Managing Business Partner Risks in a Cloud and IoT Universe
Are companies prepared for the unforeseen?
June 2017
Agenda

Third-party risk in the cloud

- Did you know?
- Introduction
- Inherent challenges
- Traditional vs. cloud service provider (CSP)-specific third-party risk management (TPRM) lifecycle
- CSP risk assessment lifecycle
- Guiding principles to developing a risk-based approach
- Approach to handle risks related to CSPs
- Use cases

Third-party risk related to medical devices

- Connected health landscape
- Definition of connected medical devices
- The United States (US) regulatory landscape
- Phase 1: Vendor-level security risk assessment
- Deloitte’s Product Security Program™ Framework
- Phase 2: Product-level security risk assessment
- Use cases
- Success factors
Speaking today

**Amit Sood**  
Advisory Senior Manager  
Deloitte & Touche LLP  
*19+ years of experience in establishing third party risk management programs and conducting supplier assessments globally.*

**Anant Sethi**  
Advisory Senior Consultant  
Deloitte & Touche LLP  
*7+ years of cyber security experience serving healthcare providers. CISSP (ISC²), CCSFP (HITRUST)*

**David Messerschmidt**  
Advisory Consultant  
Deloitte & Touche LLP  
*2+ years of cyber security experience serving healthcare providers and medical device manufacturers*
Third-party risk in the cloud
Did you know?

With increased adoption of cloud computing, organizations are focusing on security of storing and processing critical data outside of the enterprise’s control, as seen through recent statistics.

By 2020, public cloud services market will grow rapidly to $236 billion. 20%-25% of businesses are already using SaaS to replace all or most of existing systems, up from single-digit percentages in 2011 and 2012. By 2021, 27% of corporate data traffic will bypass perimeter security.

20% of organizations will develop data security governance programs to prevent data breaches from public clouds by 2018.

80% of new deals for cloud-based cloud access security broker (CASB) will be packaged with network firewall, secure web gateway (SWG) and web application firewall (WAF) platforms by 2020.

---

Introduction

Despite the risks, businesses are now using CSPs for efficiency, economies of scale, cost and scalability.

New cloud-specific security and privacy standards are not fully integrated into the assessment process, reducing the level of trust in cloud assessments, and aggravating concerns about public cloud security.

- CSPs are a more **visible target**
- **Dependency vs. visibility** into on cloud providers’ controls
- **Substantial “shadow” usage** of cloud services, in addition to known usage by organizations

**Cloud Cyber Risks**

**Common Concerns**

- **Inadequate visibility in to cloud**: Traditional methods of inventorying CSPs’ does not provide an accurate list
- **Inability to identify, measure and manage cyber risks with cloud usage**: Generic security assessments on CSPs do not fit the bill any more
- **Inability to enforce security policies on enterprise cloud services**

**Industry Insights**

- By year-end 2018, **50%** of organizations with more than **2,500 users** will use a CASB product to control SaaS usage, up from less than **5% today**
Inherent challenges

As the regulatory scrutiny and expectations have increased, organizations have evolved their CSPs’ Management (CSPM) programs. However, in managing these programs, organizations face some challenges.

- Assess and **stay ahead of the breakpoints** in CSP relationships
- **Bridge the gap between** those in the business and compliance & risk staff
- An effective organizational structure with **clear roles, accountability, and responsibility** - at multiple levels

- Using appropriate **tools & technologies** and use data & analytics to make informed decisions about CSP relationships
- Determine whether to **outsource or insource**, build or buy? And what delivery models to take advantage of

- **Constantly evolve** and yet able to manage relationships, and keep up with regulatory and compliance requirements

- **Manage and track** CSP performance and contract compliance
- An **integrated view of risk** across multiple risk areas, e.g., compliance, privacy, operational risk, business continuity
- Conducting **due diligence processes** that are integrated with overall CSP lifecycle, specially the one with higher inherent risk

- **Maintaining a consolidated inventory** of CSPs across business units and functions

- **Handle implementation challenges and drive adoption** of the program
- **Effective communication/ awareness programs** with business and their CSPs
- **Consistent adherence to process and strategy** when CSP is on boarded or terminated
## Traditional vs. CSP-specific TPRM lifecycle

The following risk management activities are proposed for the target state TPRM program:

<table>
<thead>
<tr>
<th>Pre-Selection</th>
<th>Contracting</th>
<th>Onboarding</th>
<th>Ongoing Monitoring</th>
<th>Off boarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide a subjective analysis of the risk posture of the prospective vendors</td>
<td>• Determine risk classification / tiering of the shortlisted vendor</td>
<td>• Confirm necessary checkpoints and pre requisites have been met prior to vendor initiate service delivery</td>
<td>• Determine gaps in vendor controls</td>
<td>• Confirm proper termination of vendor, addressing all potential risks to the organization</td>
</tr>
<tr>
<td>• Assist business in taking informed decision in vendor selection</td>
<td>• Determine frequency of ongoing monitoring assessments / audits</td>
<td>• Determine gaps in vendor controls</td>
<td>• Re-classify vendors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Determine sub-domains to be assessed in detail in the future</td>
<td>• Track and monitor gaps to closure (via remediation plans)</td>
<td>• Track and monitor gaps to closure (via remediation plans)</td>
<td></td>
</tr>
<tr>
<td>Traditional Model</td>
<td>CSP-specific Model</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ask questions in RFP around typical risks posed by CSPs.</td>
<td>• Refrain from <strong>clickware</strong> (T&amp;Cs) which does not undergo proper legal reviews.</td>
<td>• Engage a CASB before integration with a CSP.</td>
<td>• Modify ongoing monitoring assessment questions based on the output of the Inherent risk assessment.</td>
<td></td>
</tr>
<tr>
<td>• Conduct due diligence while comparing CSPs providing similar services.</td>
<td>• Refrain from static contract clauses, instead have flexible contract clauses to address the new threat landscape.</td>
<td>• Determine access provision and deprovision controls.</td>
<td>• Determine where and how data will be retained by the CSP in compliance with the contractual requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Customize contracts based on the risk posture of the CSP.</td>
<td></td>
<td>• Confirm proper data redaction where applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Develop a plan to address a breach that occurs after contract termination</td>
<td></td>
</tr>
</tbody>
</table>
CSP risk assessment lifecycle

Each CSP risk assessment goes through the six phases described below and involves coordination and involvement between the line of business that owns the relationship with the CSP, the TPRM team that oversees the assessment, the lead assessor (LA) that conducts the risk assessment, and the CSP.

- **Scoping**
  - Inherent risk questionnaire, scoring methodology

- **Request**
  - Submit assessment request to TPRM

- **Assess**
  - Training, specialized assessors, established baselines

- **Remediation**
  - Technology-based, self-service platform
  - Increased risk accountability
  - Ease of business operations

- **Closure**
  - Risk rating criteria

- **Report**
  - QA checklist, reporting format

- **Remediation Tracking**
  - Remedy plan templates

- **Closure**
  - Risk rating criteria

- **Consistent treatment of open/residual risk**
- **Technology-driven tracking and remediation workflow**

- **Enhanced scope based on risk tier and service category of CSP**
- **Tailored CSP review approach**

- **Enhanced risk management accountability and ownership**
- **Consistent interpretation of risk ratings across lines of business (LOBs)**
Managing Business Partner Risks in a Cloud and IoT Universe

Because cloud strategies usually lag cloud use, most organizations already have a surprising amount of unsanctioned, and even unrecognized, public cloud usage. Especially when sensitive or regulated data is involved, unapproved clouds represent an unnecessary risk exposure.

We propose an approach to address these issues based on the following guiding principles:

**Automate Identification and Management (Leveraging CASB)**

Analyze metadata obtained from CASB (e.g., cloud usage, data movement etc.) to:

- Identify shadow IT usage
- Understand total risk based on inherent rating, data movement and number of users
- Enable governance of cloud services, allowing exceptions based on risk tolerance

**Define a Cloud Risk Lifecycle Governance**

We propose an assessment approach that can address traditional issues and gaps currently in the market, including:

- Enumeration
- Risk tiering
- Risk analysis
- Risk remediation
Approach to handle risks related to CSPs

The level of due diligence that should be performed on various types of cloud providers varies with service types, business functions, regulatory compliance requirements, and a host of other factors.

** Enumeration
Identify and use a CASB in the cloud to gather meta data and provide cloud usage information such as:
- Meta data traffic
- Inventory of cloud usage

** Risk Tiering
Manual analysis of the cloud inventory to categorize CSPs based on inherent risk, scope of the services offered, volume of the data handled, etc. Some of the typical categories of CSPs include:
- Streaming Service
- File Sharing Service
- Chat/IM Service
- Placeholder for other categories

** Risk Reduction / Remediation
Tracking and mitigation of associated risks after recommendations include:
- Review and block the unwanted and unapproved services allowed by CSPs.
- Rewrite and negotiate the contract with CSPs to meet the client organization’s cloud cyber risk standards.
- Implement and enforce policies by enterprises on cloud usage responsibility and cloud risk acceptance processes.

** Risk Analysis / Recommendation
Analysis
- Analysis of the cloud cyber risk posture of the client organization against the contractual agreement of services by the CSPs for adequacy of technological capabilities and relevant assessment methodologies.

Recommendation
- Recommendations for client organization to upgrade the technological capabilities in order to fill the gaps with CSPs services and protect the data at risk.
## Use cases (1 of 3)

### USE CASE 1

<table>
<thead>
<tr>
<th>Client requirements</th>
<th>Solution/output</th>
</tr>
</thead>
</table>
| Enhancement of client’s current cloud cyber risk program in order to:  
  - Enable consistent cyber risk management practices (e.g., incident response, threat intelligence)  
  - Manage potential security risks and support the development of a "security aware" culture across all of the client | Key initiatives identified to reduce cyber risks:  
  - Cloud risk management program which defines operating model for cloud services security reviews, design, and management  
  - Implement multi-factor authentication to enhance security of cloud services usage  
  - Secure Office 365 implementation by applying adequate controls  
  - Guiding principles for CASB pilot and design support CASB implementation |
|  | **Cloud cyber risk assessment**  
  - Inherent & residual risks for cloud services identified  
  - Strategic roadmap created for guidance |

### USE CASE 2

<table>
<thead>
<tr>
<th>Client requirements</th>
<th>Solution/output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement strategic recommendations to enhance the cloud security components of the client’s program aimed at increasing the overall cyber security posture across traditional and cloud landscapes.</td>
<td></td>
</tr>
</tbody>
</table>
  - Determined key initiatives identified to reduce cyber risks  
  - Revise governance risk and compliance to cover all cloud service models (SaaS, IaaS, PaaS)  
  - Assess IAM capabilities to determine maturity and scalability for cloud consumption  
  - Define processes and implement tools to enhance system and vulnerability management  
  - Enhance incident response capabilities to include cloud in scope |
|  | **Cyber landscape assessment**  
  - In-flight cyber enhancement program assessment  
  - Areas of opportunity to enhance cloud security posture determined |
Use cases (2 of 3)

**USE CASE 3**

**Client requirements**
Understand the client’s inherent risk for cloud and steps to address gaps in strategy and protection of their environment

**Solution/output**
Key initiatives identified to reduce cyber risks:
- Identified more than 2,000 cloud services being utilized, 90+ high risk and 300+ medium risk of traffic to cloud services
- Recommendations to implement cloud governance, data loss prevention (DLP), access management tool and process updates to address high risks identified

- **Client interviews**
- **Scanned environment for Shadow IT**
- **Assessed selected PaaS and SaaS against leading standards**
- **Risk posture identified**

**USE CASE 4**

**Client requirements**
Understand the current state of the client’s enterprise cloud services consumption.

**Solution/output**
- **Cyber risk assessment using NIST CSF and CSA CCM**
- **Stakeholder interviews**

- **Prioritized plan developed**
- **Scanned environment for Shadow IT**
- **Cloud governance operating model and plan developed**

- **Recommendations to implement cloud governance operating model, cloud infrastructure baseline framework, expanding their threat & Vulnerability Management program to extend out to the cloud, data classification program encompassing Data Loss Prevention (DLP) solution to control sensitive data, IAM solution**
- **Provided cloud discovery report, identified over 1700 cloud services being utilized, 126+ high risk being consumed by the workforce and contractors**
Use Case (3 of 3)
Sample outputs of an assessment conducted on CSPs.

**30 of the discovered cloud services were previously risk assessed by IT Security.**
The cloud applications below have been through at least one security review to understand risks and needed controls. IT owners have been documented and other key attributes have been documented in client’s service catalog.

**100+ of the discovered cloud services are likely used for business, but not formally risk assessed by IT Security.**
The cloud applications below have not undergone any security reviews. However, the IT owners know that these applications are genuine and can be used for business purposes.

**The remaining 2000+ cloud services may be for personal or Shadow IT use.**
Typical personal cloud apps, such as social media sites, are among the highest use non-business apps. However, there are many more cloud services which should not be accessed from client’s networks or endpoints.

**Sample Assessment Snapshots**
Third-party risk and medical devices
Connected health landscape

"Cyber security for the healthcare and pharmaceutical sectors of the S&P 500 index worsened at a faster rate in the past year than for the other sectors."


Big data management
Companies will need to safeguard intellectual property, personally identifiable information, patient health information by complying with privacy laws and norms across jurisdictions.

Regulatory Implications of Cloud Usage
Health authorities appear to be focusing attention on cloud platform cyber risks that could inadvertently impact patient safety or product quality.

Cloud-Based Computing Attacks
With the migration of software to the cloud, the life sciences (LS) sector has been exposed to new challenges, such as Distributed Denial of Service (DDoS)attacks.

Med-Tech Security Concerns
The increasing quantity and types of potential cyber-security threats pose risks to patient confidentiality, integrity of device and patient data, and device operation.

Ransomware
Health care has become a frequent target of cyberattacks as their data (i.e., intellectual property, personally identifiable information, patient health information) is valuable; vulnerabilities are expanding as health info is shared more broadly and more individuals/organizations have access to systems.

Third-Party Access
LS companies are working with an increasing number of third parties – leading to multiple connection points and information exchange, resulting in increased cyber risk.

Harnessing the power of connected health will be a critical capability for LS companies, especially with the industry move towards value-based care and evolving patient engagement expectations and “patients-as-consumers” behavior.

There are a variety of risks associated with the move to connected health, especially around cyber security, and leading in this space will require building strong collaborative relationships with leading technology companies and other ecosystem players.
Definition of connected medical devices

**Definitions**

- **Medical Device**: Section 201(h) of the Food, Drug and Cosmetic Act defines a medical device as any healthcare product that does not achieve its principal intended purposes by chemical action or by being metabolized.

- **Connected Medical Device**: A medical device, as defined by the Food, Drug and Cosmetic Act, which communicates via a private network, public Internet, or point-to-point connection (wired or wireless) or can be accessed in standalone mode via a user or machine interface.

**Common vulnerable components**

<table>
<thead>
<tr>
<th>Device software</th>
<th>Firmware</th>
<th>Removable media</th>
<th>Physical access</th>
<th>Database and/or storage</th>
<th>Clinical applications (e.g., treatment planning software)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote support/maintenance</td>
<td>Device hardware</td>
<td>Network access/firewall</td>
<td>Operating system</td>
<td>Ports/interface</td>
<td></td>
</tr>
</tbody>
</table>
The United States (US) regulatory landscape

Medical devices distributed in the United States are subject to FDA General Controls that include pre-market and post-market regulatory controls.

**FDA Premarket Guidance on Medical Device Cybersecurity**

- Manufacturers should address cybersecurity during the “design and development” of the medical device
- The scope of the “Guidance” covers 510k, de novo submissions, pre-market approvals (PMAs), product development protocols, and humanitarian device exemption
- The FDA is looking for a specific list and justification of cybersecurity risks that were considered in the design of the device, the controls considered, summary plan, and device instructions

The FDA recommends that medical device manufacturers consider the cybersecurity framework core functions to guide their cybersecurity activities: Identify, Protect, Detect, Respond, and Recover (found in the National Institute of Standards and Technology’s (NIST) Framework for Improving Critical Infrastructure Cybersecurity)

**FDA Postmarket Guidance on Medical Device Cybersecurity**

- Medical device security is a shared responsibility between medical device manufacturers and healthcare providers
- The scope of the “Guidance” covers medical devices that contain software or programmable logic and software that is classified as a medical device
- Critical components of the cybersecurity risk management program include monitoring cybersecurity information sources, detecting vulnerabilities, establishing processes for vulnerability intake and handling, defining and deploying essential clinical performance to develop mitigations, and adopting a coordinated vulnerability disclosure policy and practice
- Manufacturers should participate in cybersecurity Information Sharing and Analysis Organizations (ISAOs) for sharing and dissemination of cybersecurity information and intelligence

The FDA recognizes that medical device cybersecurity is a shared responsibility between stakeholders including healthcare facilities, patients, providers, & medical device manufacturers

Source:
- [FDA Postmarket Guidance on Medical Device Cybersecurity](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf)
Phase 1: Vendor-level assessment strategy

The first phase of procuring a connected medical device is an assessment of the vendor and the processes they have in place to securely design, develop, and maintain the connected medical devices they are marketing.

High-level Overview of Steps

- Healthcare provider (HCP) to identify if vendor has an established medical device security organization
- If Vendor has a medical device security organization, HCP to assess that organization against a leading practice security framework (e.g., Deloitte’s Medical Device Security Program™ (MDSP):
  - Identify gaps against the identified security framework and the associated level of risk
  - As appropriate, escalate risk to leadership for approval
  - If the HCP concludes they would like to proceed with procurement, proceed to Phase 2: Product-Level Security Risk Assessment
Phase 2: Product-level assessment strategy

The second phase of procuring a connected medical device is a device-level security risk assessment of design and implementation features built into the device and installed upon fielding.

High-level Overview of Steps

- Option A: Vendor to provide the results of a security risk assessment and technical security test conducted by third party
  - HCP leadership sign off on the level of risk
  - Proceed with product procurement

- Option B: Vendor to provide the results of a security risk assessment and technical security test conducted in house
  - Vendor implements mitigating control
  - Terminate procurement

HCP to request vendor to provide device documentation including, but not limited to:

- Overview of the system
- Architectural, network, and data flow diagrams
- Software components
- Hardware components
- Network information
- Data assets and usage
Product security risk assessment framework

The overall depiction of the end-to-end security risk assessment process, which aligns with the FDA guidance and AAMI TIR57, is highlighted in the figure below. There are nine (9) steps that cover:

- Identification of assets, threats, and vulnerabilities
- A specific list of cybersecurity controls that were considered
- A “traceability matrix” that links the actual cybersecurity controls to the cybersecurity risks that were considered
- Assessment of the impact vulnerabilities on device functionality and end users/patients
- Assessment of the ability to exploit a threat and vulnerability
- Determination of risk levels and suitable mitigation strategies

**Detailed breakdown of a nine-step, end-to-end security risk assessment process, which aligns with FDA Guidance and AAMI TIR57:**

1. Conduct planning and information gathering
2. Identify applicable device profiles
3. Develop a component register
4. Perform controls analysis
5. Calculate the residual risk rating
6. Identify mitigating controls
7. Calculate the risk rating of the vulnerability
8. Identify vulnerabilities and pair with threats
9. Conduct threat modeling

The overall depiction of the end-to-end security risk assessment process, which aligns with the FDA guidance and AAMI TIR57, is highlighted in the figure below. There are nine (9) steps that cover:

- Identification of assets, threats, and vulnerabilities
- A specific list of cybersecurity controls that were considered
- A “traceability matrix” that links the actual cybersecurity controls to the cybersecurity risks that were considered
- Assessment of the impact vulnerabilities on device functionality and end users/patients
- Assessment of the ability to exploit a threat and vulnerability
- Determination of risk levels and suitable mitigation strategies
Technical Security Testing Methodology

The below graphic illustrates Deloitte’s methodology for conducting technical security testing of connected medical devices.

### Planning and initiation
- Plan, identify and map requirements around the medical device architecture
- Gather requirements for threat modelling

### Performing medical device technical security testing
- Perform technical testing on the components identified in the planning phase

### Roadmap development / reporting
- Create plans based on assessment of the gaps, the risk assessment, risk tolerance, and resource considerations

<table>
<thead>
<tr>
<th>Components</th>
<th>Types of testing</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Mobile App</td>
<td>Application security testing</td>
<td>• Prepare an executive summary and technical report based on the requirements.</td>
</tr>
<tr>
<td>Web App &amp; Services</td>
<td></td>
<td>• Prioritized roadmap</td>
</tr>
<tr>
<td>Wired &amp; Wireless Communications</td>
<td>Network security testing</td>
<td>• Technical engineering report:</td>
</tr>
<tr>
<td>System Functionalities</td>
<td>Firmware security testing</td>
<td>• Risk-ranked vulnerabilities with detailed recommendations suitable for engineering teams’ remediation efforts</td>
</tr>
<tr>
<td>Physical and Electronic Components</td>
<td>Hardware / Physical security testing</td>
<td>• Safety considerations</td>
</tr>
</tbody>
</table>

The below graphic illustrates Deloitte’s methodology for conducting technical security testing of connected medical devices.

![Diagram of Technical Security Testing Methodology](image-url)
Product and vendor assessment upkeep strategy

As part of a continuous assessment maintenance strategy, the HCP would re-assess the Vendor security risk posture driven by various changes, such as vendor mergers & acquisitions, vendor contract renewals, service-level agreement amendments, major product version upgrades, changes in available security control configuration options, and industry certification attestation schedules.

High-level Overview of Steps

• HCP to identify changes and assess the impacts
• During the change impact assessment, HCP requests vendor to provide documents that describe, but are not limited to:
  – Changes in the medical device security organization
  – Changes in service agreement contracts and processes
  – Changes of product details including intended and unintended use cases, security features and security controls, security change impacts to safety and privacy, known issues and plan of mitigation actions, available security configurations, etc.
• If the HCP concludes they would like to fully re-assess the vendor organization, proceed to Phase 1: Vendor-Level Security Risk Assessment
• If the HCP concludes they would like to fully re-assess the product, proceed to Phase 2: Product-Level Security Risk Assessment
Use Case – Healthcare Provider’s assessment integration into the procurement process

**Assessment Process & Inputs**

1. Assess the security program of the vendor
2. Submit product security questionnaire to the vendor
3. Assess vendor responses and request additional documentation as applicable
4. Complete product security risk assessment

**Assessment Components**

<table>
<thead>
<tr>
<th>Device profile</th>
<th>Threat model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product diagrams</td>
<td>Vulnerability list</td>
</tr>
<tr>
<td>Component register</td>
<td>Threat &amp; control mapping</td>
</tr>
<tr>
<td>Controls assessment</td>
<td>Risk treatment plan</td>
</tr>
</tbody>
</table>

**Toolkit**

- Device profile template
- Control framework
- Vendor subject matter expert questionnaire
- Threat register
- Risk register

**Organizational Integration**

Departments/functions may include: procurement, information technology, cyber security, risk management, clinical engineering

**Risk Context**

- Safety Context
- Regional Context
- Technical Context
- Business Context
Success factors

Establish criteria to determine device prioritization
Attributes such as care criticality, PHI volume, number of devices in use, upcoming procurement decisions, threat landscape changes, and other factors can help HCPs prioritize which devices to assess first.

Create and socialize information to be collected in advance of assessment
Different business functions may find value in different information, creating a risk of scope creep. Assessments can range from simple attribute-based checklists to comprehensive control-based assessments based on the HCP’s unique needs and security initiatives.

Use procurement/sales to open dialogue with the vendor
Medical device manufacturers are more likely to fully engage in assessment collaboration when procurement is involved in initiating the conversation.

Ensure the right people are engaged and have ownership of the process
The relevant medical device manufacturer subject matter experts from the product teams need to be engaged to provide organizational-insight and ensure that each step in the assessment process has an owner.

Process integration, automation, tooling, and scale can drastically increase efficiency
Organizational buy-in, cross-function collaboration, tooling (e.g., GRC), and learning efficiencies can dramatically reduce the cost and time needed to complete a device profile.
Q & A
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.