Cloud Cyber Risk Management

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

Deloitte
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.
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.

Managing cyber risk is a shared responsibility.
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

BYOD and remote users

---

Traditional enterprise
- Applications
- Databases
- Infrastructure

On-premise users
Enterprise networks and legacy data centers

Traditional perimeter

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

BYOD and remote users

---

Traditional enterprise
- Applications
- Databases
- Infrastructure

On-premise users
Enterprise networks and legacy data centers

Traditional perimeter
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

- Identity and context
- Cloud data protection
- Cloud vigilance
- DevSecOps
- Cloud resilience
- Apps, services and data in a hybrid cloud
- Cloud provider cyber risk governance
- Network & infrastructure
- Traditional enterprise
  - Applications
  - Databases
  - Infrastructure
- Unsanctioned cloud
- New cloud services: custom & SaaS
- Cloud infrastructure
- AWS

BYOD and remote users
On-premise users
Enterprise networks and legacy data centers
Traditional perimeter

Copyright © 2017 Deloitte Development LLC. All rights reserved.
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

---

Copyright © 2017 Deloitte Development LLC. All rights reserved.
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

---

### Traditional Enterprise

- Applications
- Databases
- Infrastructure

### On Premise Users

### Enterprise Networks and Legacy Data Centers

### Traditional Perimeter

---

### BYOD and remote users

---

### Data governance, data protection & privacy policies

---

### Apps, services and data in a hybrid cloud

- Unsanctioned cloud
- New cloud services: custom & SaaS
- AWS
- PaaS/SaaS

---

### Key management

---

---
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**

<table>
<thead>
<tr>
<th>IR lifecycle</th>
<th>Key focus areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident detection logging and tracking</td>
<td><strong>Incident detection logging and tracking</strong></td>
</tr>
<tr>
<td>Categorization and prioritization</td>
<td>• Perform the analysis for understanding what incident types are possible for AWS cloud integration.</td>
</tr>
<tr>
<td>Initial diagnosis</td>
<td><strong>Categorization and prioritization</strong></td>
</tr>
<tr>
<td>Communication, containment and escalation</td>
<td>• 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.</td>
</tr>
<tr>
<td>Investigation and diagnosis</td>
<td><strong>Initial diagnosis</strong></td>
</tr>
<tr>
<td>Resolution and recovery</td>
<td>• 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.</td>
</tr>
<tr>
<td>Incident closure</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Communication, containment, and escalation</strong></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Determine and establish proper communication paths (escalation, hand-off, etc.) with AWS that can be consistently followed in the event of an incident.</td>
</tr>
<tr>
<td></td>
<td><strong>Investigate and diagnosis</strong></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Resolution and recovery</strong></td>
</tr>
<tr>
<td></td>
<td>• Post Recovery &quot;Lessons Learned&quot; activities involves sharing detailed incident reports with AWS and related organizations, in addition to your internal IR team.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Foundation &amp; discovery</th>
<th>Readiness</th>
<th>Onboarding</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the business strategy and growth objectives to align cloud adoption capabilities and priorities</td>
<td>Building a holistic cloud governance and risk management framework for consistency and efficiency</td>
<td>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</td>
<td>Operationalization of the cloud governance framework across the enterprise through onboarding of business units, products and functions</td>
<td>Continuous management and improvement of the cloud governance program through assessment, monitoring, tool deployment, extension of program, etc.</td>
</tr>
</tbody>
</table>
The path for enhancing cyber risk management for customer cloud control responsibilities

1. Establish governance and technology
   Establish controls & responsibilities specific for the cloud to address governance and technology gaps that will support risk reduction efforts.

2. Assess cloud security risk
   Baseline security requirements and assess current maturity and capabilities, identify and prioritize gaps and create roadmap for secure cloud as an integrated part of your cloud strategy.

3. Design security capabilities
   Build a baseline reference security architecture and repeatable design patterns with a prioritized implementation plan.

4. Implement security capabilities
   Build, test and deploy a robust security architecture with integrated controls. Deploy and document updated processes.

5. Maintenance and support
   Detail a support model, establish a baseline and sustain operation of services.
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
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**

<table>
<thead>
<tr>
<th>Service</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud risk assessment</td>
<td>- Identify cloud cyber risks and provide specific recommendations to remediate the risks</td>
</tr>
<tr>
<td></td>
<td>- Define prioritized strategic cloud cyber risk roadmap</td>
</tr>
<tr>
<td>Cloud platform assessment</td>
<td>- Determine ability to identify / track cyber security risks for platforms</td>
</tr>
<tr>
<td></td>
<td>- Identify gaps and prioritize recommendation to improve platforms’ security posture and cyber defense controls</td>
</tr>
<tr>
<td>Cyber risk strategy implementation</td>
<td>- Establish overall cyber risk strategy</td>
</tr>
<tr>
<td></td>
<td>- Confirm existing capability gap/fit for cyber risk requirements</td>
</tr>
<tr>
<td></td>
<td>- Develop core cyber risk conceptual designs</td>
</tr>
<tr>
<td></td>
<td>- Develop integration plans covering technical specifications for priority cloud technology</td>
</tr>
<tr>
<td></td>
<td>- Establish project team</td>
</tr>
<tr>
<td></td>
<td>- Assign integration roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>- Scope and plan additional cyber risk capability improvements</td>
</tr>
<tr>
<td></td>
<td>- Provide on going implementations support</td>
</tr>
<tr>
<td>CASB implementation</td>
<td>- Continuous visibility to cloud usage and risk exposure</td>
</tr>
<tr>
<td></td>
<td>- Manage risk and compliance</td>
</tr>
<tr>
<td></td>
<td>- Protect data and privacy</td>
</tr>
<tr>
<td></td>
<td>- Monitor security activity and threats</td>
</tr>
<tr>
<td>Cyber wargames</td>
<td>- Improve cyber response plan by exposing missing roles, data , and controls</td>
</tr>
<tr>
<td></td>
<td>- Build consensus and shared vision through practice in a safe environment</td>
</tr>
<tr>
<td></td>
<td>- Increase probability of success if/when faced with similar event</td>
</tr>
<tr>
<td>Secure Software Enablement (SSE)</td>
<td>- Integrated, managed service solution to enable the design, construction, and deployment of secure applications and systems</td>
</tr>
<tr>
<td></td>
<td>- Address security risks within applications, continuously monitor, remediate application security risks and defects</td>
</tr>
<tr>
<td>Threat intelligence and analytics</td>
<td>- Provide specific threat insights through ongoing research, custom threat reports, technical indicators, and monthly executive briefings</td>
</tr>
</tbody>
</table>
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

### BUSINESS PRIORITIES & CONCERNS

**PRIORITIZED IMPROVEMENT OPPORTUNITIES**

### STAGE 1 Define and Design

**STEP 1 Define objectives**

### STAGE 2 Coordinate

**STEP 2 Design scenario**

### STAGE 3 Develop and Refine

**STEP 3 Coordinate logistics**
**STEP 4 Develop materials**
**STEP 5 Conduct dry-run**

### STAGE 4 Execute and Evaluate

**STEP 6 Deliver wargame**
**STEP 7 Develop report**

---

Copyright © 2017 Deloitte Development LLC. All rights reserved.
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 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.

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.

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 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.

**Inputs**
- Industry standards
  - ISO\(^1\) 27001/2
  - NIST\(^2\) cybersecurity framework
  - Global privacy and data protection laws
  - ITIL\(^3\)
- Leading practices
  - Recognized information security leader
  - Project / engagement experience
  - Published industry research

**Threat Landscape**
- Who might attack?
- What are they after?
- What tactics will they use?

---

1. International Organization for Standardization
2. National Institute for Standards and Technology
3. Formerly known as the Information Technology Infrastructure Library
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.

<table>
<thead>
<tr>
<th>Secure</th>
<th>Vigilant</th>
<th>Resilient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk and Compliance</td>
<td>Vulnerability Management</td>
<td>Crisis Management</td>
</tr>
<tr>
<td>• Policies and standards</td>
<td>• Vulnerability management framework</td>
<td>• Crisis response (including readiness, forensics, notification, etc.)</td>
</tr>
<tr>
<td>• Risk Management Framework</td>
<td>• Vulnerability management</td>
<td>• Cyber insurance</td>
</tr>
<tr>
<td>• Risk Assessment and Mitigation</td>
<td>• Vulnerability scans (external and internal)</td>
<td>• Case management</td>
</tr>
<tr>
<td>• Regulatory exam management</td>
<td>• Vulnerability scoring model</td>
<td>• Resilience &amp; Recovery</td>
</tr>
<tr>
<td>• Compliance testing</td>
<td>• Vulnerability remediation</td>
<td>• Business Continuity and Disaster Recovery Planning</td>
</tr>
<tr>
<td>• Issue management and remediation</td>
<td>• Threat intelligence</td>
<td>• Continuity Testing and Exercising</td>
</tr>
<tr>
<td>• Risk and compliance reporting</td>
<td>• Threat intelligence and modeling</td>
<td>• IT Backups and Media Handling</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>• Cyber profile monitoring (including internet presence, typo squatting, social media, etc.)</td>
<td>• Service Continuity and Availability Management</td>
</tr>
<tr>
<td>• Identity repositories</td>
<td>• Content / use case development</td>
<td>• Capacity Management</td>
</tr>
<tr>
<td>• Provisioning and de-provisioning</td>
<td>• Log correlation</td>
<td>• Incident Response and Forensics</td>
</tr>
<tr>
<td>• Authentication and authorization</td>
<td>• Threat Intelligence and Analytics</td>
<td>• Incident management framework</td>
</tr>
<tr>
<td>• Role based access control</td>
<td>• System, network and application monitoring</td>
<td>• Incident reporting</td>
</tr>
<tr>
<td>• Segregation of duties</td>
<td>• User activity monitoring</td>
<td>• Incident response procedures</td>
</tr>
<tr>
<td>• Access re-certification and reporting</td>
<td>• Privileged user monitoring</td>
<td>• Incident triage</td>
</tr>
<tr>
<td>• Federation and SSO</td>
<td>• Penetration testing (external and internal)</td>
<td>• Incident reporting and monitoring</td>
</tr>
<tr>
<td>• Privileged user management</td>
<td>• Cyber Security Operations</td>
<td>• Forensics</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Threat Intelligence</td>
<td>Cyber Simulations</td>
</tr>
<tr>
<td>• Data classification and inventory</td>
<td>• Threat intelligence and modeling</td>
<td>• Simulation plans and schedule</td>
</tr>
<tr>
<td>• Data encryption and obfuscation</td>
<td>• Cyber profile monitoring (including internet presence, typo squatting, social media, etc.)</td>
<td>• Table top exercises</td>
</tr>
<tr>
<td>• Data loss prevention</td>
<td>• Network admission control</td>
<td>• Full scale simulation</td>
</tr>
<tr>
<td>• Data retention and destruction</td>
<td>• Intrusion Detection / Prevention Systems (host and network)</td>
<td>• Post exercise analysis and improvement</td>
</tr>
<tr>
<td>• Records management</td>
<td>• Key and Certificate Management</td>
<td></td>
</tr>
<tr>
<td>• Developer access to production</td>
<td>• E-mail security</td>
<td></td>
</tr>
<tr>
<td>• Records management</td>
<td>• Web Proxy</td>
<td></td>
</tr>
<tr>
<td>• Third-party risk</td>
<td>• Device to device authentication</td>
<td></td>
</tr>
<tr>
<td>• Security during selection onboarding</td>
<td>• Remote access</td>
<td></td>
</tr>
<tr>
<td>• Security during contracting</td>
<td>• Endpoint protection</td>
<td></td>
</tr>
<tr>
<td>• Third-party monitoring and SLA’s</td>
<td>• Secure file transfer and storage</td>
<td></td>
</tr>
<tr>
<td>• Termination and removal of assets</td>
<td>• Device to device authentication</td>
<td></td>
</tr>
<tr>
<td>• Cloud Services</td>
<td>• Patch management</td>
<td></td>
</tr>
<tr>
<td>• Integration with the Enterprise</td>
<td>• Cloud Services Management</td>
<td></td>
</tr>
<tr>
<td>• Access Controls</td>
<td>• Threat feeds and honey pots</td>
<td></td>
</tr>
<tr>
<td>• Segmentation</td>
<td>• Brand monitoring</td>
<td></td>
</tr>
<tr>
<td>• Monitoring</td>
<td>• Insider threat monitoring</td>
<td></td>
</tr>
<tr>
<td>• Tenant Management</td>
<td>• DOOS monitoring</td>
<td></td>
</tr>
<tr>
<td>• Service Level Agreements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Regional Availability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2017 Deloitte Development LLC. All rights reserved.