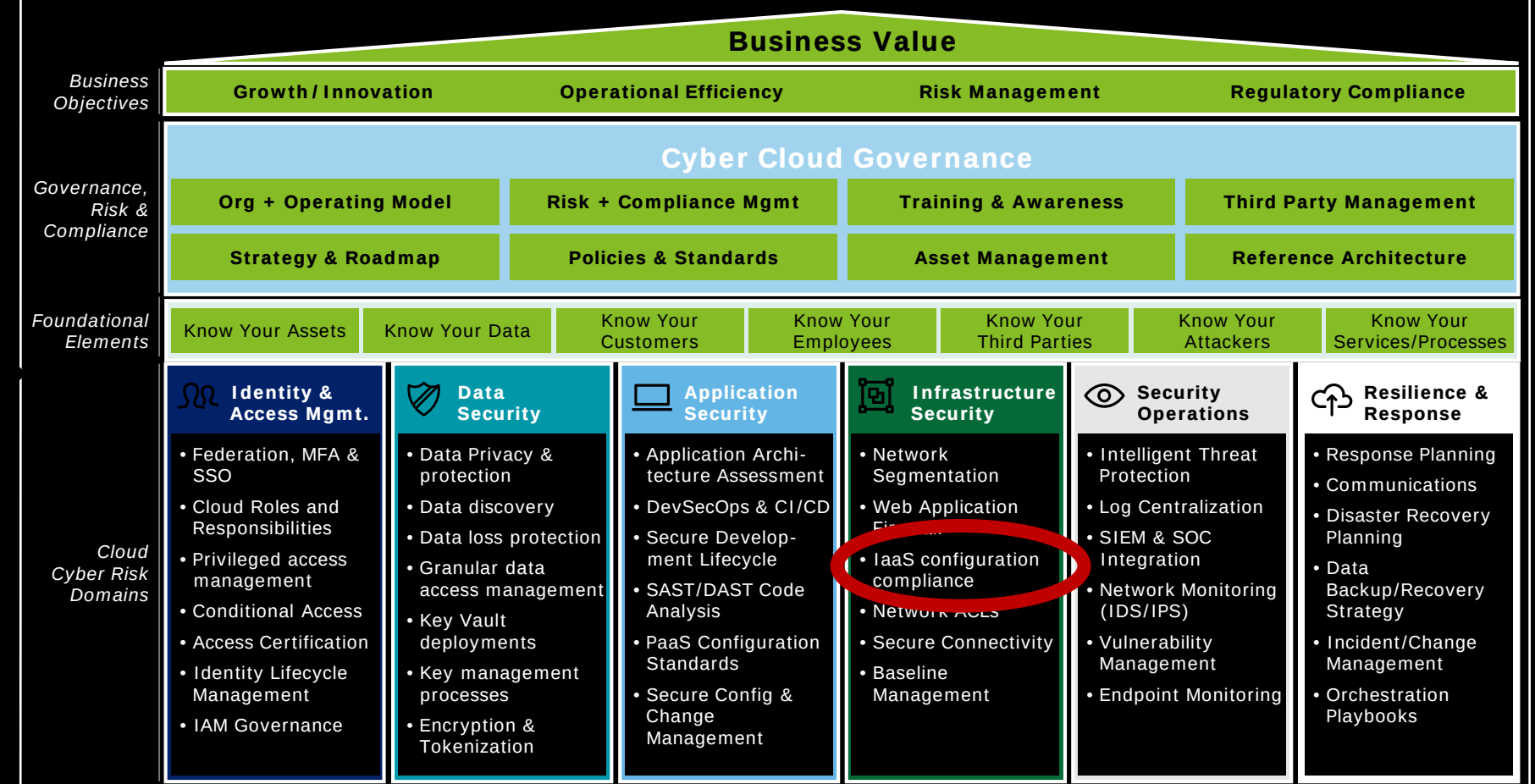
¹ International Organization for Standardization

² National Institute for Standards and Technology

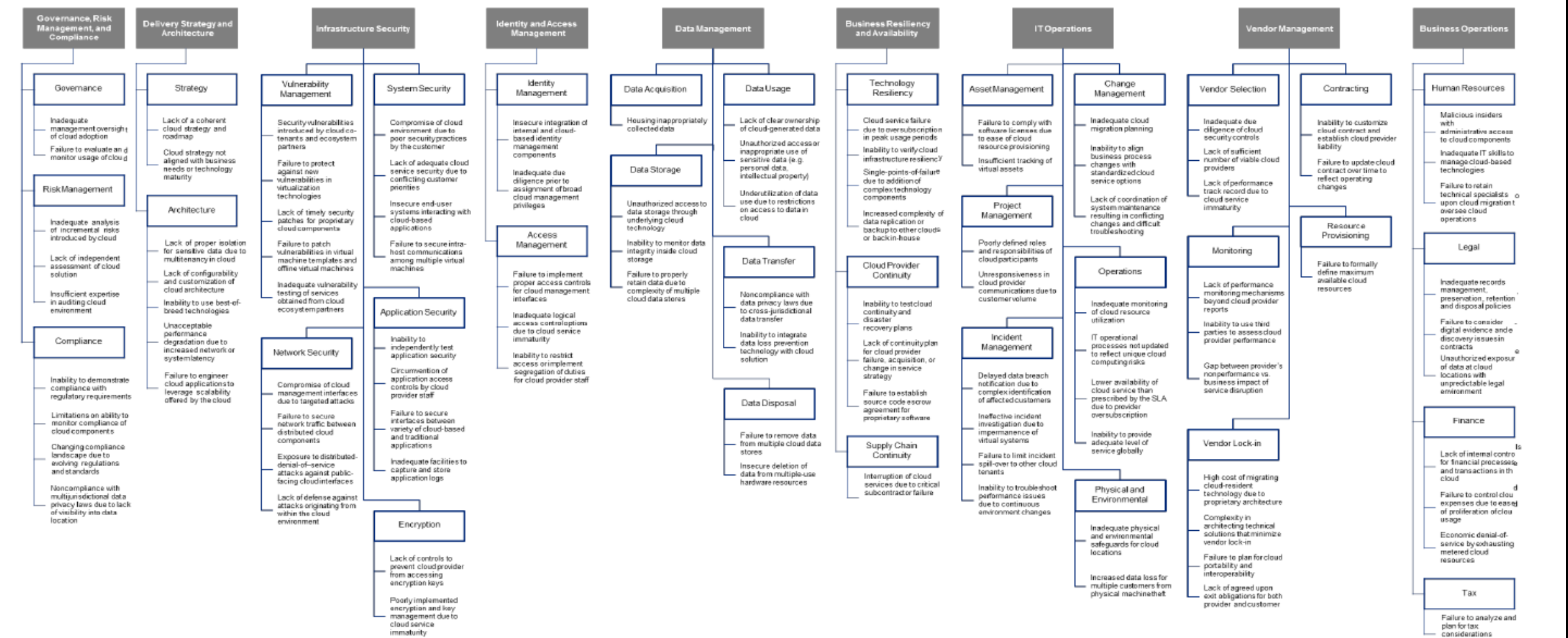
³ Cloud Security Alliance

⁴ Center for Internet Security

Deloitte Cloud Cyber Risk Framework



Deloitte Cloud Computing Risk Intelligence Map



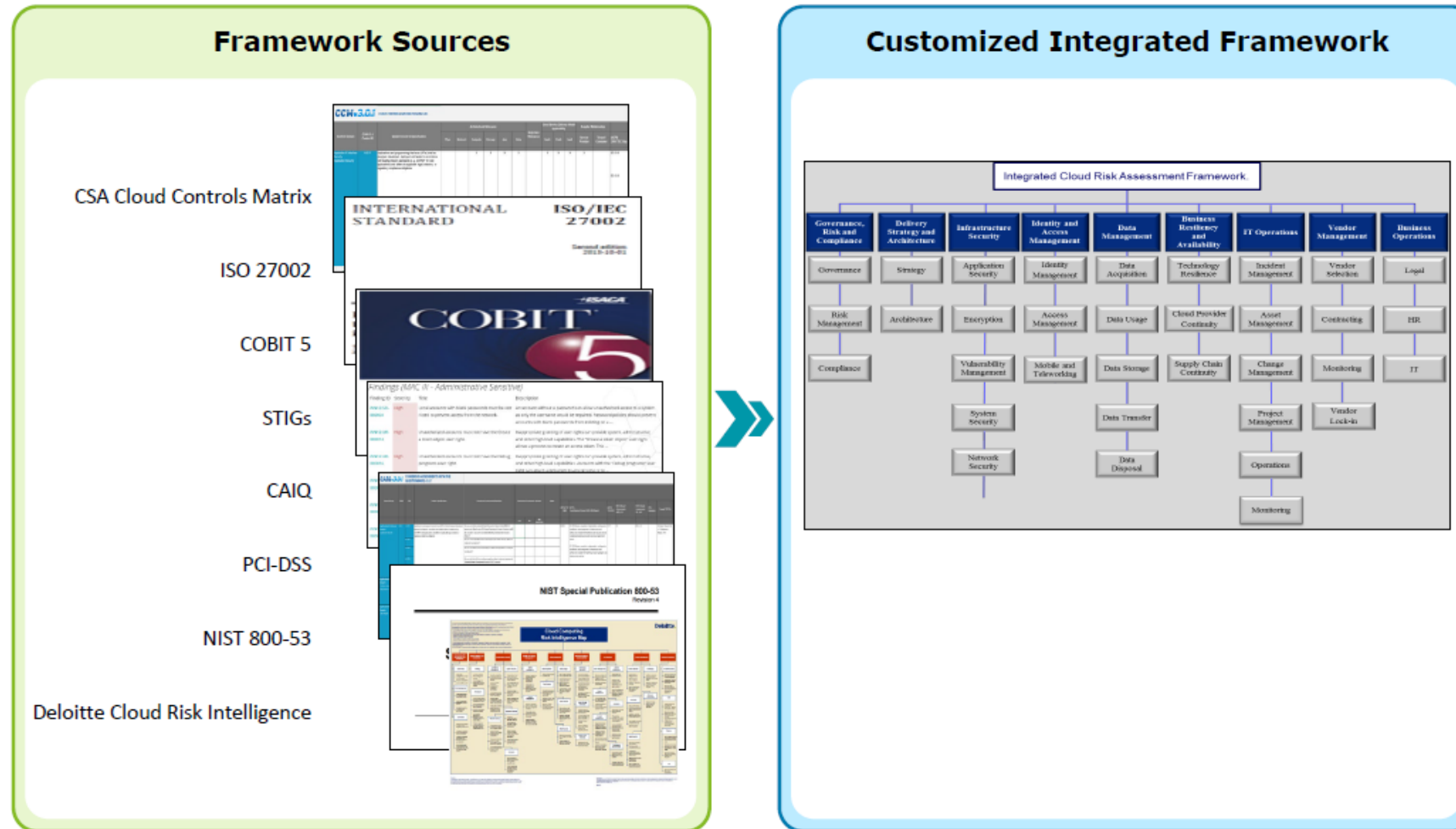
Disclaimer

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Cloud Security
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a separate legal entity. Please see <https://www.deloitte.com/uk/en/about-us/deloitte-network> for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see <https://www.deloitte.com/uk/en/about-us/deloitte-network> for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.
Copyright © 2019 Deloitte Development LLC. All rights reserved.
Deloitte or Deloitte Touche Tohmatsu Limited
Version 1.0
Item #228

Cloud Cyber Risk Framework customization

Based on authoritative sources and leading practices, a customized, organization-specific cloud risk framework should be developed to evaluate cloud vendors.

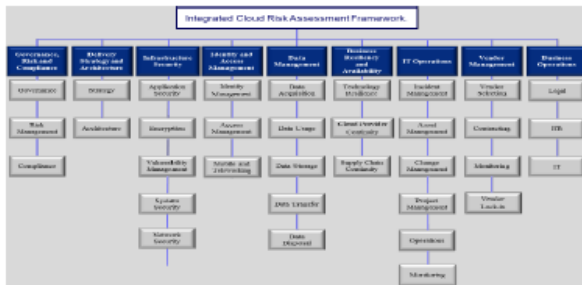


Cloud Vendor Risk procedure

Based on authoritative sources and leading practices, a customized, organization-specific cloud risk framework should be developed to evaluate cloud vendors.

1. Assess

Use vendor artifacts to assess risks against customized cloud risk framework



Cloud questionnaires, SOC 2 reports, cloud vendor policies, procedures, standards, etc.



Interviews and workshops

2. Identify

Identify and document gaps/risks of each cloud vendor



Regulatory/Compliance risks

+



Incident response risks

+



Data protection risks

+

.

.

.

3. Mitigate

Document controls and response to identified risks



Contract terms updates



Additional controls

Configuration Management & Compliance

One of the highest priority risks: misconfiguration of cloud services

A HIGH-RISK THREAT VECTOR...

In-line **injection of infrastructure vulnerabilities** by DevOps teams to the public cloud in addition to manual configuration errors pose risks to cloud services.

Due to Continuous Integration / Continuous Deployment (CI/CD) **automation, vulnerabilities can potentially be deployed at scale in the public cloud.**

In a **matter of minutes, misconfigurations can be exploited** and lead to **data breach** or service disruption.

Traditional CI/CD without automated security controls



Objectives to be met



Address security issues at the speed of cloud

Enable a time-constrained security team while keeping pace with DevOps teams using automation



Deploy technical controls aligned with compliance requirements

Align preventative, detective, and corrective controls with regulatory and enterprise security requirements



Gain real-time visibility to compliance issues

Analyze compliance posture across cloud environments, as well as, accountability across users to address issues

Automation & Orchestration as foundational capabilities

Cloud native security: leverage the advantage of cloud like up-to-date standardized logs, accurate asset data, and fully programmable configuration for security!

1. Baseline the cloud security controls framework

2. Cloud compliance monitoring using Cloud Security Posture Management (CSPM) capabilities



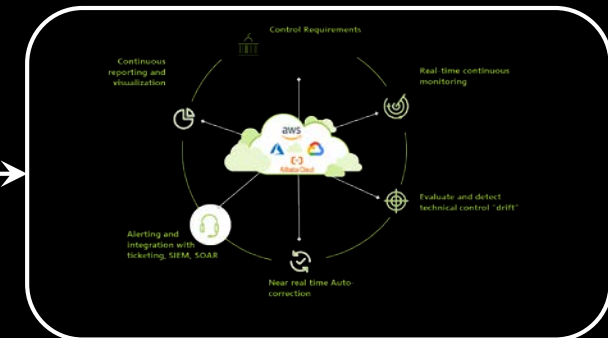
Monitor for misconfiguration of resources which may leave environments susceptible to attacks within minutes

3. Establish continuous Cloud Compliance Metrics and Analytics

Policy Type	High	Medium	Low	Total
	6			
	5			
	4			

Analyze cloud security alert data to prioritize high-risk and high-volume alerts to address with automation

4. Implement security automation and orchestration

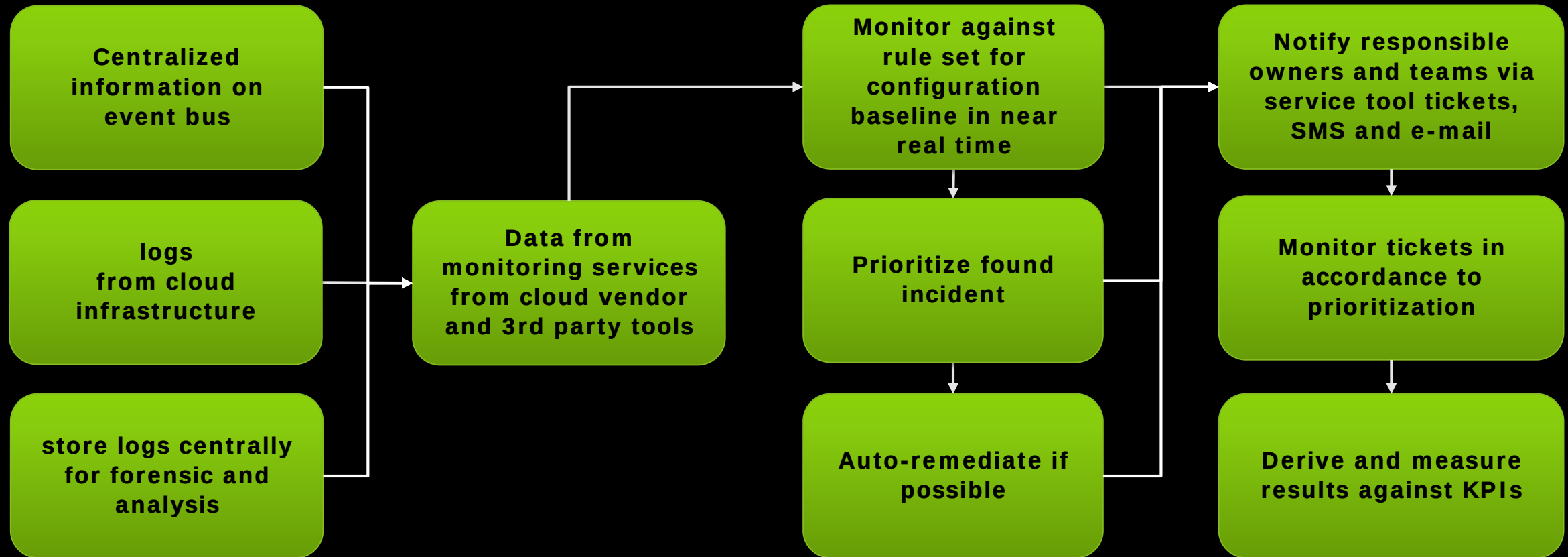


Implement structured workflows and automation of security tasks, preventative, detective, and corrective controls.

Security Operations Enhancements: CI/CD integration, secrets management, network protection updates, access control updates, incident response, SIEM triage

Cloud Configuration & Compliance Management

Example of one of our customers: > 1.000 AWS accounts, > 300 workloads services, > 3.000 developers as users, >200 baseline rules deployed



Cyber Cloud

We enable organizations to use cloud solutions safely in a dynamic environment and to fully exploit their potentials

Challenges



The increasing use of cloud creates new security incidents and challenges



Cloud services implicate new and altered challenges



Mitigation strategies and concepts must be adapted



Cloud is changing the way of how security must be anchored

Key offerings



Our expertise

Cloud First: The right approach?
(2019)
[Link](#)

Cloud-Risk and Compliance
(2019)
[Link](#)

The integration of cloud technology
(2019)
[Link](#)

Establish a cloud strategy
(2019)
[Link](#)

Additional resources

Deloitte cybercloud services

<https://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html>

Deloitte Fortress - automated cloud configuration and compliance management

https://www.youtube.com/watch?v=R__jRqHPQU4

Deloitte Risk Advisory services

<https://www2.deloitte.com/sk/sk/pages/riadenie-rizik/topics/kyberneticke-riziko.html>

Deloitte cloud Services overview

<https://www2.deloitte.com/us/en/pages/consulting/solutions/cloud-consulting-services.html>



Rudolf Klein
Senior consultant
Risk Advisory

Deloitte Advisory s.r.o.
Digital Park II
Einsteinova 23
851 01 Bratislava

Mobile: +421 917 632251
ruklein@deloittece.com

www.deloitte.sk

Thank you.

This publication contains general information only, and none of the member firms of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collective, the “Deloitte Network”) is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2021 Deloitte Development LLC.
All rights reserved. Member of Deloitte Touche Tohmatsu Limited