



Cloud Cyber Risk Management

Managing cyber risks on the journey to
Amazon Web Services (AWS) solutions



Cloud and security are not an “either-or” proposition.

Together, Deloitte and AWS can offer AWS customers services that help them reap the benefits of cloud services *and* **improve their cyber risk posture.**

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

Contacts to support your AWS cyber risk needs



Aaron Brown

Partner | Deloitte Advisory
Cyber Risk Services
Deloitte & Touche LLP
aaronbrown@deloitte.com



Mark Campbell

Sr. Manager | Deloitte Advisory
Cyber Risk Services
Deloitte & Touche LLP
markcampbell@deloitte.com

Not all security and compliance controls are inherited or “automatic”

Security **of** the AWS cloud is Amazon’s responsibility
Security **in** the AWS cloud is the enterprise’s responsibility

	Private Cloud (Self-Hosted)	Private Cloud (Co-Located)	IaaS	PaaS	SaaS
Security Governance, Risk & Compliance (GRC)					
Data Security					
Application Security					
Platform Security					
Infrastructure Security					
Physical Security					

Enterprise Responsibility

Shared Responsibility

Cloud Provider Responsibility

Managing cyber risk
is a shared
responsibility

Representative Cloud Security Responsibility Matrix

A cloud strategy must address cyber risks associated with the customer control responsibilities

Strategic business initiative for new services and applications

Adopt the AWS cloud as the core platform for business services and applications

As enterprises build new IT services and data in the AWS cloud, customer controls are needed for achieving a compliant & secure integrated cloud platform

New business services initiative

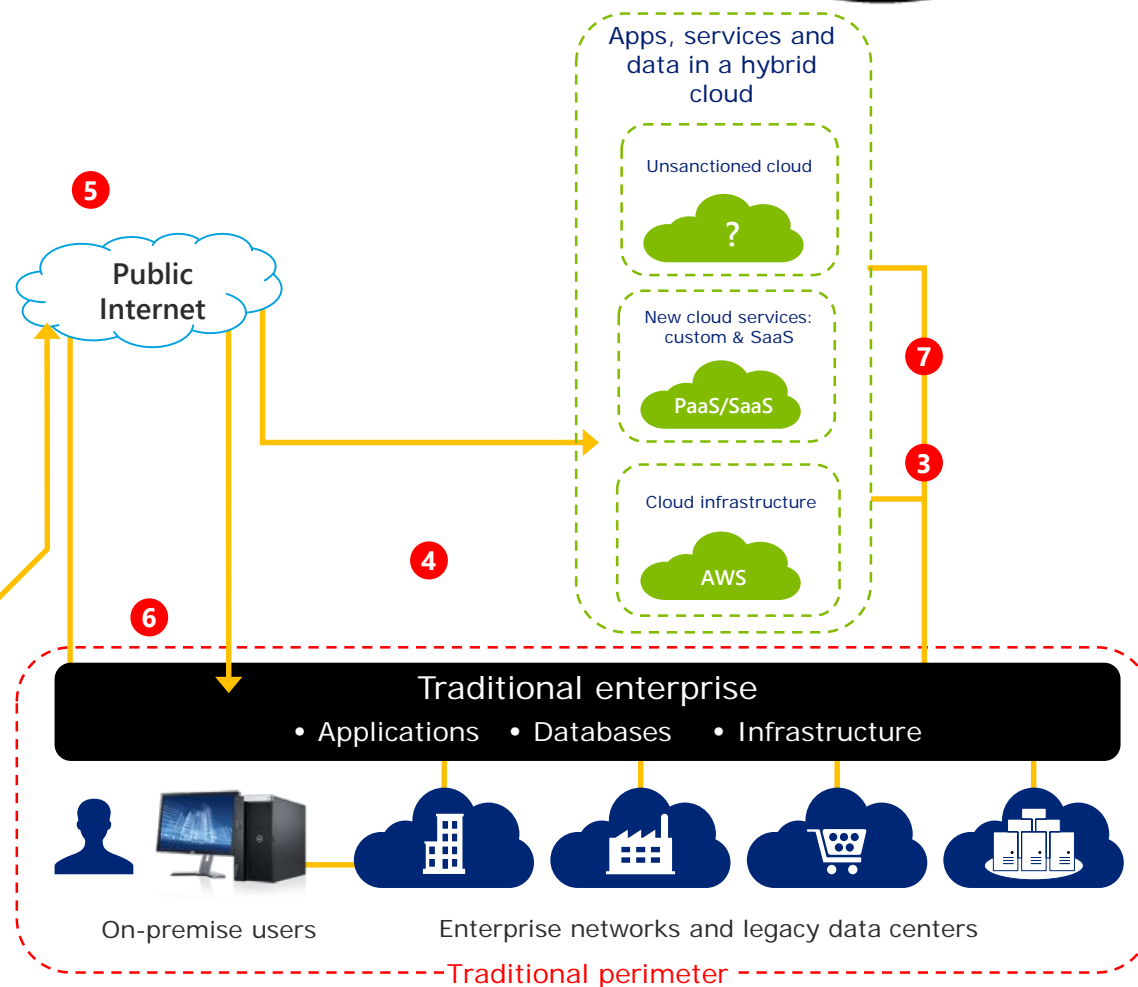
Adopt AWS cloud as core platform



Customer controls for the cloud

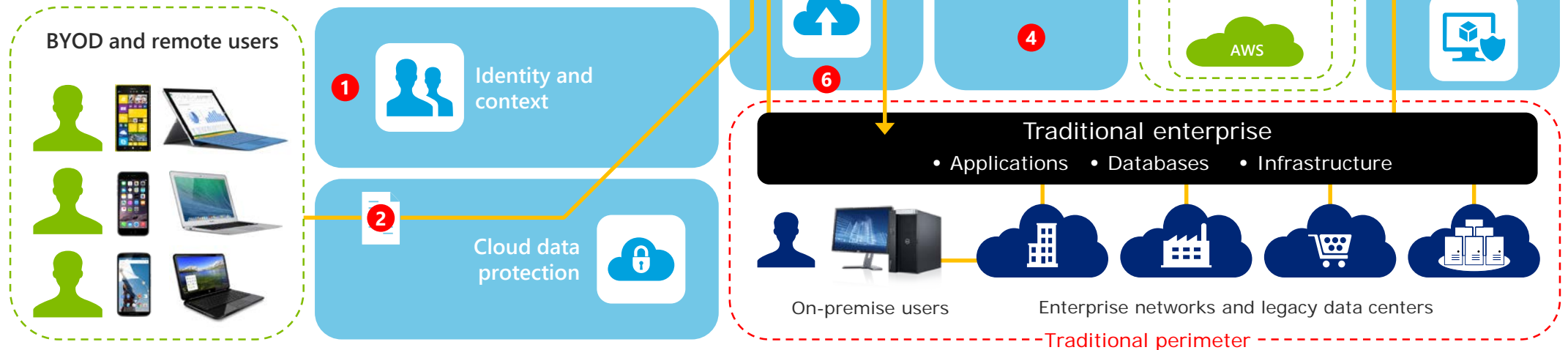
Cloud integration presents common challenges that need security re-architecture

- 1 Unmanaged users, bring your own devices (BYOD) and systems
- 2 Data outside of the perimeter
- 3 Hybrid cloud architecture is a new attack surface
- 4 Direct access to cloud applications from public networks
- 5 Lack of activity visibility outside the traditional perimeter
- 6 Events outside of the enterprise impact operations
- 7 Reliance on ungoverned providers



Deloitte provides security capabilities needed for managing cyber risks associated with customer controls

- 1 Identity, access, and contextual awareness
- 2 Data protection and privacy
- 3 Virtual infrastructure and platform security
- 4 Secure all cloud applications
- 5 Vigilance and monitoring of risks of cloud traffic and integrations with other cloud services
- 6 Resilience and incident response across the cloud
- 7 Govern risk and compliance



Extend existing security products or augment with new ones?

A critical consideration across all domains is rationalizing whether to leverage existing security products vs. augmenting with new security products for cloud:

- Fit of security product features to security requirements
- Compatibility of security product with hybrid cloud components
- Product costs
- Maturity and scaling of products
- Deployment option analysis (e.g., Amazon Machine Image vs. Application Program Interface vs. proxy)
- Delegation of operational responsibilities for enterprise vs. cloud
- Operational costs (Operate vs. Managed Service)

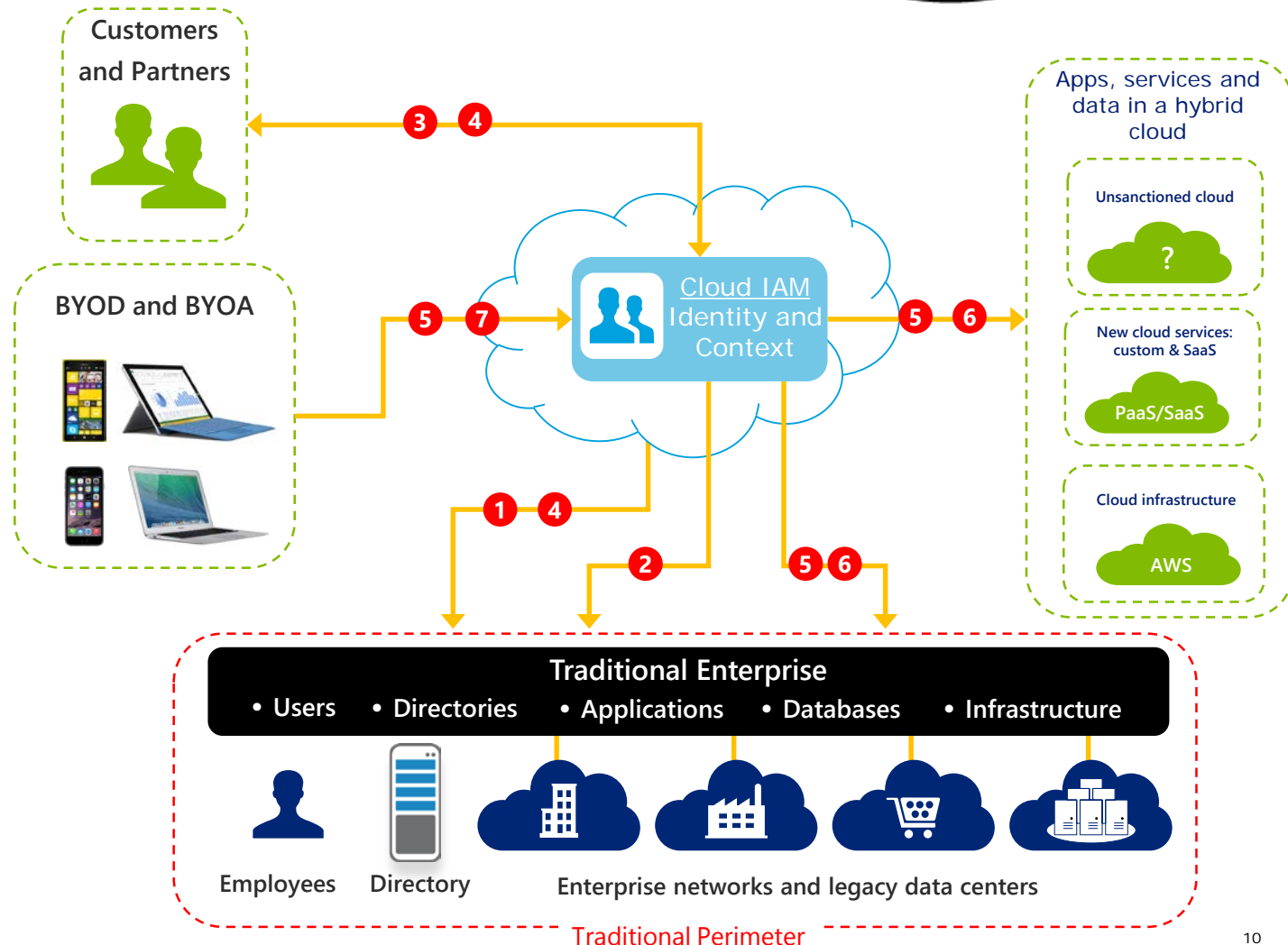


What are specific considerations for each cloud security capability?

1. Identity and Access Management (IAM) – Hybrid cloud and the extended enterprise drive complex identity requirements

Key considerations:

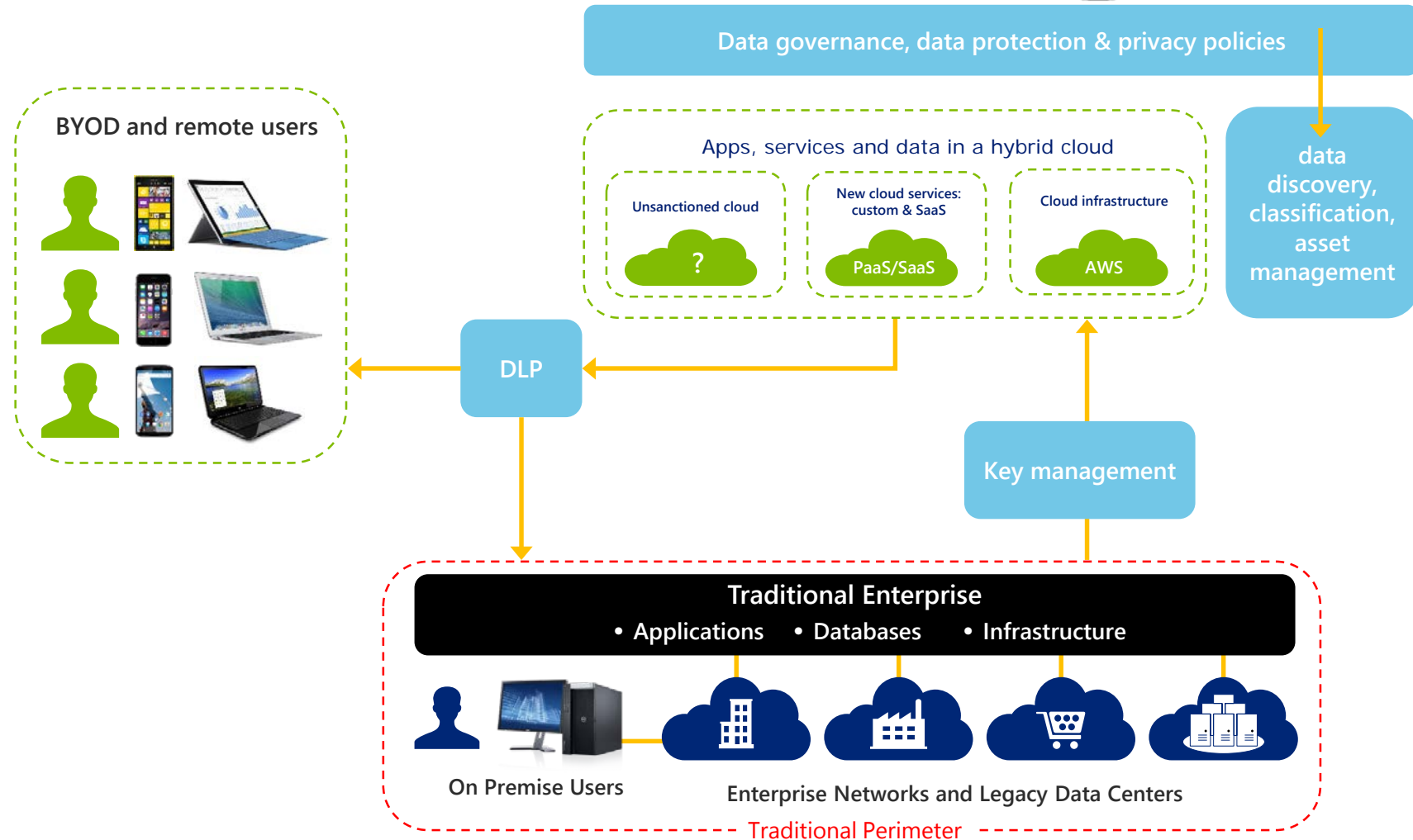
- 1 Employee identity context
- 2 Integration with enterprise directories
- 3 Customer and partner identity context
- 4 Enterprise SSO + strong authentication MFA
- 5 User provisioning, AWS IAM roles, role-based access controls (RBAC)
- 6 Privileged account management
- 7 Mobile device app & data management



2. Data protection – It's ALL about the data

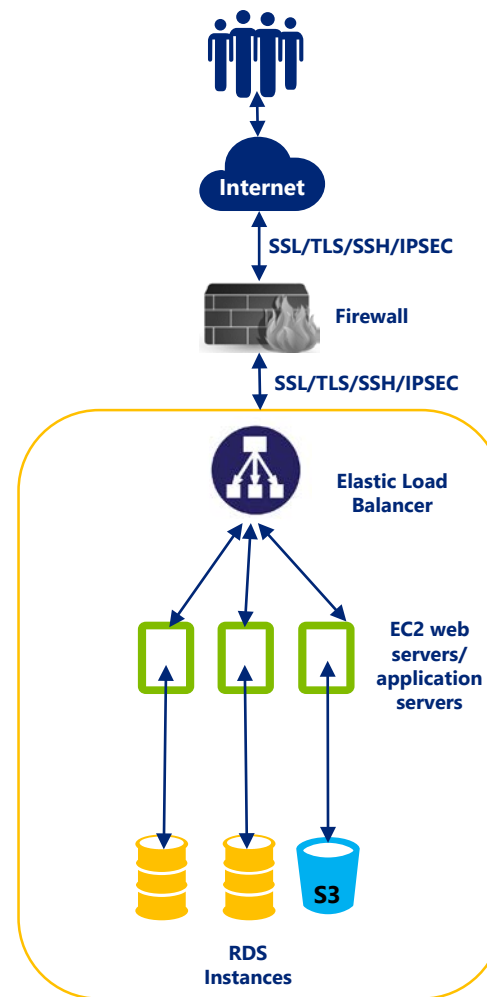
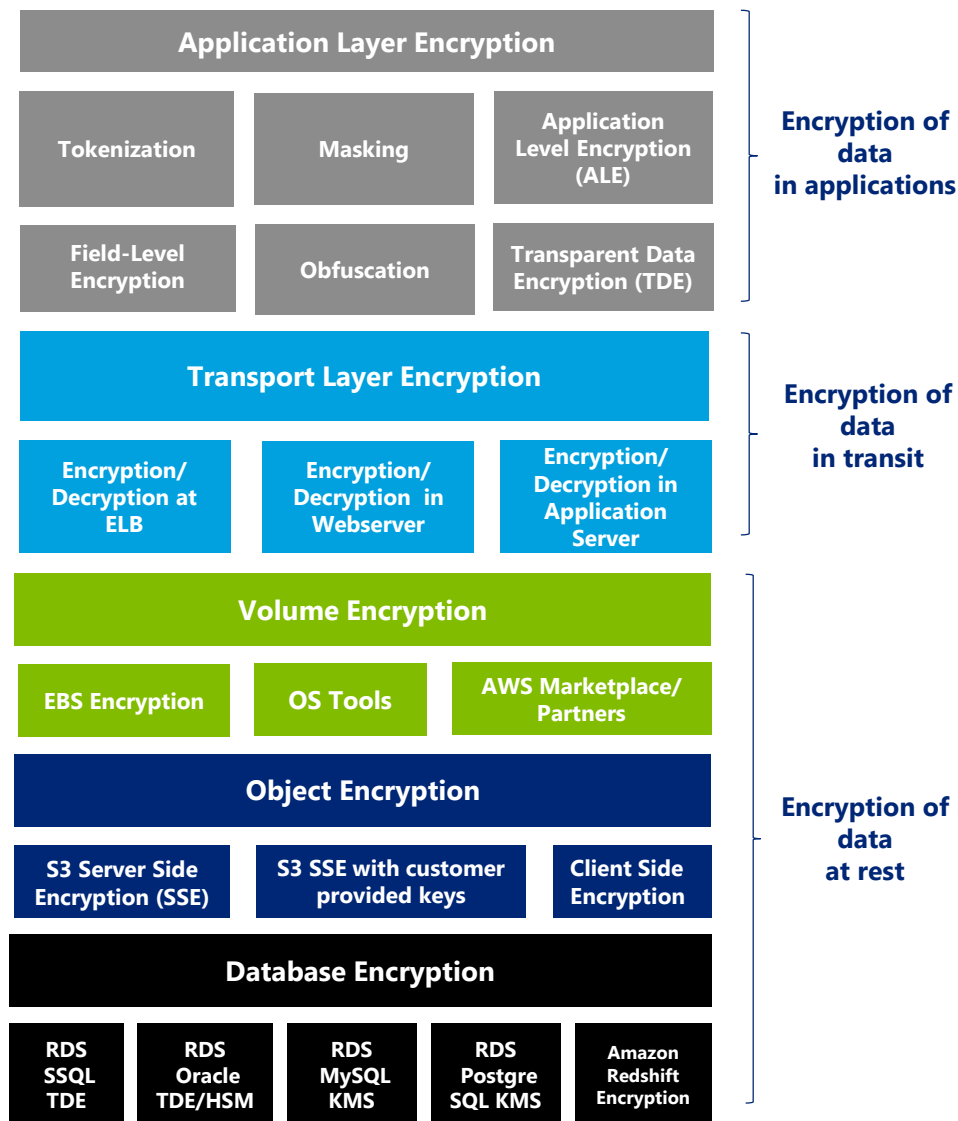
Key considerations:

- Identify data assets in the cloud
- Revisit data classification and implement tagging
- On-premise or in the cloud security tools:
 - Data Loss Prevention (DLP)
 - Key Management Service (KMS)
 - Hardware Security Module (HSM)
- What remains on-premise vs. in the cloud (keys, encryption, etc.)
- Data residency issues
- Encryption, tokenization, masking



Encryption, tokenization, and masking

- What data needs to be encrypted based on classification?
- Secure structured and unstructured data throughout all logical layers within your AWS environment using encryption technologies
- Proper use of encryption minimizes the attack surface and mitigates cyber risks related to exposure or exfiltration of data
- Encrypt data in running applications, at rest, and in transit (including audit logs)



3. Network and Infrastructure Security in the Cloud

Key considerations:

Virtual Private Cloud (VPC) and access defense:

- Secure access for enterprise users, customers, and partners
- Securing ingress/egress between AWS, traditional enterprise and other cloud providers

Internal network protection and visibility:

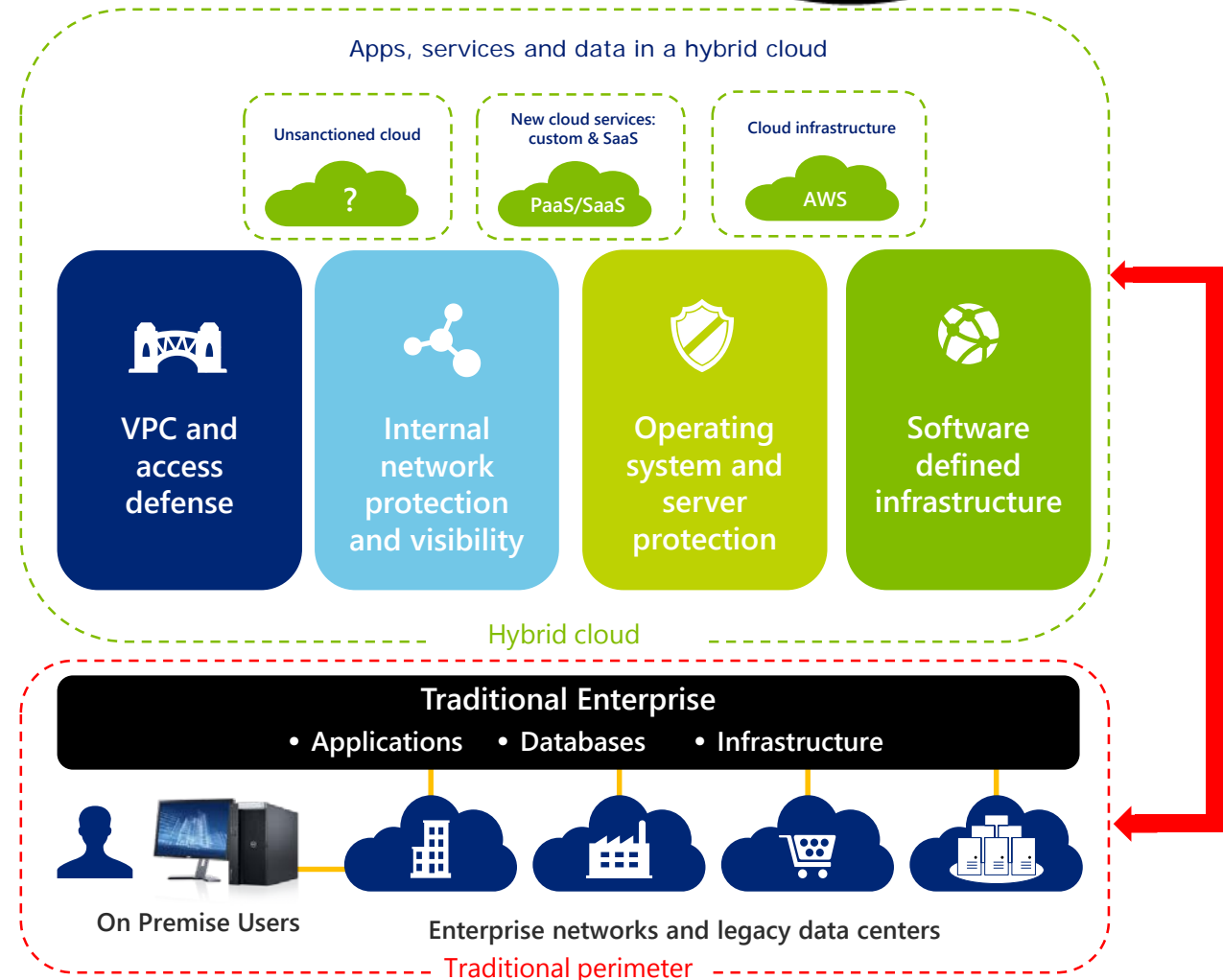
- Segmentation, Micro-segmentation (Subnets, Security Groups, NACLs, etc.)
- Visibility on transmission down to the guest to guest level:
 - AWS Web Application Firewall (WAF)
 - Intrusion Detection and Prevention

Operating system and server protection:

- Operating system integrity, performance, and endpoint protection
- Host configuration and management
- Vulnerability scanning

Software defined infrastructure:

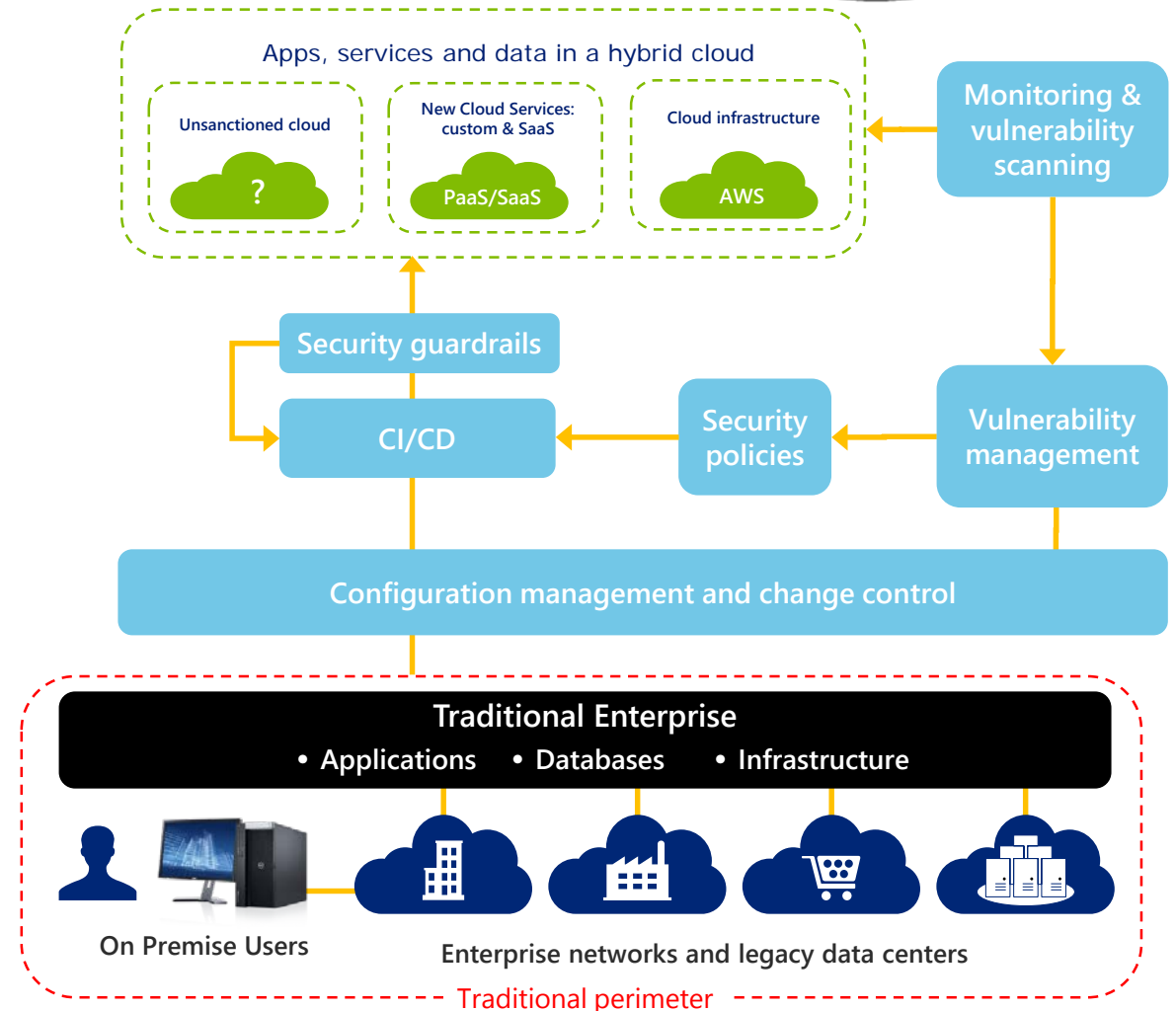
- Compliance scanning before deployment
- Integrity and version management
- Backup and access controls for continuous integration and deployment (CI/CD) automation components



4. DevSecOps expands the responsibilities for application security

Key considerations:

- Adapt DevSecOps with guardrails and compliance validations leveraging AWS Inspector, AWS Config
- Application architecture assessments
- Secure coding, standard application logging, error handling
- Integrate security controls into continuous integration and deployment (CI/CD), AWS Code Deploy and Code Commit
- Protect source code and configurations
- Code scanning (SAST) including automation scripts
- Application testing (DAST)
- Vulnerability management



5. Vigilance – new visibility and detection requirements outside the traditional perimeter

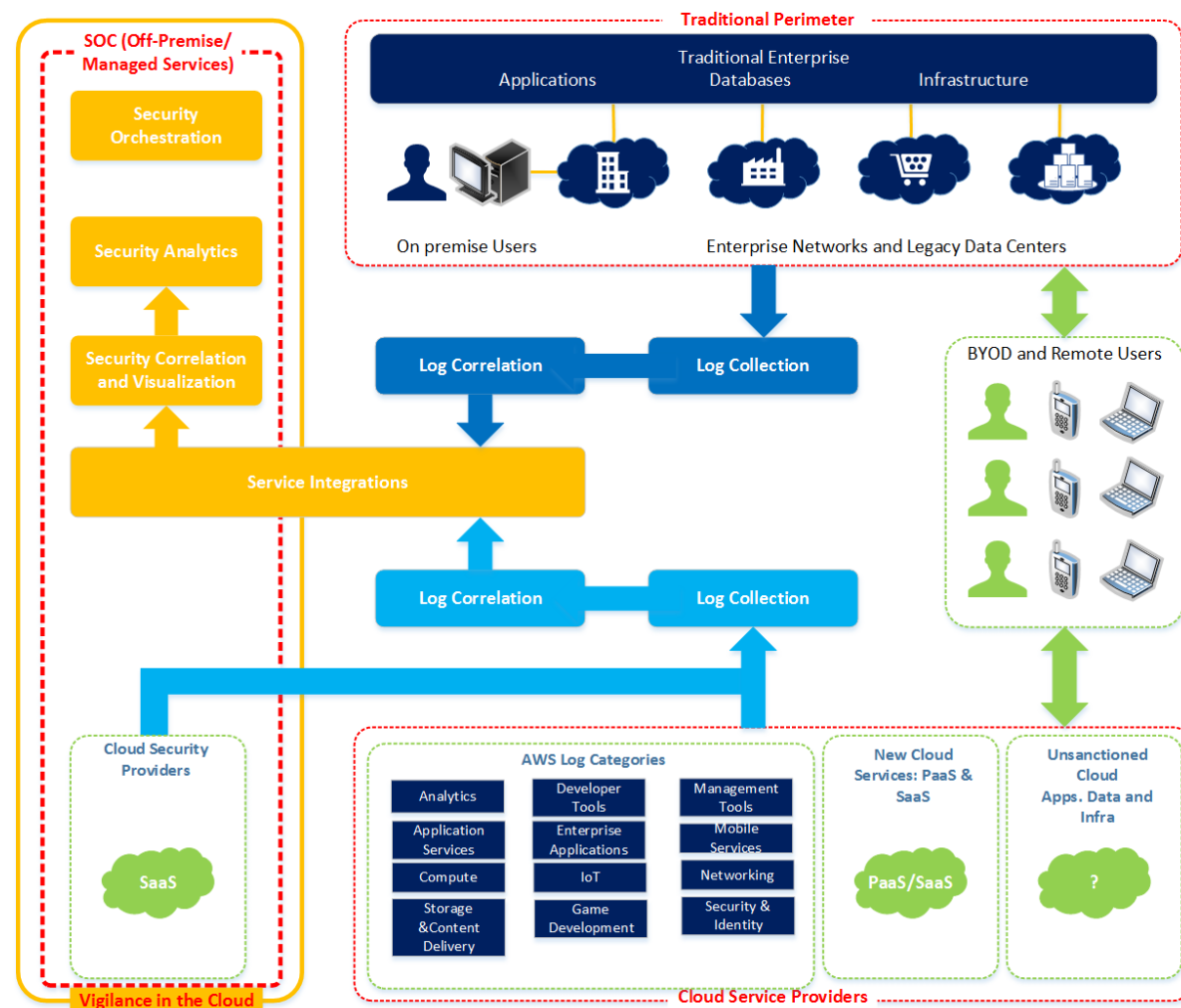
Key considerations:

Security monitoring capabilities:

- Achieving comprehensive visibility of cloud assets down to the guest-level
- Keeping up with elastic environments with proprietary IaaS and PaaS technology
- Use on-premise Security Information and Event Monitoring (SIEM) or build new one in the cloud?
- Do I have defined use cases?
- Where do my capabilities reside?
- How mature are my operations?

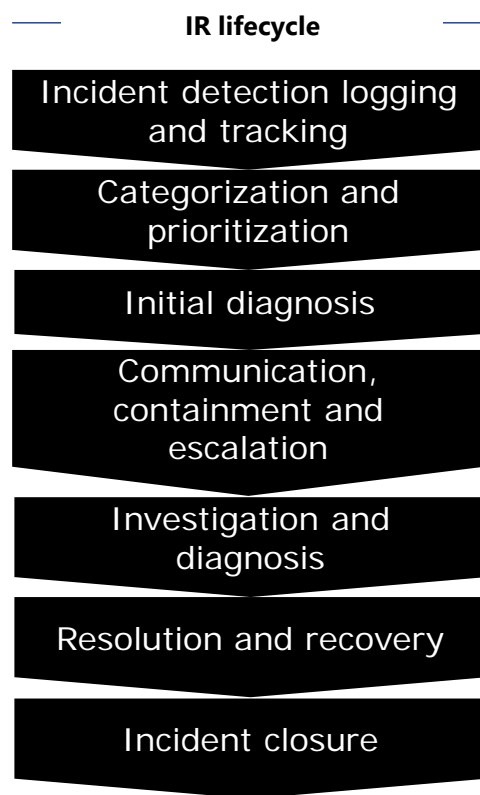
Continuous improvements:

- Do I have documented procedures?
- Do I have a continuous improvement program (DevSecOps)?



6. Resilience at the next level – take advantage of technology with process and organization

Extend existing incident response programs to AWS. Identify the most relevant incident classes and prepare strategies for the incident containment, eradication and recovery assistance.



Key focus areas

Incident detection logging and tracking

- Perform the analysis for understanding what incident types are possible for AWS cloud integration.

Categorization and prioritization

- Understand and agree on the definition of events of interest vs. security incidents by AWS and what events/incidents the cloud-service provider reports to the organization and in which way.

Initial diagnosis

- The organization must understand the AWS support model incident analysis, particularly the nature (content and format) of data that AWS will supply for analysis purposes and the level of interaction with the AWS incident response team.
 - In particular, it must be evaluated whether the available data for incident analysis satisfies legal requirements on forensic investigations that may be relevant to your organization.
- Understand what AWS has by way of a knowledge base that the IR team can tap into for understanding capabilities with AWS tools. This may can be in the form of an FAQ.

Communication, containment, and escalation

- Understand what is necessary to implement containment related to the cloud integration. The organization must carefully analyze the potential containment cases, and negotiate mutually agreeable processes for containment decision and execution.
- Determine and establish proper communication paths (escalation, hand-off, etc.) with AWS that can be consistently followed in the event of an incident.

Investigate and diagnosis

- The organization must evaluate the AWS support model in forensic analysis and incident recovery such as access/roll-back to snapshots of virtual environments, virtual-machine introspection, etc.

Resolution and recovery

- Post Recovery "Lessons Learned" activities involves sharing detailed incident reports with AWS and related organizations, in addition to your internal IR team.

Evaluate resilience preparedness with AWS through cyber wargames

Cyber wargames involve an interactive technique that immerses potential cyber-incident responders in a simulated cyber scenario to help organizations evaluate their cyber incident response preparedness leading to deeper, broader lessons learned

Cyber wargames can drive improvements in cyber resiliency, including:



Stronger response capabilities aligned toward mitigating the highest impact risks of a cyber incident



Broader consensus on the appropriate strategies and activities to execute cyber incident response



Improved understanding of the people, processes, data, and tools needed to respond to a cyber incident



Better identification of gaps in cyber incident response people, processes, and tools



Enhanced awareness of the downstream impacts of cyber incident response decisions and actions



Tighter integration between parties likely to be collectively involved in the response to a cyber incident

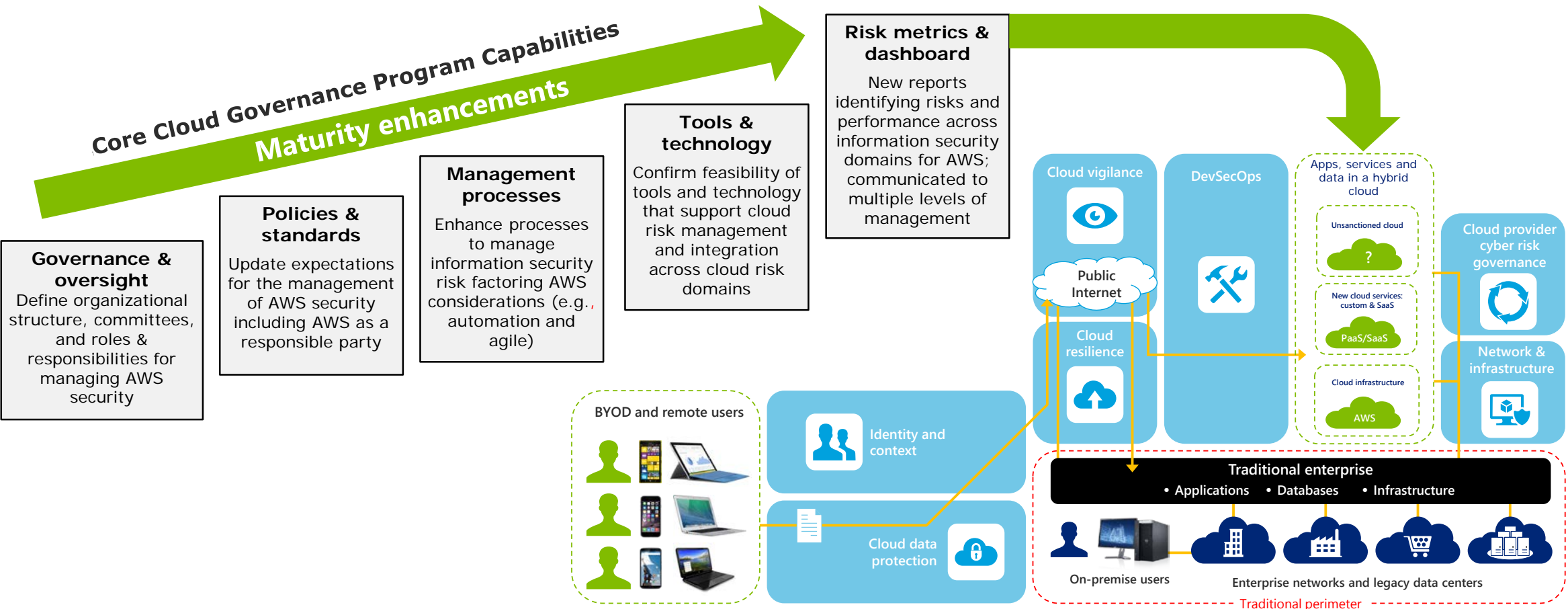


Improved clarity regarding ownership of authority related to certain key cyber incident response decisions



Reduced time-to-response through the development of cyber incident response "muscle memory"

7. Cloud governance – bring the pieces together and measure success



Building a sustainable cloud cyber risk governance program



Strategy

Understanding the business strategy and growth objectives to align cloud adoption capabilities and priorities



Foundation & discovery

Building a holistic cloud governance and risk management framework for consistency and efficiency

Leveraging business view (top-down) and technology aided (bottom-up) discovery techniques to profile cloud use, including shadow IT, and risk landscape



Readiness

Assessing cloud risks, capabilities and controls across the enterprise and determining a cloud governance program strategy and roadmap for ongoing program operations, risk assessment, remediation and certification



Onboarding

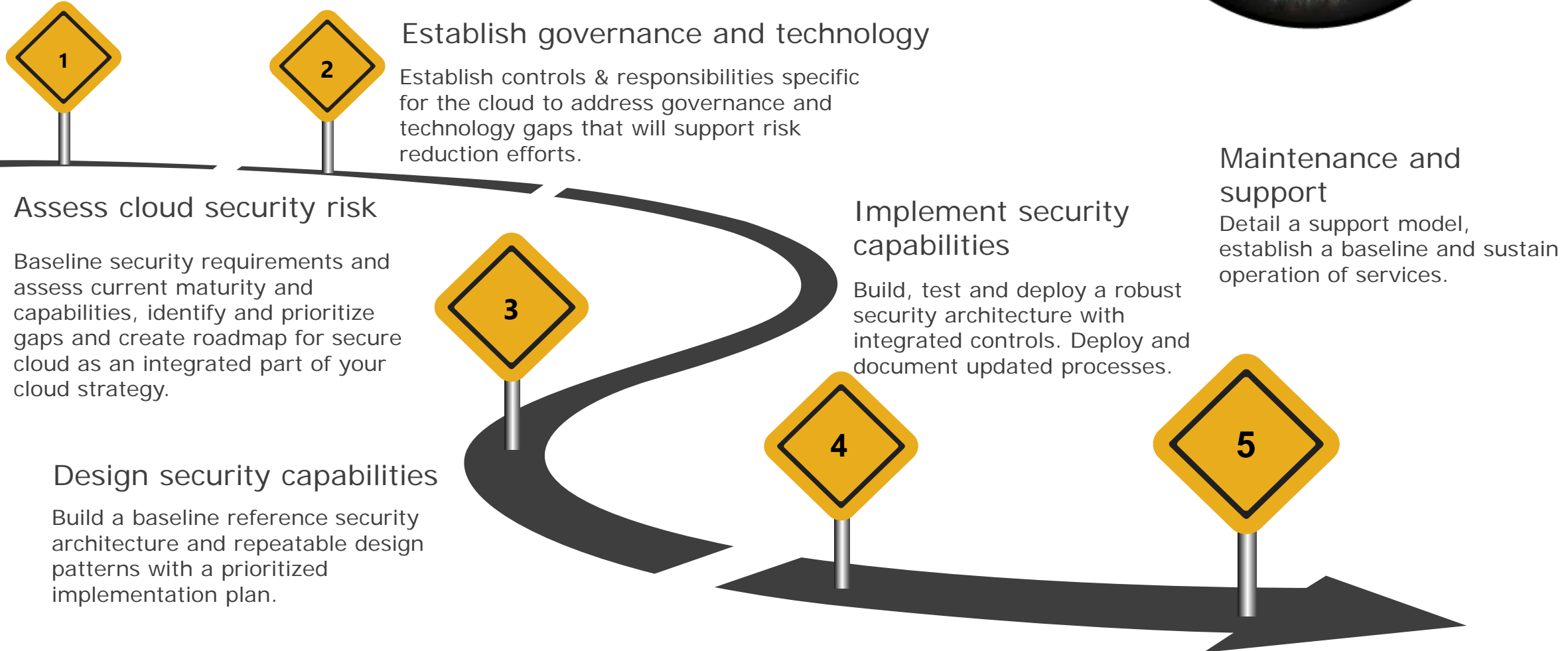
Operationalization of the cloud governance framework across the enterprise through onboarding of business units, products and functions



Improvement

Continuous management and improvement of the cloud governance program through assessment, monitoring, tool deployment, extension of program, etc.

The path for enhancing cyber risk management for customer cloud control responsibilities



Considerations when enhancing cloud security capabilities

1

Security capability development based on risks and gaps



Derive relative risks from actual cloud application and service gap assessments



Further prioritization of which security domains to focus on first

2

Security architecture dependencies



Dependencies between security architecture components to enable capabilities



Enabling visibility and monitoring of security risks in the cloud

3

Strategic investment



Align security investment with business priorities and investments



Security architecture with AWS



Prioritize applications and services to address first based on risk profile

4

Cost and effort



Prioritize initiatives based on cost and risk



Roadmap is a phase approach and dependent on organizational maturity and ability to absorb change

Factors that
need to be
prioritized










Deloitte cloud cyber risk capabilities

Prioritize objectives to address typical challenges

Challenges

- Does the organization know the business objectives for the compliance, security, and operations of the AWS cloud?
- Are the data assets being put in the AWS Cloud already inventoried and classified?
- How can security keep up with DevOps that is already configuring and deploying on AWS?
- How should the various cloud services integrate with the existing enterprise security architecture?
- Is the security design aligned with the business delivery model and AWS cloud architecture?
- What enhanced policies, processes, security capabilities are needed for compliance?
- How does the organization keep up with compliance maintenance?

Objectives

-  Identify and prioritize cyber risk capabilities needed for the AWS solution. Separate anecdotes from must-have requirements.
-  Manage cloud data protection and privacy
-  Security as a baseline within standardized and repeatable DevOps
-  Align cloud environment with existing enterprise security architecture and control requirements to drive value
-  Agile and modular security architecture with repeatable practices
-  Introduce secure operations changes to achieve compliance
-  Develop benchmarking criteria for measuring operational efficiency and maturity development

Compliant
& secure
AWS
cloud

Proactively managing cloud cyber risk and developing an adaptive strategy

Challenges and opportunities

- What the organization's current exposure to cloud cyber risks?
 - Determine current cloud cyber risk profile based on present inherent risk and identify prioritized risk-based cloud strategy
- Are cyber risk investment/processes are really working for cloud services?:
 - Real world testing to confirm the effectiveness of security controls across cyber risk domains
- There has been an increase in number of attacks such as phishing/hack/other security incidents targeted against the company:
 - Understand what the adversary sees and how the adversary approaches exploiting your company's risks
- We need a "Cloud Security Assessment" for compliance readiness

Results

- Deloitte is a leading provider of cyber risk management solutions
- Organization with the breadth, depth and insight to help complex organizations become secure, vigilant, and resilient.
- Access to 11,000 risk management and security professionals globally across the Deloitte Touche Tohmatsu Limited (DTTL) network of member firms.

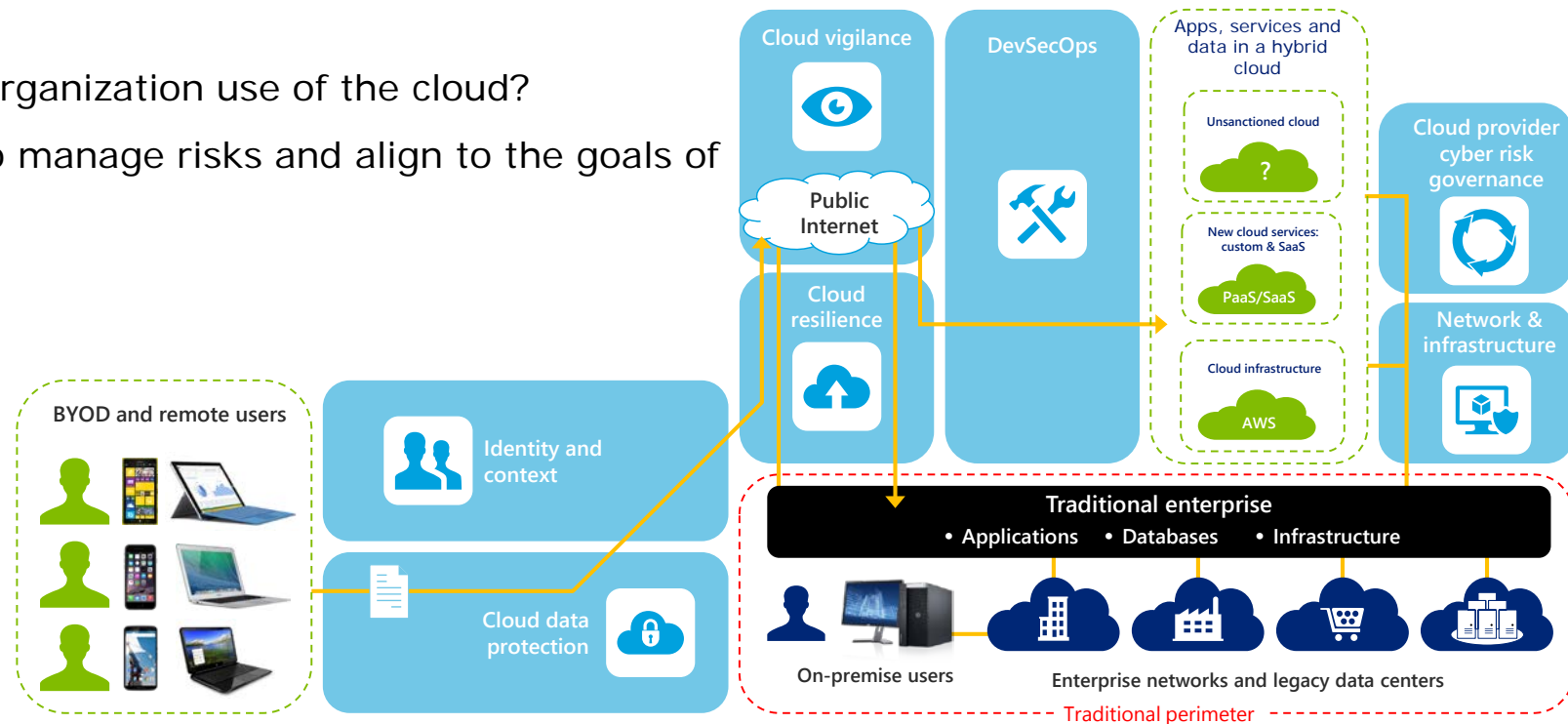
Our selected key solutions

Cloud risk assessment	<ul style="list-style-type: none">Identify cloud cyber risks and provide specific recommendations to remediate the risksDefine prioritized strategic cloud cyber risk roadmap
Cloud platform assessment	<ul style="list-style-type: none">Determine ability to identify / track cyber security risks for platformsIdentify gaps and prioritize recommendation to improve platforms' security posture and cyber defense controls
Cyber risk strategy implementation	<ul style="list-style-type: none">Establish overall cyber risk strategyConfirm existing capability gap/fit for cyber risk requirementsDevelop core cyber risk conceptual designsDevelop integration plans covering technical specifications for priority cloud technologyEstablish project teamAssign integration roles and responsibilitiesScope and plan additional cyber risk capability improvementsProvide on going implementations support
CASB implementation	<ul style="list-style-type: none">Continuous visibility to cloud usage and risk exposureManage risk and complianceProtect data and privacyMonitor security activity and threats
Cyber wargames	<ul style="list-style-type: none">Improve cyber response plan by exposing missing roles, data , and controlsBuild consensus and shared vision through practice in a safe environmentIncrease probability of success if/when faced with similar event
Secure Software Enablement (SSE)	<ul style="list-style-type: none">Integrated, managed service solution to enable the design, construction, and deployment of secure applications and systemsAddress security risks within applications, continuously monitor, remediate application security risks and defects
Threat intelligence and analytics	<ul style="list-style-type: none">Provide specific threat insights through ongoing research, custom threat reports, technical indicators, and monthly executive briefings

Conduct cloud assessment to identify and prioritize risks

Identify customer control risks and provide specific recommendations to remediate the risks:

- What is the actual cloud service inventory/use?
- Do the organization's existing controls meet industry and organization standards?
- What is the inherent risk for the organization use of the cloud?
- What are the recommendations to manage risks and align to the goals of the business?



Cloud Access Security Broker (CASB) implementations

Continuous visibility to the hybrid cloud usage and risk exposure

Definition



A new class of security products (tools and services) that reside between the enterprise and a cloud provider that acts as an extension to enterprise controls across risk management, data privacy and protection, and monitoring for cloud-based services.

Common problems



- Shadow IT
- Ability to manage and measure risk in the extended enterprise
- Lack of consistent data protection and privacy across cloud providers
- Inadequate visibility in cloud activity

Typical capabilities



- Understand cloud usage and risk exposure
- Manage risk and compliance
- Protect data and privacy
- Monitor security activity and threats

Technology companies in the space

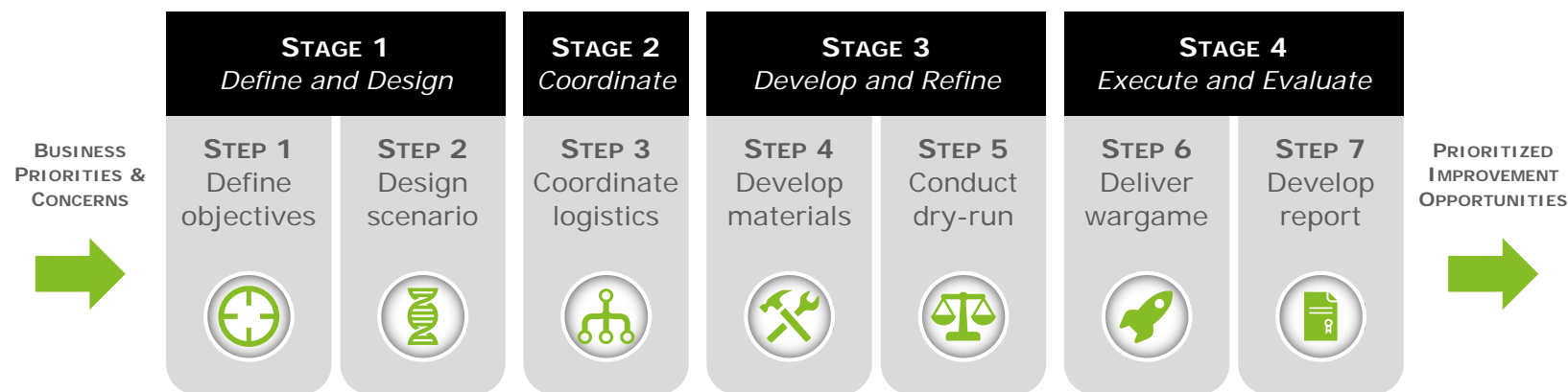


30 CASB Providers



Deloitte's approach to designing and delivering cyber wargames

Effective cyber wargames require precise planning, structured execution, and comprehensive post exercise analysis. Through experience delivering hundreds of wargames, Deloitte has developed a seven-step approach and toolkit to support the consistent delivery of effective cyber wargames.



Deloitte's Cyber Wargaming Toolkit

Methodology	A wargame design and engagement execution methodology informed by military practices, educational research, and Deloitte's experience from prior engagements	Scenario and Inject Inventories	An inventory of scenarios, ranging from basic to complex; and inventory of injects including SOC alerts, news articles, social media feeds, news clips, etc.	Delivery Tools	Customized tools to enable realistic exercises – including a secure player communications platform, electronic player status placards, and participant polling system
Engagement Artifacts	A library of sample artifacts and templates – including activity checklists, design workbooks, facilitator guides, etc.	Training Material	Materials to train cyber wargame facilitators, players, and observers on how to participate effectively in a cyber wargame	Production Team	An experienced roster of printers, video producers, etc., to support efficient, secure, and quality production of wargame materials

Appendix

Why Deloitte



Providing value at the intersection of risk, regulation and technology

- We have a dedicated cloud cyber risk practice and alliances with leading cloud security vendors
- Use a case-driven innovation environment built on emerging platforms and technologies designed to help clients address cloud cyber risk
- We assisted in developing the National Institute of Standards and Technology (NIST) cyber security framework
- We are currently assisting in the development of Cloud Security Application Program Interface Standards the Cloud Security Alliance (CSA) working group
- We bring deep understanding of the client-side role in the collaborative relationship between client and cloud vendor, through security program engagements for some of the largest cloud providers
- Our services are built on leading cloud security technologies, leveraging pre-built integrations to shorten time-to-value
- Our Secure.Vigilant.Resilient.™ Cyber Risk Management Framework helps clients manage their information risks and provides a structure for governance and organizational enablers
- Our rich experience across a range of industry sectors guides focus on the regulations, standards, and cyber threats that are most likely to impact your business
- We are recognized by major analyst firms as a global leader in security

Depth and breadth of experience

- Approximately 2,000 cyber risk professionals in the US
- Part of a global network of 11,000 risk management and cyber risk professionals across the DTTL network of member firms

Our cloud accelerators

Deloitte leverages demonstrated proven methodologies and standard accelerators to streamline engagement activities

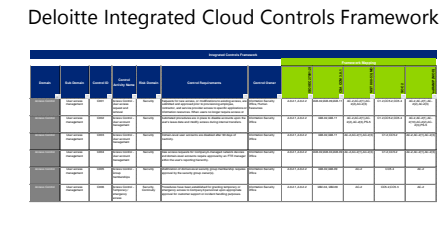
Deloitte Secure.Vigilant.Resilient.™ Framework

Deloitte has IT assessment data Gathering templates, which can be customized for an enterprise's needs to evaluate current risk. Deloitte can analyze the risk gap and make prioritized recommendations through pre-developed models.



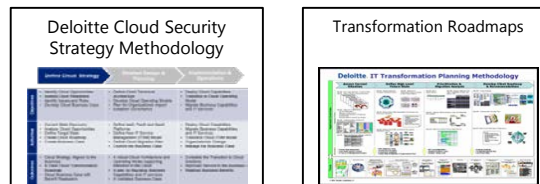
Deloitte Cloud Controls Framework

Deloitte has an Integrated Cloud Controls Framework with mappings to industry control sets and common controls,. It is an accelerator and can be customized for an enterprise's specific controls environment.



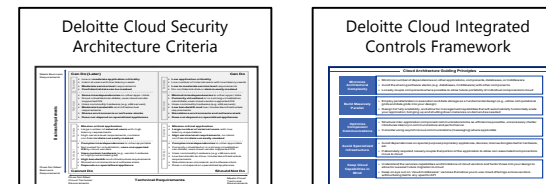
Cloud Security Strategy

Deloitte has experience in building cloud security strategy and roadmaps that can be leveraged to identify business drivers and requirements for cloud cyber risk management.



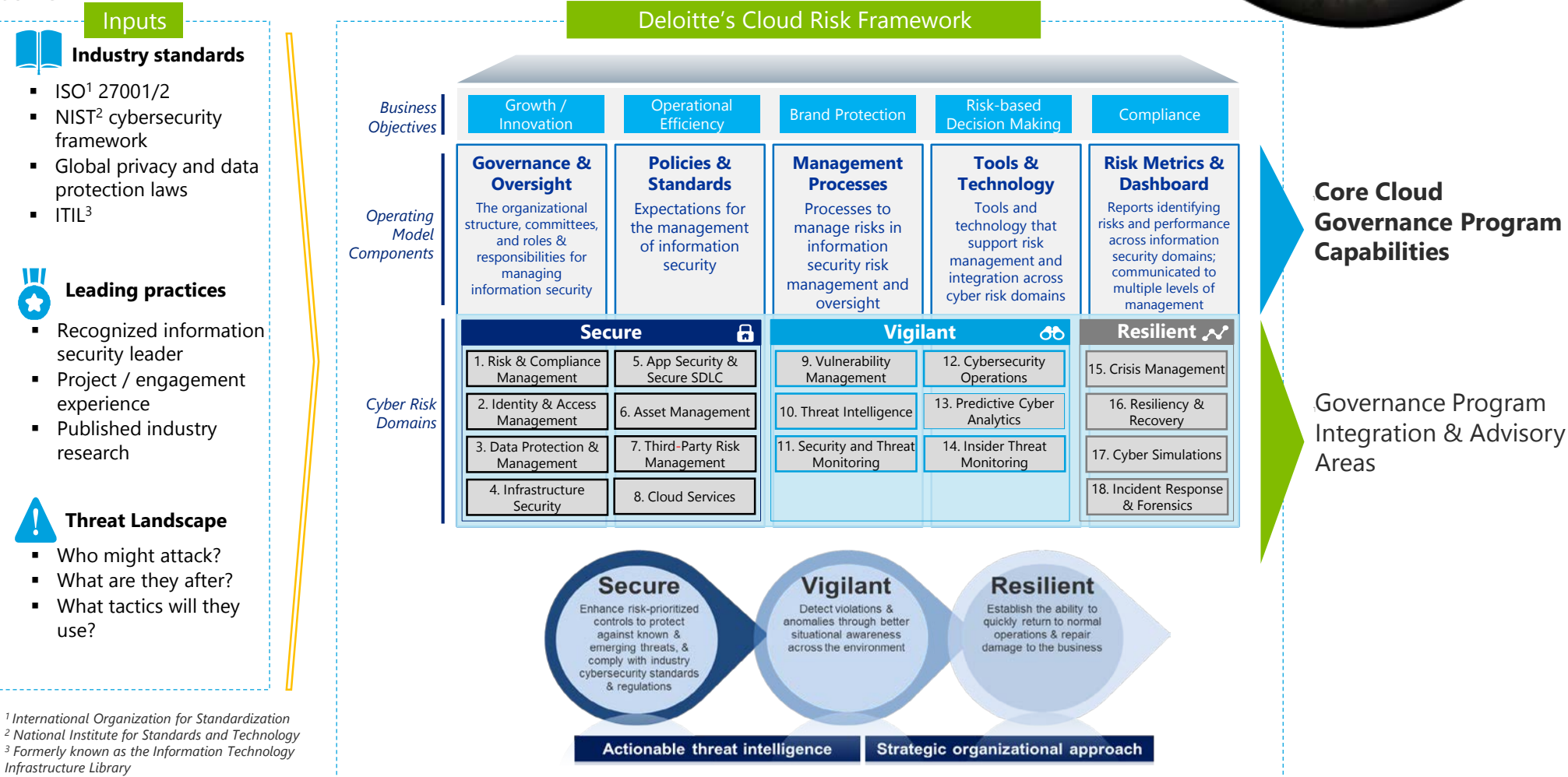
Cloud Security Architecture

Deloitte has a repository of Cloud Security Architecture Guiding Principles and Controls Framework, which can be leveraged to build cloud security blueprints for the future cloud cyber risk program.



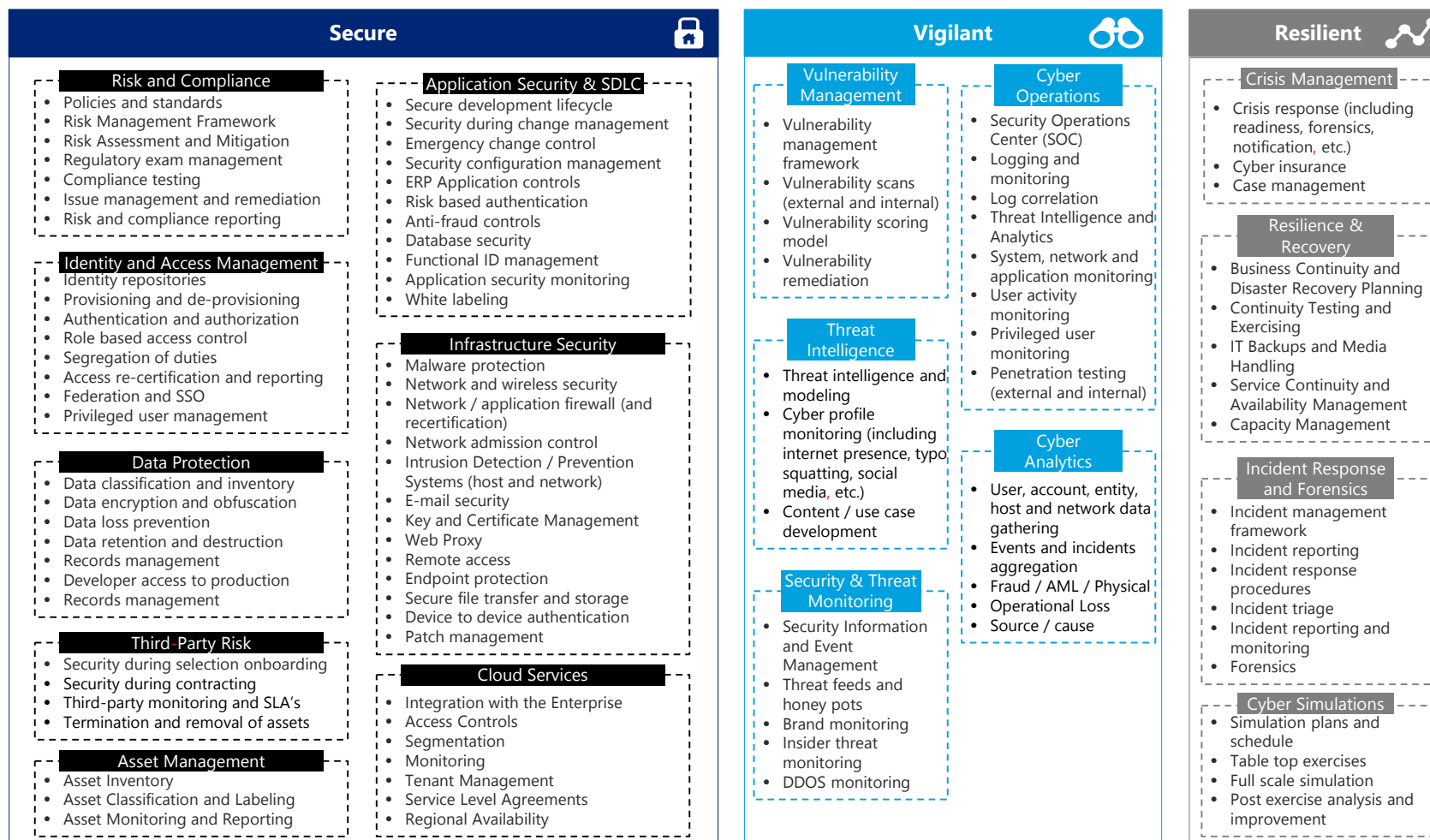
Cloud Risk Framework and Cloud Governance

Deloitte's cloud risk framework and services incorporate key security areas and is built on industry leading practices and regulatory expectations. It allows an organization to take stock of current capabilities to manage cloud risk.



Deep Dive – Deloitte Cloud Risk Framework Components & Capabilities

Deloitte's cloud risk framework is organized by key capability areas that cover leading practices that are prevalent in many organizations. These capability areas are derived based on our experience serving clients, industry leading practices and applicable regulatory requirements.





Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation 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 shall not be responsible for any loss sustained by any person who relies on this presentation.

Copyright © 2017 Deloitte Development LLC. All rights reserved.