# Cloud Governance

**ISACA Information Security & Risk Conference**
**Halifax NS**

**November 2017**

KPMG

# Cloud Challenges and Benefits

# Cloud adoption and innovation is a top priority for our clients

| Cloud | Social networks | Information explosion | Mobility | Industry verticals as the 3rd Cloud platform |
|---|---|---|---|---|
| **21%** Estimated CAGR in SaaS market through 2018 | **82%** of Sales teams will adopt public social networks by 2016 | **100%** growth every two years, reaching 44 zettabytes by 2020 | **66%** of mobile apps developed in the next 3 years will be integrated with Enterprise Apps (Oracle, Microsoft, SAP) | **35%** High value industry solutions will become the 3rd platform for cloud expansion. (health, energy, Govt.) |

**40%** of enterprises IT dollars will be spent outside of IT by 2016 – Gartner

**$1** of every **$4** spent on applications will be consumed via the cloud by 2018 – IDC

**30%** of all new business software purchases will be service-enabled by 2018 – IDC

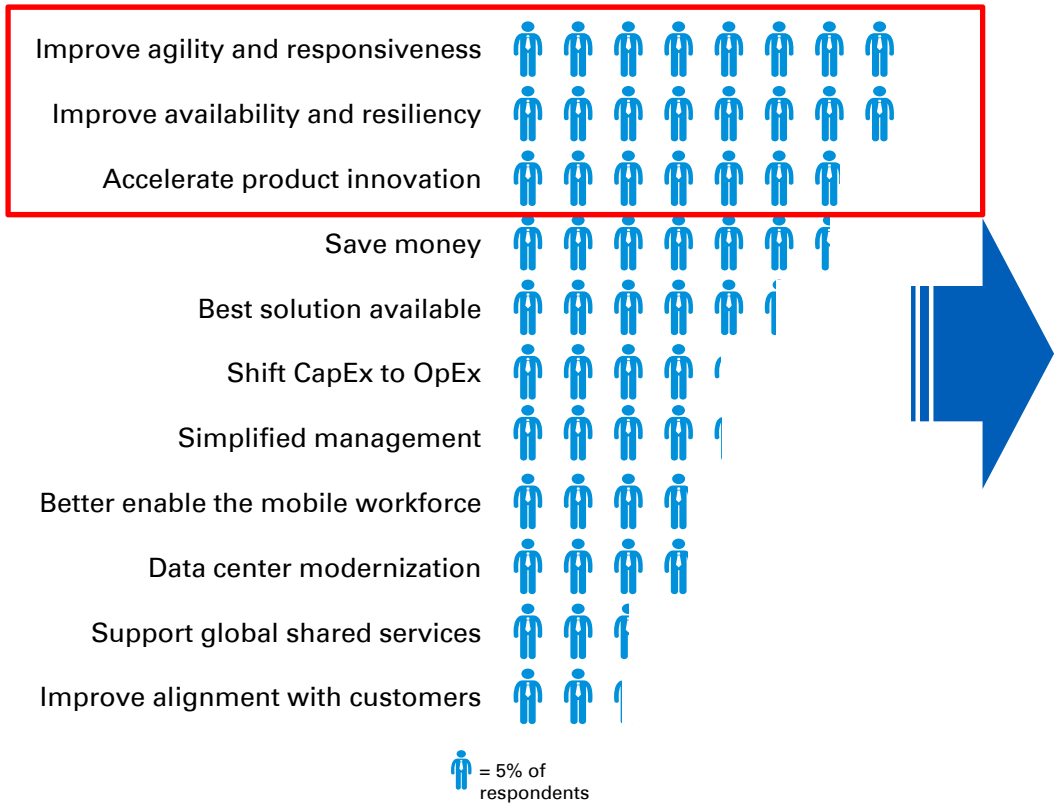
**70%** of the G2000 will still have 75% of IT resources running onsite by 2018 – IDC

**So what?**

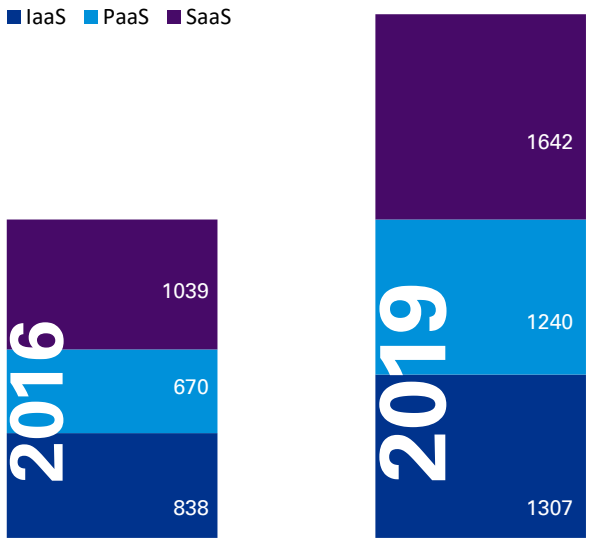
- Our clients are dealing with the question of how to adopt cloud. Significant portion of their budgets will go towards cloud.
- Cloud architectures are changing business models and require different thinking and solutions.
- Product, corporate IT, and business are transforming around cloud-based models.
- Security, risk, and compliance are top concerns.

# Desire for Cloud Benefits is Driving More Investment

***What are your top three reasons for using cloud technology?***




***CIOs Planning 'Significant Investment' in Cloud:***




Source: KPMG CIO Survey 2016

# …Leads to A Number of Challenges

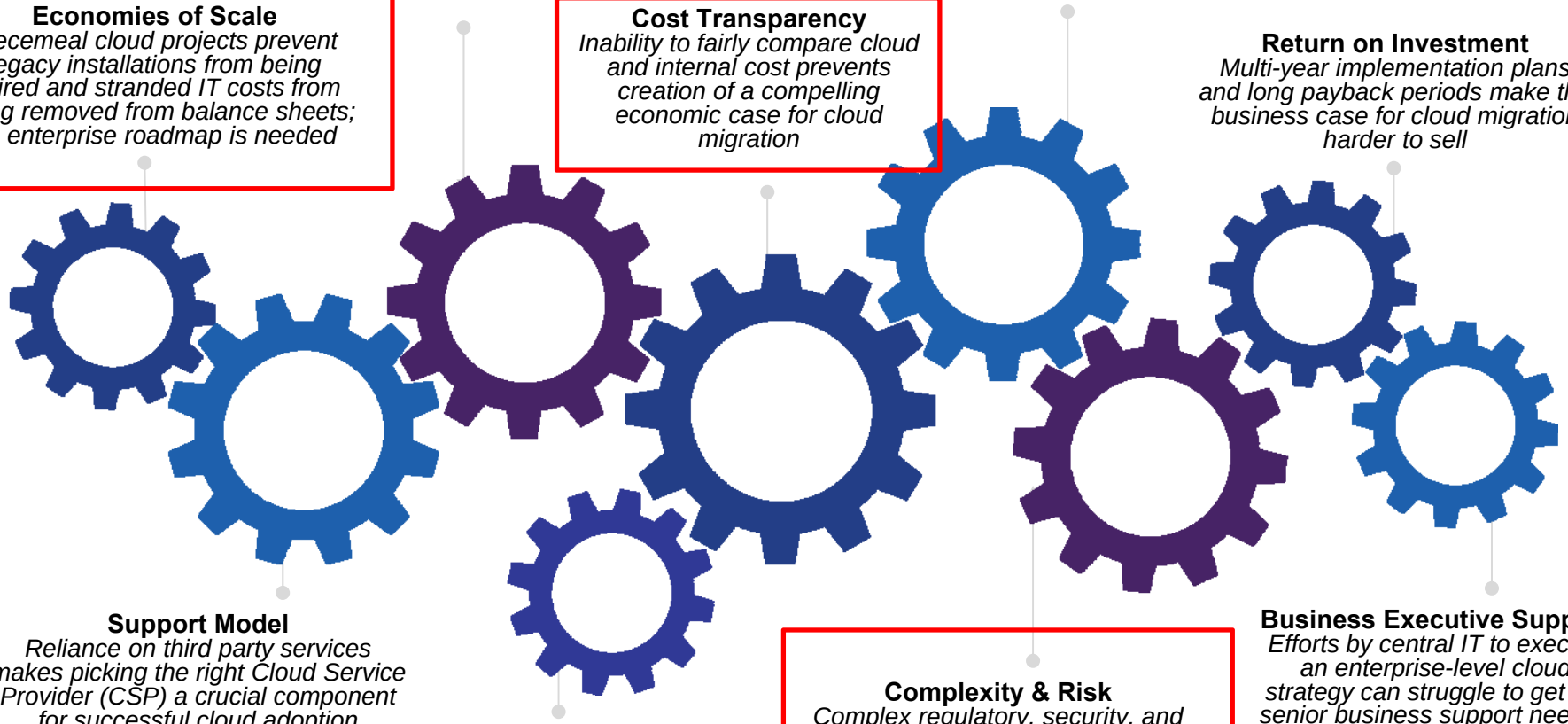
**Vendor Pressure**
*Vendors are overstating need to end support for on-premise solutions while pursuing market share*

**Organic Cloud Expansion**
*External (vendor) and internal (business unit) demands tend to focus on one-off solutions and ignore requirements of the enterprise*

**Economies of Scale**
*Piecemeal cloud projects prevent legacy installations from being retired and stranded IT costs from being removed from balance sheets; an enterprise roadmap is needed*

**Cost Transparency**
*Inability to fairly compare cloud and internal cost prevents creation of a compelling economic case for cloud migration*

**Return on Investment**
*Multi-year implementation plans and long payback periods make the business case for cloud migration harder to sell*



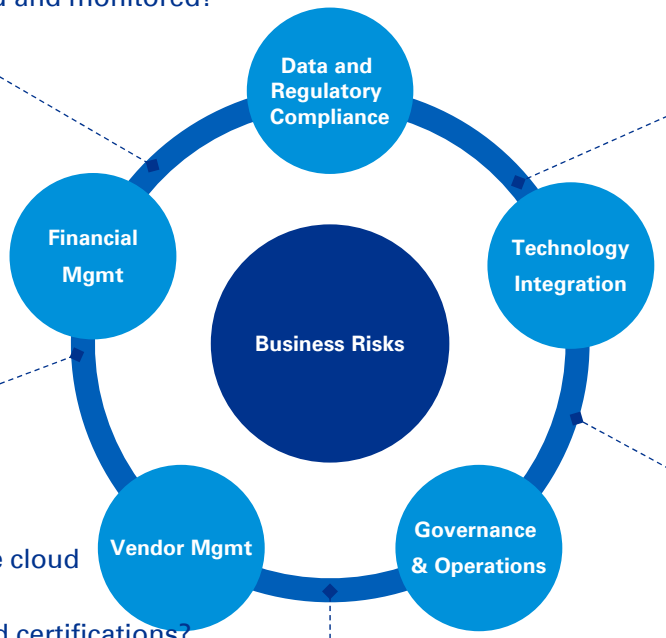
**Support Model**
*Reliance on third party services makes picking the right Cloud Service Provider (CSP) a crucial component for successful cloud adoption*

**Organizational Impact**
*Choice of cloud model could greatly impact, or eliminate the need for, members of the IT organization*

**Complexity & Risk**
*Complex regulatory, security, and information protection considerations, especially for multi-national corporations*

**Business Executive Support**
*Efforts by central IT to execute an enterprise-level cloud strategy can struggle to get the senior business support needed to overcome conflicts, reinforcing the status quo*

# Resulting in the following risks




- Do I know where my data is located in the cloud?
- Has data been classified as per company policies and secured accordingly?
- Am I aware of the compliance requirements to be met?
- Is member data appropriately isolated, segregated and masked?
- What accounts do I have in the cloud and is access to confidential data logged and monitored?

- How do I account for spending in the cloud and by who?
- What is my financial exposure?
- Is there a consistent approach to defining the business case for leveraging cloud solutions?
- Is there a clear process to predict and manage spending on cloud solutions?

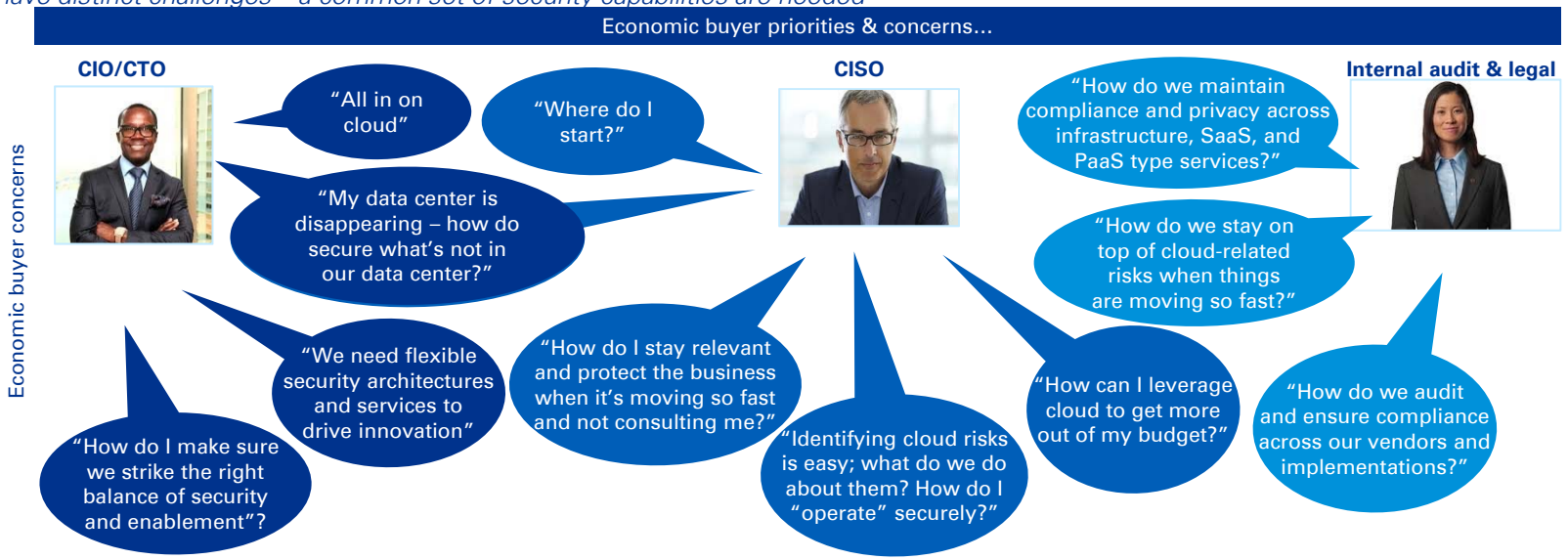
- Have I integrated the cloud environment to leverage existing IT and technology services?
- Are my production and development environment appropriately segregated?
- Do I have a process to monitor for evolving technology?

- Is there a clear process to manage cloud procurement?
- Does the vendor have the required certifications?
- How stable is the provider?
- Have expected contract terms and conditions, including SLA, been defined for cloud vendors?
- Is there monitoring of cloud vendors to ensure they meet compliance requirements and controls?
- Is there a defined exit strategy?

- Is the cloud strategy operationalized across the organization through a governance model and exception management?
- Is my cloud application backed up appropriately?
- Is there DR in place?
- Do I have a process to monitor SLA compliance?

# A business challenge

*Cloud services adoption and operations is fundamentally changing all aspects of the digital business ecosystem; while stakeholders have distinct challenges – a common set of security capabilities are needed*




1. Securing move to cloud infrastructure: Azure & AWS
2. Securing move to cloud apps and services: O365, SFDC, Google, ServiceNow, Workday, etc.
3. Enable secure engineering and Security DevOps

1. Cloud security strategy & architecture for IaaS, SaaS, and PaaS
2. Implementing security solutions – for and as cloud
3. Security operations for and as cloud
4. Privacy, risk, and compliance

1. Privacy, risk, and compliance
2. Cloud vendor risk management
3. Auditing cloud use

KPMG

# Cloud Governance Maturity Model

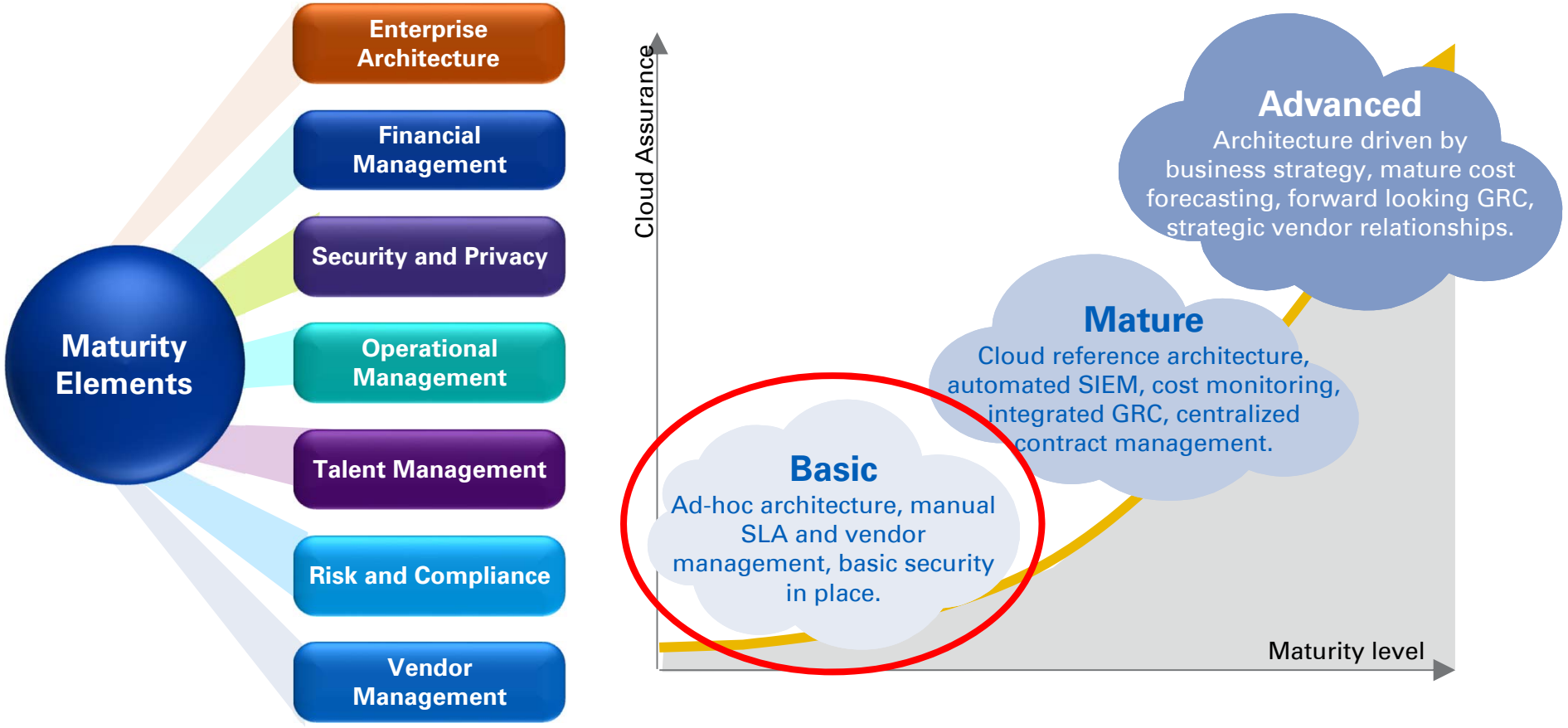
# Cloud Maturity Model

**Organizations need to take a comprehensive view of IT capabilities and understand the implications of cloud on the IT organization. While many traditional IT capabilities can be leveraged, many will need to be enhanced to work in a cloud environment:**


| | |
|---|---|
| Enterprise Architecture | • Cloud Architecture linked with Business and IT Strategy<br>• Risk-based reference architecture for cloud |
| Financial Management | • Mature cost forecasting and business case models<br>• Continuous monitoring and adjustment |
| Security and Privacy | • Fully integrated security model with cloud solutions |
| Operational Management | • Defined SLA by workload and automated management<br>• Reducing cost of operations as a percentage of total IT spend |
| Talent Management | • Cloud talent strategy tie-in with HR strategy and workforce planning |
| Risk and Compliance | • Cloud decision framework incorporates Risk and Compliance |
| Vendor Management | • Cloud decision framework<br>• Alignment of business, IT and procurement across the vendor lifecycle<br>• Contracts align to relevant risks |

# Cloud Maturity Model

Cloud governance requires all the elements to be built and in place – most organizations are still creating or tailoring these elements to a cloud first world:

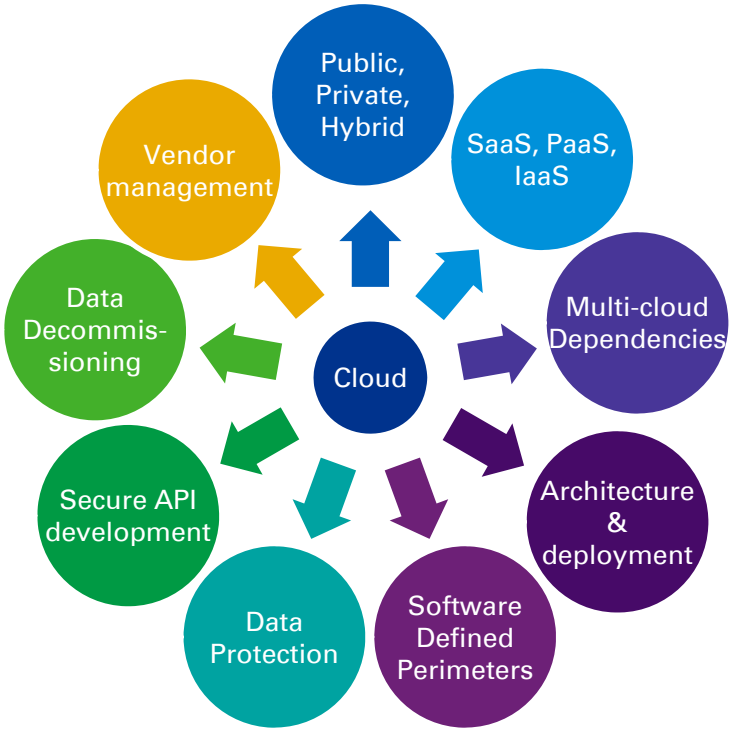


# Cloud security point of view

# Compounding security challenges as a result of cloud

*As cloud services are introduced to the environment, security risks are compounded as a larger and more complex security perimeter is exposed to increased threat vectors*

**New models, architectures, and relationships**




**New and existing threats**

| Threat actor | Threat objective |
|---|---|
| *Organized crime* | — Financial Gain<br>— Corporate espionage |
| *Competitor* | — Financial Gain<br>— Competitive Advantage |
| *Nation state* | — Economic Advantage<br>— Financial Gain<br>— Intelligence |
| *Hacker* | — Fame<br>— Notoriety<br>— Embarrassment<br>— Financial Gain |

*As organizations adopt cloud technologies and services, security leaders will need to revisit how they secure their environments to sustain their security posture and reduce exposure to new and existing threats.*

# Key Cloud security risks

*Most organizations already have robust IT Security capabilities and tools in place. However, the unique attributes of Cloud require a new framework and approach. We see six top cloud-related risks driving a majority of security discussions:*

**System and application vulnerabilities**

How do I address application vulnerabilities and risks when my applications live outside my organization and they broker other cloud services?

**Cloud to Cloud**

How do I securely build and operate when services are built on other cloud services? How do I manage my risks in an inter-dependent cloud world?

**Data security and compliance across Cloud**

How do I detect, respond, and protect what's already in the cloud across heterogeneous cloud environments?

**Shadow IT and Cloud governance**

We can't protect what we don't know. How do I detect and govern shadow IT's use of cloud without impeding innovation?

**Malicious insider threat**

All service models IaaS, PaaS and SaaS are vulnerable to attacks by malicious insiders. How do I monitor, protect and prevent unauthorized actions on my data?

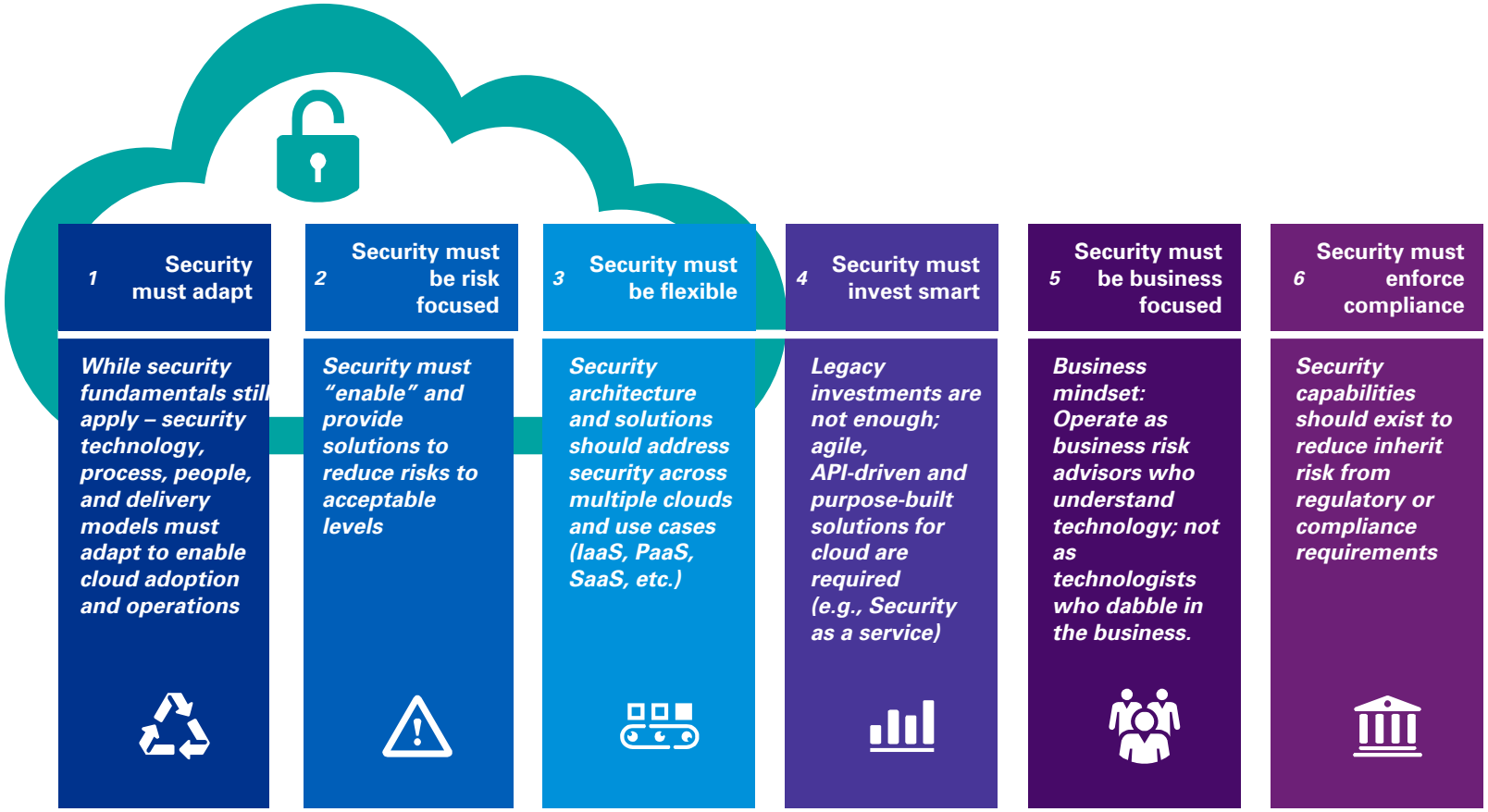
**Secure cloud development**

How do I bake security into my continuous development and release lifecycles? How do I securely develop across cloud APIs?

*The framework for addressing these issues must to be in place before Cloud planning and implementation can begin. As the organization continues to transform, the principles developed for the cloud must be integrated into the larger IT Security framework.*

# Guiding principles for cloud security

Although cloud technologies have provided organizations powerful tools along with the ability to decrease IT costs, it has increased the potential risks and threats to the organizations. Ensure your organizations security by assessing its security posture.



# Leading practices to implementing a secure cloud

**API-based security:** Traditional security solutions (e.g., heavy, on premise, UI-based) solutions impede adoption and often times are unable to natively integrate with cloud services. Organizations need integrated, native-cloud API-based security solutions (e.g., identity, data protection, logging, configuration checks, etc.) to unlock the innovation and flexibility cloud offers.

**Incident response:** Organizations should develop detailed response plans to mitigate different types of security threats that could affect them. Policies should be established and resources should be allocated for the response team and periodic drills should be implemented to ascertain any gaps in the policies

**Federated identity and access management:** Organizations should extend their existing Identity Management model to the cloud service; mapping roles, entitlements, and user-base and ensure existing policies can be enforced and procedures can be followed. An isolated domain leads to limited context and a higher potential for access control errors.

**Data-centric security:** For SaaS and PaaS models, securing the perimeter is the responsibility of the provider; thus for consumers to have confidence they must protect the data directly. Organizations are adopting native-cloud encryption and digital rights management solutions to provide reliable, data-centric protections in the cloud.

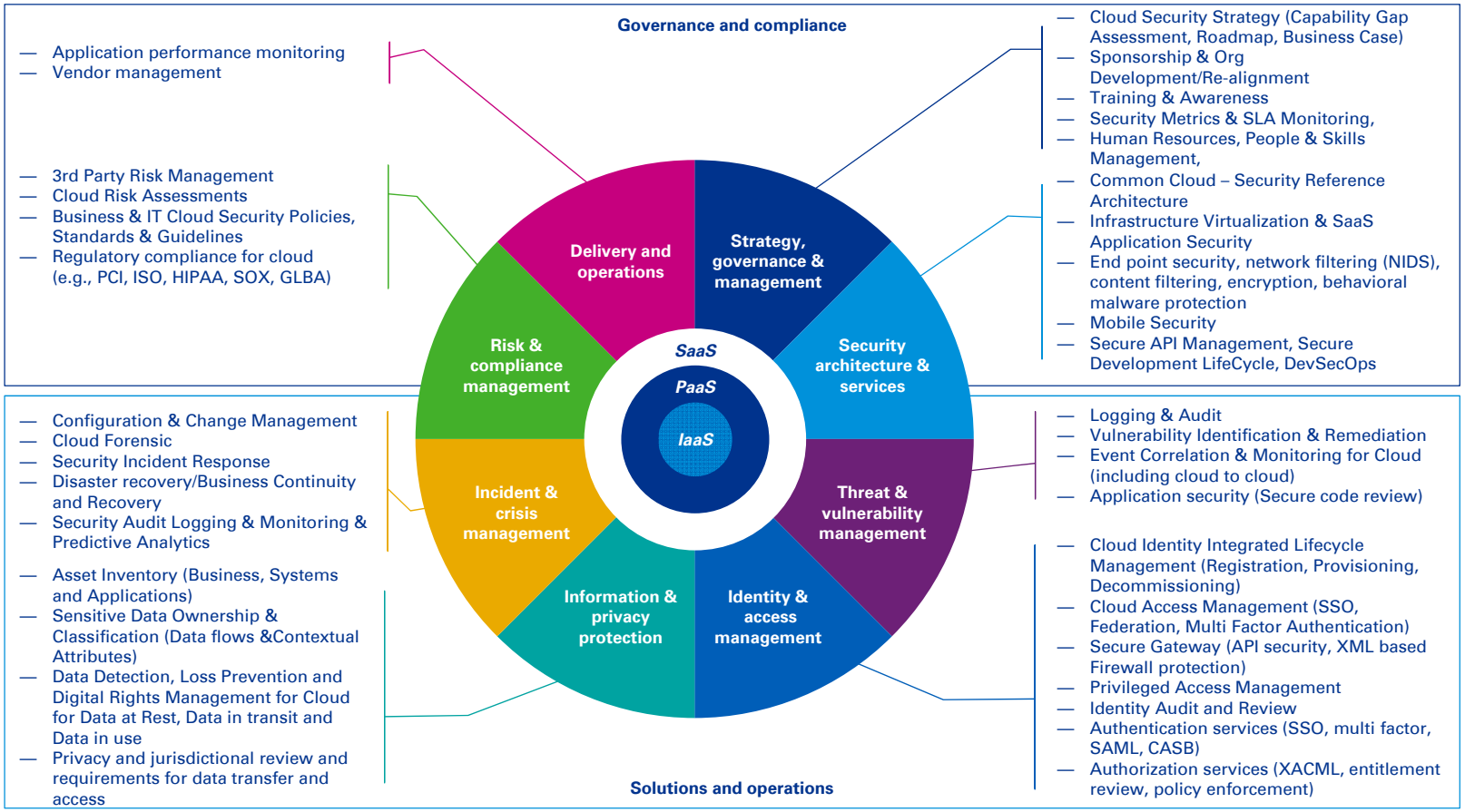
**Secured perimeter that spans the entire stack:** The software-defined nature of cloud-based networks means perimeter security is critical and challenging. Perimeter security will need to be re-evaluated based on the new cloud services being introduced into the environment. The network architecture must allow for complex segmentation and filtering without increasing time to configuration.

**Integrated security monitoring and operations:** Secure Cloud adoption can underscore the challenges of obtaining actionable intelligence. Organizations should implement smart logging, threat intelligence, and monitoring tuned to business, architecture, and data-specific contexts and that integrates with native cloud platforms.

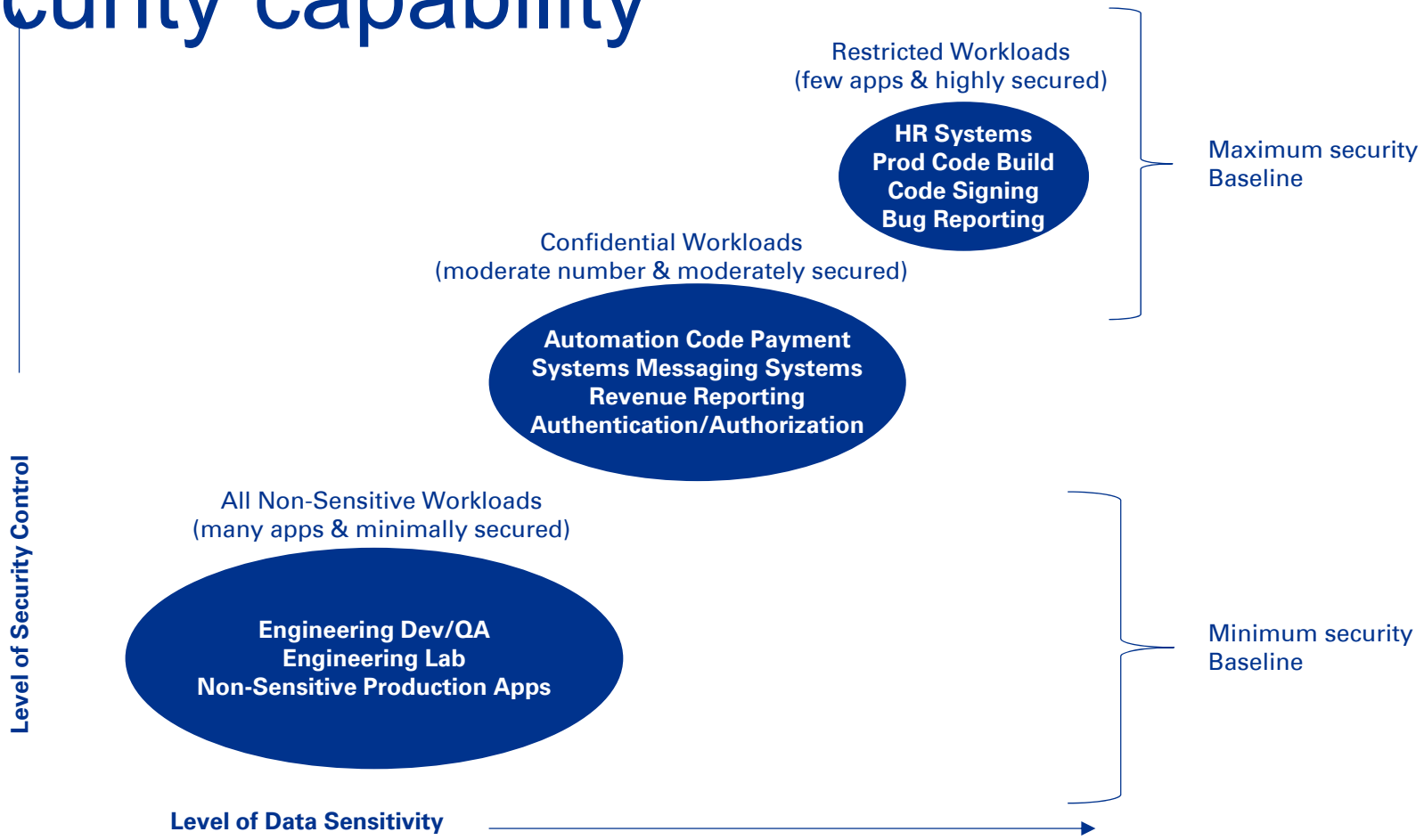
# Taking a multi-dimensional approach to securing the Cloud

*We combine our experience with leading control and regulatory frameworks, our cloud implementation and operations experience, with our deep cybersecurity and risk management insight to help organizations securely adopt and operate in the cloud.*

**CSA Capability wheel**



# Not all workloads require same security capability



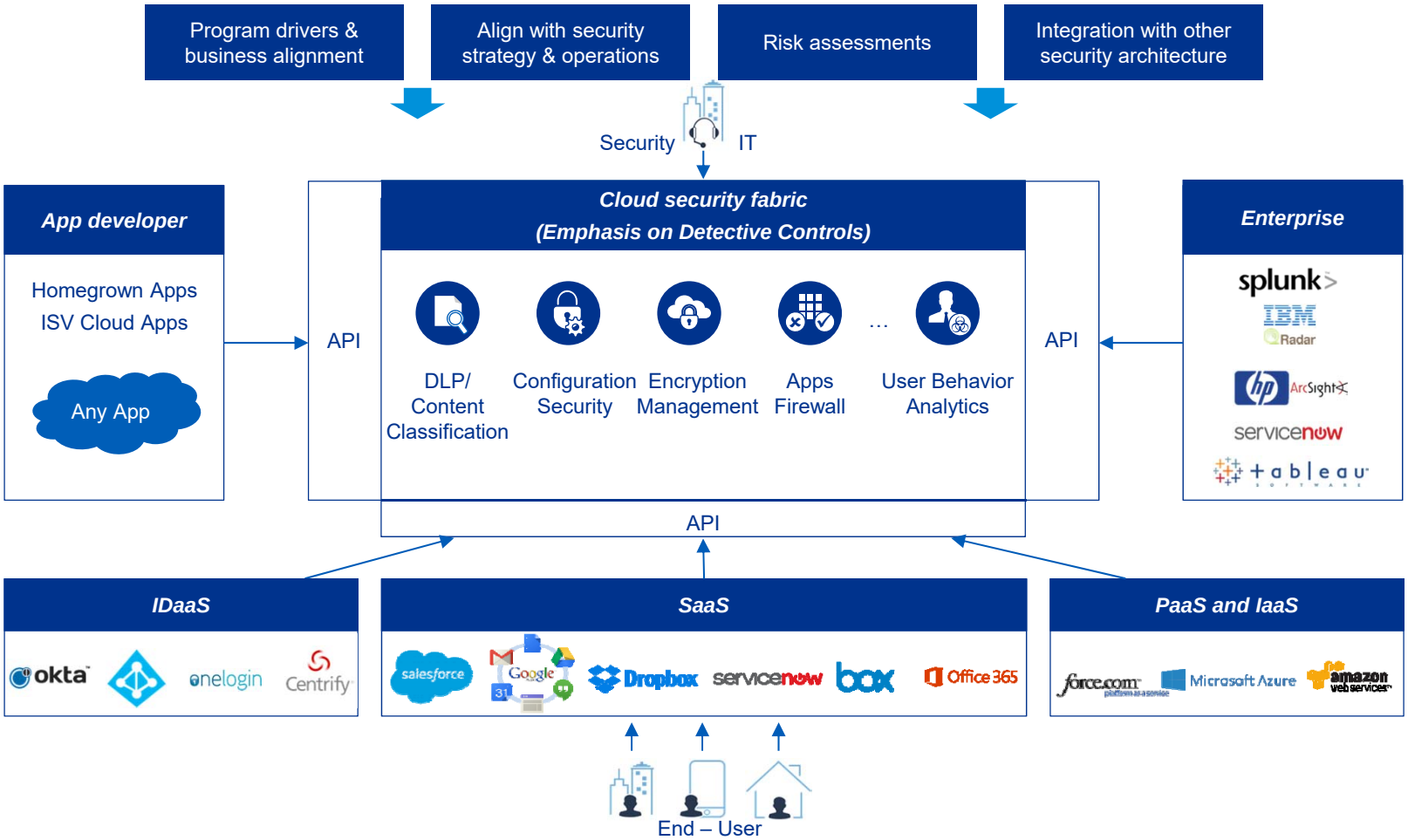
# 5 Steps toward a posture to enable and protect cloud adoption

1. Develop a cloud security reference architecture and strategy to enable and protect the business across your SaaS, IaaS, and PaaS journey and migrations
2. Discover and protect sensitive and high value cloud data and files already in the cloud using purpose built tools and integration with existing security and operational processes
3. Develop cloud governance and monitoring policy, process, and technology to detect, help prevent, and respond to cloud service misuse
4. Understand your adversaries – including their motives, resources, and methods of attack to help reduce the time from detect to respond
5. Assess cybersecurity of third parties and supply chain partners, and ensure they adhere to your security policies and practices and address common cloud gaps

KPMG

# Cloud Governance and Reference Architecture

# Cloud platform security overview



# Cloud architecture & control alignment

| Cloud arch layer | Definition | CSA domains |
|---|---|---|
| **Customer access** | Hosts, end users and all the end points accessing the cloud services | Encryption & Key Mgmt. · Application & Interface security · Identity & Access Management |
| **Apps & data** | Customer application security and data layer | Data security & Info Lifecycle Mgmt. · Application & Interface security · Encryption & Key Mgmt. · Identity & Access Management |
| **Cloud orchestration** | Abstraction layer referring to cloud orchestration services to manage a single cloud or multiple clouds | Identity & Access Management · Change control & config |
| **Cloud provider management (Native provider)** | Abstraction layer representing the native cloud provider services | Interoperability & Portability · Infra & Virtualization security · Encryption & Key Mgmt. · Identity & Access Management |
| **Virtualized resources** | Security services provided for Compute, Network, Storage and OS images at virtualization level | Infra & Virtualization security · Identity & Access Management · Encryption & Key Mgmt. · Business continuity mgmt. and operational resilience · Threat & Vulnerability Mgmt. · Change control & config |
| **Provider physical resources** | Hardware, data centers – Network, storage and images | N/A |

Governance & Risk Mgmt. (Applicable across all layers)

Audit, Assurance & Compliance(Applicable across all layers)

SIEM, E-discovery & Forensics(Applicable across all layers)

# Level 1 – Legend

| Cloud layers | Applicable security controls | Description |
|---|---|---|
| **Customer access** | Encryption & key mgmt. | — End point encryption<br>— Device encryption |
| | Application & interface security | — Cloud API security – API access<br>— Customer access models |
| | Identity & access mgmt. | — End-point access control processes |
| **Apps & data sec** | Datasec & info Lifecycle mgmt. | — Data security – Data and asset classification<br>— Data protection<br>— DLP<br>— Information lifecycle management |
| | Encryption & key mgmt. | — Data encryption (at rest and transit) and tokenization,<br>— Key generation<br>— Key storage<br>— Key entitlement and lifecycle management |
| | Application & interface security | — API security<br>— SDLC<br>— Application security |
| | Identity & access mgmt. | — Identity and access management of customer data and applications |
| **Cloud orchestration** | Identity & access mgmt. | — Access control<br>— Audit logging and RBAC policies for admin users who are logging into console and managing cloud services |
| | Change control & config | — Change control and configuration tracking of any console/API activities |
| **Cloud provider management** | Identity & access mgmt. | — User management and access management (authentication, 2FA, privileged access, authorization policies to restrict access, RBAC) for admin users accessing console or API's |
| | Interoperability & portability | — Platform and VM portability,<br>— Information portability |

# Level 1 – Legend (continued)

| Cloud layers | Applicable security controls | Description |
|---|---|---|
| **Cloud provider management (continued)** | Infra & virtualization security | — Audit logging,<br>— Change detection,<br>— Capacity/resource planning,<br>— Infrastructure automation security |
| **Virtualized resources** | Encryption & key mgmt. | — Encryption of virtualized resources<br>— HSM |
| | Infra & virtualization Security | — OS hardening<br>— VM security<br>— Virtual networks<br>— Segmentation<br>— Storage<br>— Network security |
| | Threat & vulnerability mgmt. | — Antivirus/Malware software<br>— Patch management |
| | Business continuity mgmt. & operational resilience. | — Data backups<br>— Archiving and retention<br>— Redundancy and recovery |
| | Change control & config | — Detect unauthorized installations<br>— Production changes (tracking changes)<br>— Configuration changes |
| | Identity & access mgmt. | — Restricted/authorized access to storage<br>— Network<br>— VM and other virtualized resources<br>— Periodic review of access |
| **Provider physical resources** | N/A | N/A |

# Level 1 – Legend – Common controls across all Cloud layers

| Security controls | Description |
|---|---|
| **Governance & risk mgmt.** | — Develop, document, maintain, execute, audit and review information security management program<br>— Information security policy framework<br>— Risk management program<br>— Risk framework and related cloud security governance documents and frameworks |
| **Audit, assurance & compliance** | — Meet industry and regulatory compliance requirements<br>— Conduct third party audits |
| **Security incident management, e-discovery & cloud forensics** | — Develop, document, maintain, execute, audit and review the incident response plan<br>— Incident management framework<br>— Forensic procedures |

# Cloud control maturity approach

*This Cloud Security Assessment incorporates information from the Cloud Security Alliance, and industry leading experience. Each control is mapped across technical characteristics and relevant regulatory guidance, and assessed based on our industry leading framework.*

All controls are mapped to the Cloud Security Framework

Relevant control questions describe each security control

| KPMG Cloud security framework domain | KPMG Cloud security control ID | Cloud security control | Control questions |
|---|---|---|---|
| Information and Privacy Protection | IPP-03 | Sensitive Data Protection/Encryption | Does policy, procedure, technology exist to ensure sensitive data is encrypted at rest and in transit as per regulatory, legal, and corporate policy? |

| IaaS | PaaS | SaaS | CSA Cloud controls matrix area | OCC bulletin | Cobit 5.0 | AICPA 2014 TSC | FFIEC handbook | FedRAMP security controls | … | PCI DSS v3.0 |
|---|---|---|---|---|---|---|---|---|---|---|
| X | X | X | Encryption & Key Management | OCC-064 | APO09.01/2/3<br>APO13.01<br>DSS05.02<br>DSS06.06<br>MEA03.01/2 | CC5.6 | FFIEC-005,<br>FFIEC-003 | NIST SP 800-53 R3 AC-1<br>NIST SP 800-53 R3 SC-1<br>NIST SP 800-53 R3 SC-13 | … | 6, 6.5 |

Relevance of each control mapped to deployment method

Cloud security control is mapped to the relevant CSA area

Each security control is mapped to leading practices for future remediation steps

Controls are mapped across 30+ regulatory frameworks

| 1) Policy/ governance readiness (None, partial, full) | 2) Process readiness (None, partial, full) | 3) Technology readiness (None, partial, full) | Current state observations<br>1 – Governance readiness comments<br>2 – Process readiness comments<br>3 – Technology readiness comments | Leading practices for Cloud adoption | Leading Cloud tools |
|---|---|---|---|---|---|
| Full | Partial | None | 1. Policy exists that states sensitive data should be encrypted "Information security classification, handling and labelling"<br>2. No data encryption standard processes observed; encryption is not enforced. DLP for email encryption exists; no processes observed for cloud environments. NERC/FERC/SOX requirements adhered to but other data encryption is not followed<br>3. No tech enforces encryption policy. In place with email, RSA DLP licenses exist outside of it; considering web sense proxy DLP | 1. Specify the levels of encryption that should be used at all phases of the information lifecycle. For example, require all transmissions to use SSL, all back-ups to be encrypted, and specific user attributes (such as email addresses) to be encrypted at all times.<br>2. Specify controls on the handling, storage and archiving of keys used in the encryption process.<br>3. (IaaS only) Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.<br>4. Employees handling data in this cloud service that require encryption on a regular basis should be trained in encryption best practices<br>5. Comply with industry standards (AES 256-bit encryption) | — TrendMicro SecureCloud<br><br>**Emerging Cloud tools**<br>— CipherCloud<br>— HyTrust Cloud Control<br>— SafeNet ProtectV<br>— Vormetric Transparent Encryption |

Controls are evaluated across Policy, Process and Technology Readiness

Observations and assessments are captured in detail across assessment areas

Leading and emerging tools that support achieving the tool are provided for each control.

FOR INTERNAL USE ONLY

KPMG

# Questions

# Thank you

KPMG's Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

## Contact us

**Darren Jones**

Director, Cyber Security Services
T: 416 777-3737
M: 647 580-7399
E: darrenjones@kpmg.ca