

# SUPPLY CHAIN SECURITY: MANAGING THIRD-PARTY RISK IN THE CLOUD ECOSYSTEM

John Stevenson, Joe Burkard and Siobhan Moran

October 7, 2021

Note: To ensure the best webinar experience, we recommend that you use Google Chrome as your web browser.

# UPCOMING WEBINARS

#ProtivitiTech

Register for the other webinars in our series!

#ProtivitiTech

Don't miss our

## Cybersecurity Webinar Series

Innovate. Transform. Succeed.

**Robert Half**  
Talent Solutions

**protiviti**

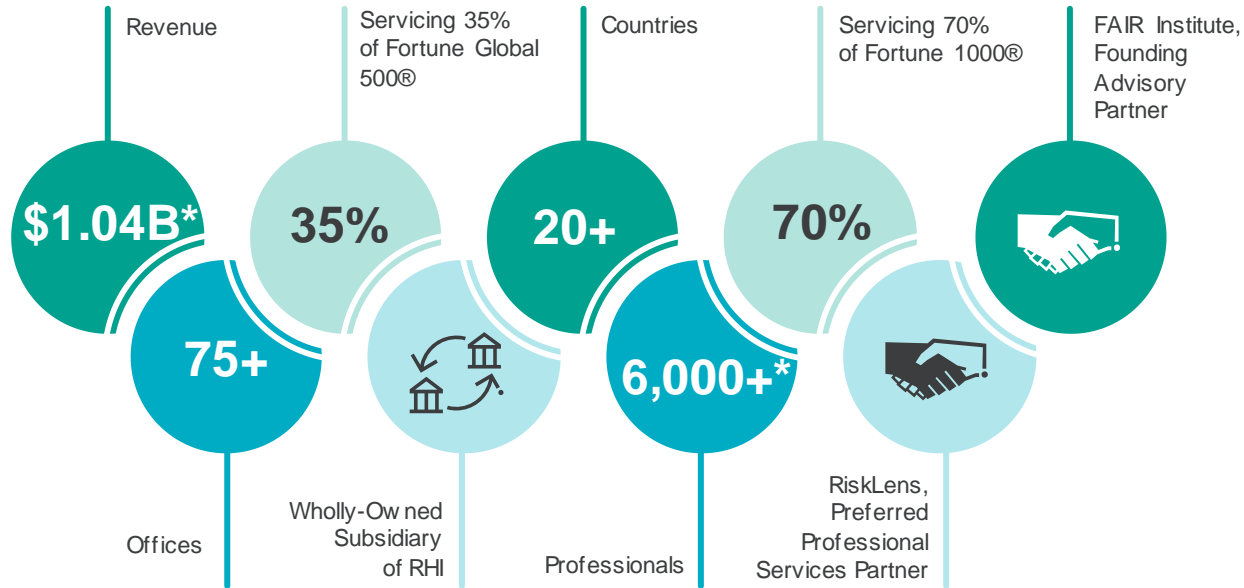
<p><b>Certifications – There Has to Be a Better Way</b></p> <p>Wednesday Oct 13 3 pm BST</p>	<p><b>Your Security Blanket: How to Develop an IAM Strategy that Works</b></p> <p>Thursday Oct 14 1PM ET</p>	<p><b>To Form a More Protected Union: Preparing for the Future of Cybersecurity</b></p> <p>Tuesday Oct 19 1PM ET</p>	<p><b>IT and OT and IoT, Oh My! Securing the “Enterprise of Things” With Microsoft Defender</b></p> <p>Thursday, Oct 21 1PM ET</p>
--	--	--	--

[Protiviti CyberSecurity Webinar Series Registration Link](#)

# ABOUT PROTIVITI

#ProtivitiTech

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders face the future with confidence. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.



# A FEW REMINDERS

- 1 Audio will be streamed through your computer.
- 2 If you are experiencing technical difficulties during the webcast or you have a question during the webinar, let us know by submitting your questions through the Q&A area of your screen.
- 3 We are recording today's webinar and it will be available for on-demand viewing following the live event.
- 4 Chrome is the recommended browser. Earlier versions of IE are no longer supported so if you are experiencing issues, please update IE or use another browser.
- 5 CPE credit is **not** available for this webinar.

# TODAY'S SPEAKERS

#ProtivitiTech



**John Stevenson**

Managing Director  
Security & Privacy – Cloud Security  
Protiviti



**Joe Burkard**

Director  
Security & Privacy – Cloud Security  
Protiviti



**Siobhan Moran**

Associate Director  
Security & Privacy – Cloud Security  
Protiviti

# TODAY'S TOPICS

#ProtivitiTech

**The Cloud Ecosystem**

**Challenges & Risks**

**Evolving TPRM for Cloud**

**Monitoring the Cloud: Case Study**

**Let's Talk About SolarWinds**

**Update GRC Processes**

**Final Thoughts**

# The Cloud Ecosystem

Future of remote work resides in the Cloud

# CLOUD SERVICE MODELS

#ProtivitiTech



Logos are registered trademarks of their owners

Key Characteristics and Benefits			
	IT Costs	Scalability	Deployment Efforts
<b>SaaS</b>	Licensing costs	Transparent – part of SaaS model	Already Deployed
<b>PaaS</b>	Lower <u>upfront</u> Costs	Improved	Quicker and Easier
<b>IaaS</b>	No infrastructure management costs	Dynamic (scaling up & out)	Faster with on-demand provisioning

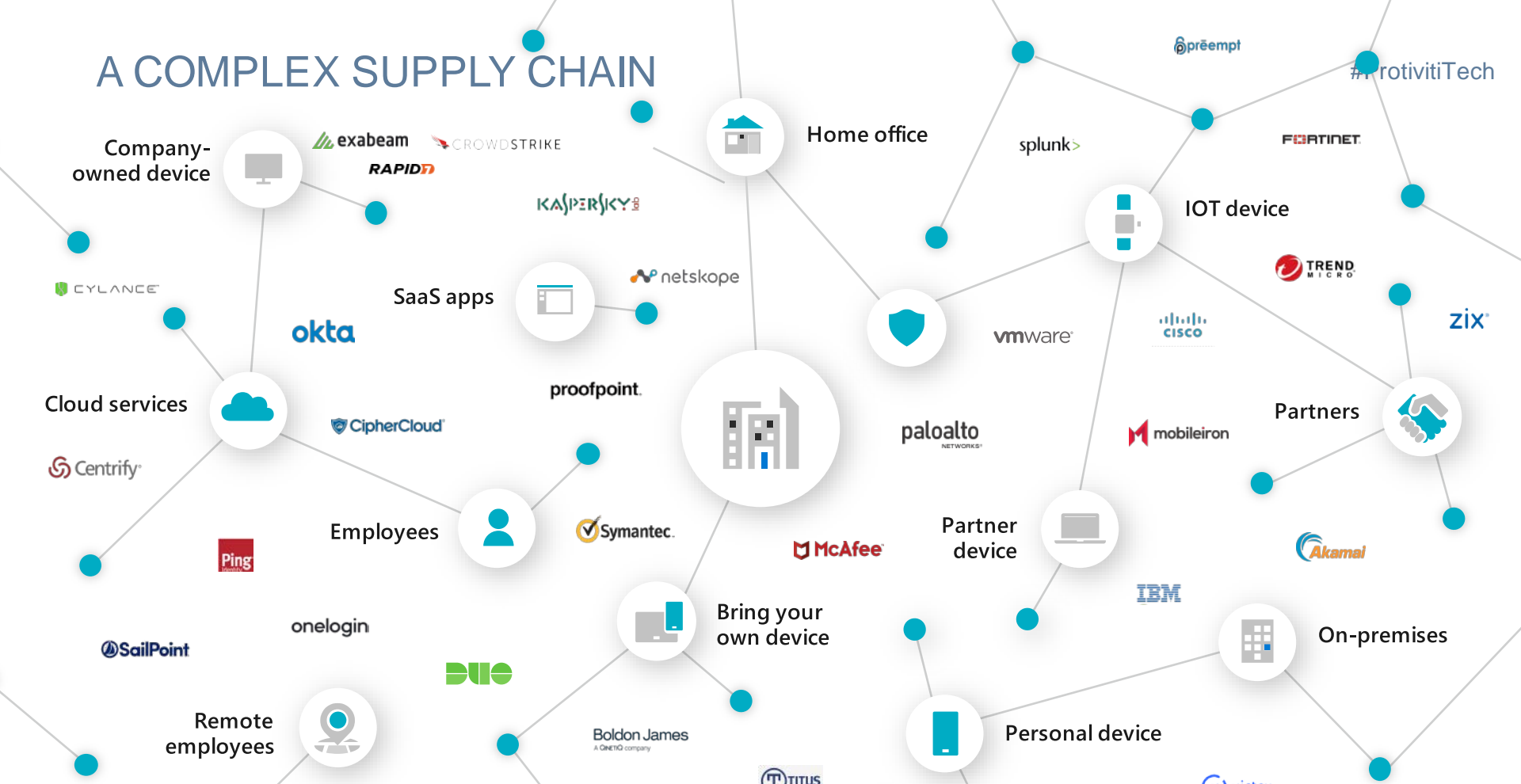


# NEW NORMAL-A COMPLEX LANDSCAPE



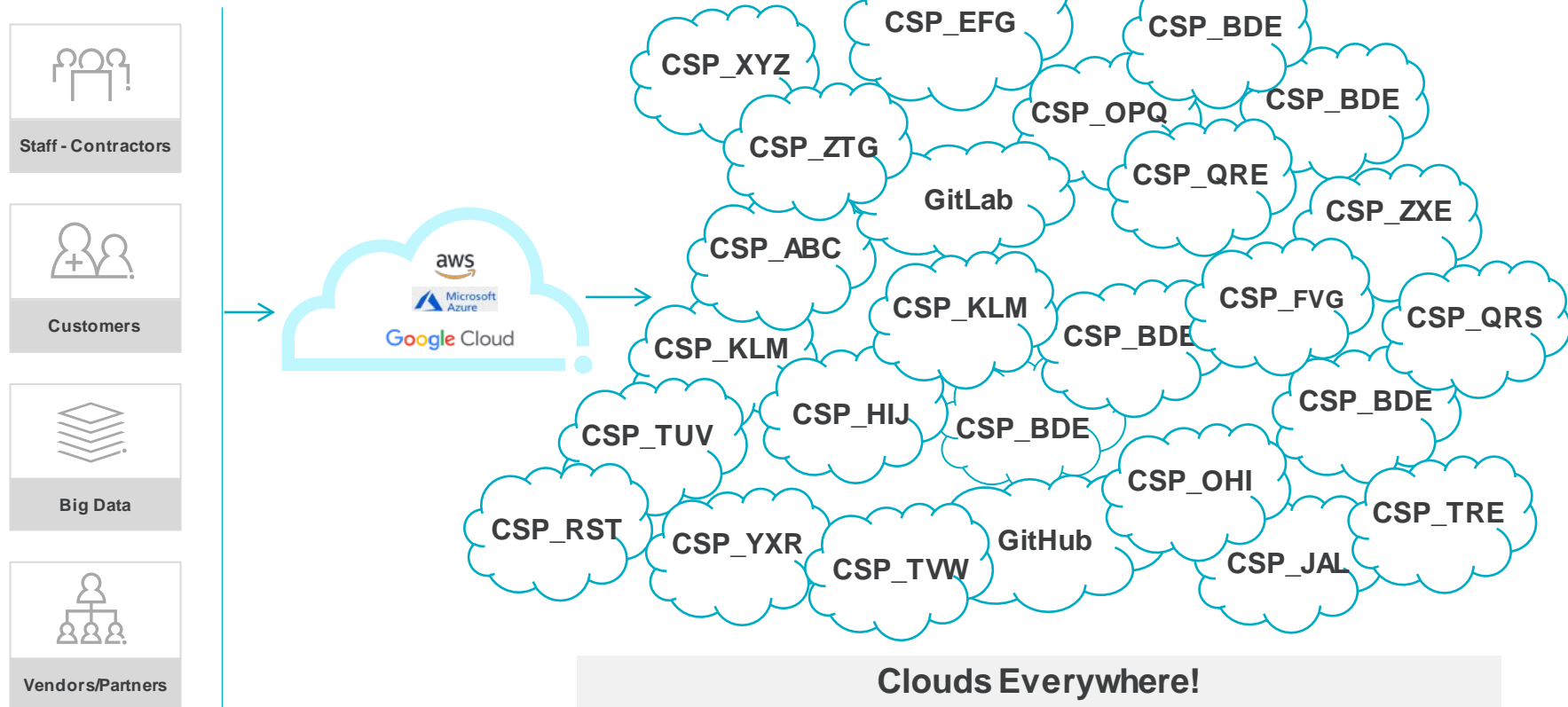
#ProtivitiTech

# A COMPLEX SUPPLY CHAIN



# WHO'S IN THE SUPPLY CHAIN?

#ProtivitiTech



# Challenges & Risks

Today's Organizations are Facing Unprecedented Challenges

# CHALLENGES & RISKS

#ProtivitiTech

Cyber threats that are increasing rapidly in volume and sophistication. Threat actors using techniques we simply didn't see but have always been there.

The cloud ecosystem makes it's harder to protect sensitive data; leading to financial, legal , reputation and safety consequences.

Shared Responsibility of the ecosystem is not well understood across the business; traditional GRC practices have not evolved to the new reality.



# CHALLENGES & RISKS

Data regulations are  
**increasing** around  
the world



Personal Information  
Protection and Electronic  
Documents Act (PIPEDA)



General Data  
Protection Regulation  
(GDPR 2016)



California Consumer  
Privacy Act (CCPA) 2018



The Privacy Protection  
Act (PPA) 2017



Federal Data  
Protection Law 2000



Personal Data  
Protection Bill 2018



Texas Privacy  
Protection Act (2019)



Personal Data Protection  
Act (PDPA 2012)



Lei Geral de Proteção  
de Dados Pessoais  
(LGPD 2019)



Personal Information  
Security Specification 2018



Australia Privacy  
Principles 2014



Personal Information  
Protection Act (PIPA) 2011



Protection of Personal  
Information Act 2013  
(POPI)



Act on Protection of  
Personal Information  
(APPI) 2017

## Identity and Access Control

Organizations struggle to provision and control access consistently across IaaS, PaaS and SaaS services due to the lack of centrally managed identities and access rights.

## Monitoring and Response

Organizations need visibility and control of access to data and services, regardless of location, and they must respond rapidly to any threat.

## Data Leakage

The cost of sensitive data leaking from cloud storage services and code repositories can be huge in terms of both reputational damage and non-compliance penalties.

## Governance

Shared Responsibility Model not well understood across the business, IT, security, risk, privacy and compliance.  
**Regulatory ambiguity**



## Skill Shortages

Cloud skills are at a premium, cloud security skills are even rarer. Traditional thinking is costly and highly problematic.

## Business Alignment

Ownership of strategy and risk is not always defined, leading to a lack of control, with little agreement on secure way of working and operational silos.

## Shadow IT

Staff bypass central IT to adopt cloud services, exposing organizations to unquantified risk. How do you manage EU GDPR compliance if you cannot identify where your personal data is stored?

TPRM needs to evolve for cloud



# GOVERNANCE PROGRAMS NEEDS TO BE UPDATED FOR CLOUD

#ProtivitiTech



- What are the Cloud Services we are prepared to Adopt?
- Who Owns and is Accountable for the Cloud Service Relationship, Services, Subscriptions or Tenants?
- Does our Cloud Adoption align with our Business Strategy?
- Do we have a Common Language when we speak of Cloud?
- How our Use of Cloud for Compliance Effectiveness?
- How does Cloud Adoption introduce new Risks into our Organization?
- Do we have Understanding and Visibility of What and Where Cloud Services are Deployed?
- What Compliance Activities are we Responsible for versus our CSP's?
- Do we Know what Cloud Controls are in Place and Are they Different from our Traditional Standards?

*“Of 1200 companies surveyed, 69% **wrongfully** believed that Data Protection, Compliance and Privacy obligations were the Responsibility of the Cloud Provider “ —Veritas 2020 Data Survey*

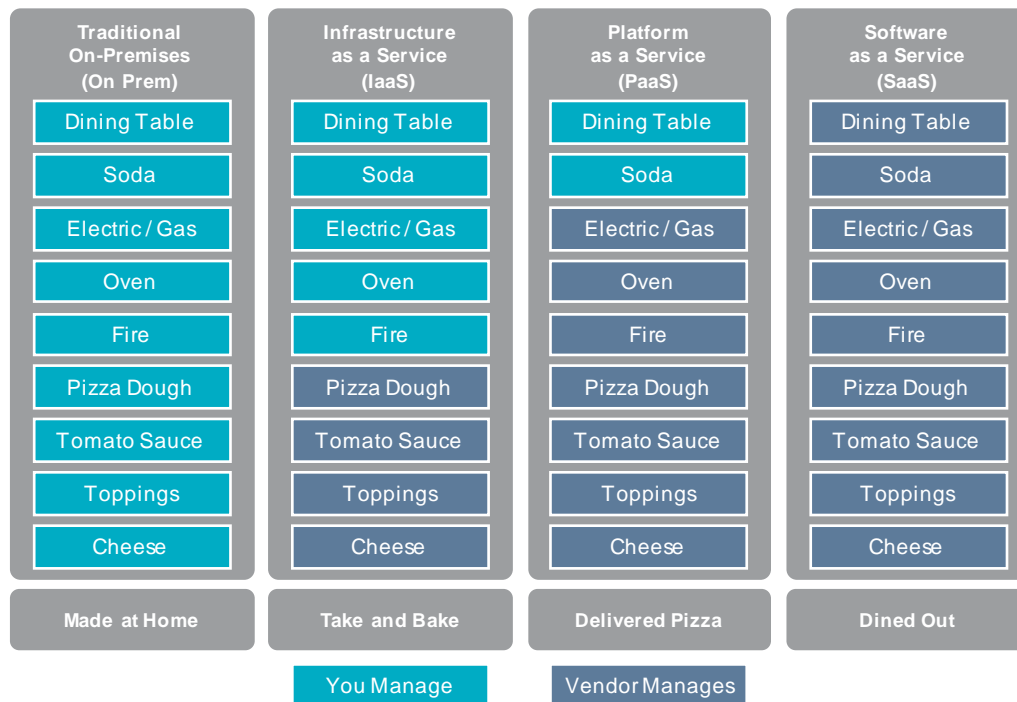
# A NEW GOVERNANCE PARADIGM – SHARED RESPONSIBILITY

#ProtivitiTech

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Network controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Host infrastructure	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Physical security	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer

Legend: Cloud Customer (Blue), Cloud Provider (Grey)

## Pizza as a Service



The **higher** the cloud stack, the **less control** you have over the environment

# WHERE IS OUR DATA?

#ProtivitiTech

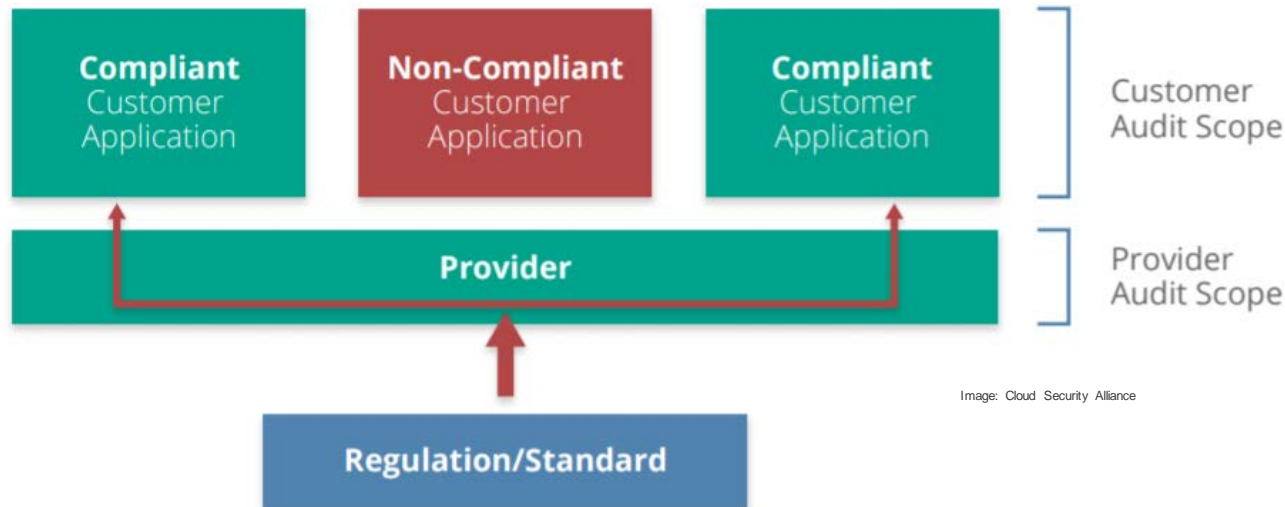
The dynamics of Hybrid Cloud deployments have changed the way Governance, Risk and Compliance Programs need to treat data lifecycle management.

Cloud Requires a New POV	
Managing Data Lifecycle	Data is Ethereal
Multi-Tenancy	Shared Governance
Data Custodian	Trust/Privacy Clarity
Data Owner	Supply Chain/BIA's Contract
Data Processor	No Collection Standards
Data Sovereignty	Data Flows not Known

Governance Considerations
Data Assets and Locations are Elastic
Your Data GRC policies do not bind Multi-Tenants or the CSP's; Weak security could leak to other tenants
Hosting a SaaS solution on an IaaS platform makes you the custodian and processor but not the owner
As the Data Owner, you are responsible for 3 <sup>rd</sup> , 4 <sup>th</sup> , 5 <sup>th</sup> party handling which includes unknown CSP Supply Chain
CSP becomes Data Processor and is not bound by your Data GRC nor adherence to a Standard
CSP's do not allow inspection of Orchestration and Abstraction layers Managed Services/Forensics

# THE CLOUD PROVIDER SUPPLY CHAIN IS MASSIVE!

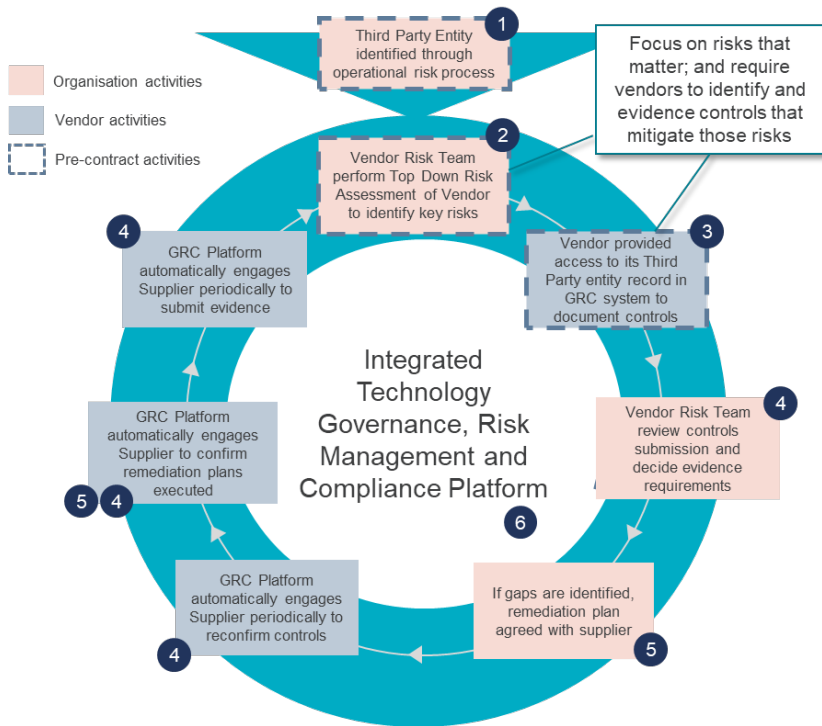
#ProtivitiTech



**Cloud Providers Infrastructure is not in scope for its customer's audits; they support it but not responsible for it**

# INTEGRATED APPROACH TO THIRD PARTY RISK

#ProtivitiTech



- 1 Scoping of vendors based on risk
- 2 Organisation focused on key specific risks that the supplier/service presents
- 3 Vendors can manage customer risk through their own process
- 4 System reminds supplier of their commitments
- 5 Process established to track/manage the closure of remediation plans
- 6 Process fully integrated with business risk process

# CHALLENGES WE SEE IN EXECUTION

#ProtivitiTech

As a result of an increase in outsourcing of business and IT services, including the acceleration of cloud adoption, the proportion of services and technology which sits outside of the boundaries of an organization has increased significantly. Vendor risk management processes have often not effectively evolved to address this change in focus



Risk management versus blanket control adherence



Pre-contractual due diligence –Does this include the Cloud Supply Chain?



Risk tracking and reporting –Who owns this for Cloud Licenses?



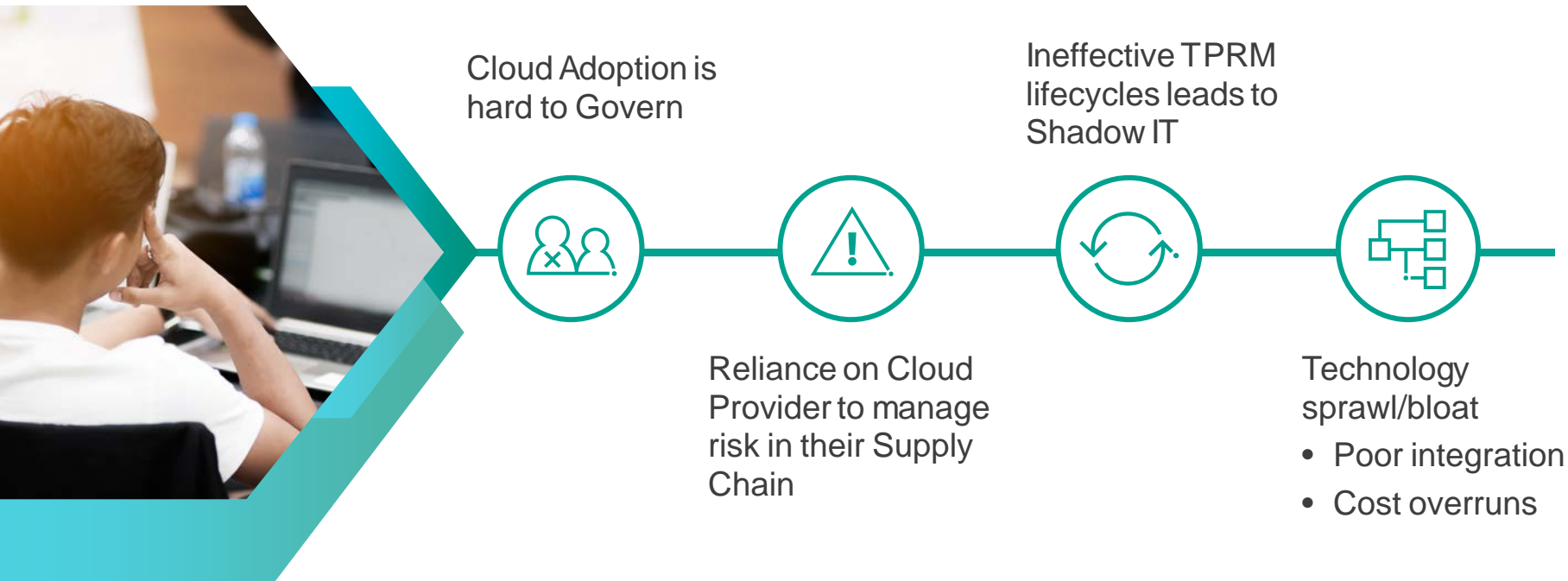
Risk acceptance not risk management



Regulatory drivers

# OUTCOMES OF TRADITIONAL APPROACHES TO TPRM

#ProtivitiTech



# Monitoring the Cloud: Case Study



# MONITORING THE CLOUD ECOSYSTEM: CASE STUDY1

#ProtivitiTech

Situation: AWS identified potentially compromised credentials and escalated to client via Email. Once client became aware, they escalated, investigated, and deleted credentials. Significant business impact ensued.



Situation: Organization relies on third-party marketing firm to provide logo for organizational Email. Marketing firm unknowingly hacked resulting in poor reputation score, which led to organizational Email to clients blocked.



Let's Talk about SolarWinds

# WHAT HAPPENED

#ProtivitiTech

SolarWinds is an American company that has provided software products to almost all Fortune 500 companies to help manage their networks, systems, and IT infrastructure.

In early 2020, hackers gained access and added malicious code into SolarWinds's software system, "Orion," which is used by 33,000 of its customers.

As many as 18,000 customers ran this software and spread the vulnerability to several major companies and federal agencies.



## Organizations Attacked



**National Nuclear  
Security  
Administration**

“

Source: [Microsoft says SolarWinds hackers downloaded some Azure, Exchange, and Intune source code \(msn.com\)](#)

“

**Companies will need to do clean-up similar to a hurricane," she added. "It is going to be expensive and extensive — companies are going to have to identify what has been breached and what, if anything, remained stable.**

– Kiersten Todt (former cybersecurity official in the Obama administration)

”

## Actions Taken



**Ongoing  
Investigations**



**Hearings**



**Remediation  
Efforts**



**Investments in  
Cybersecurity**



**Researching New  
Cybersecurity  
Methods**

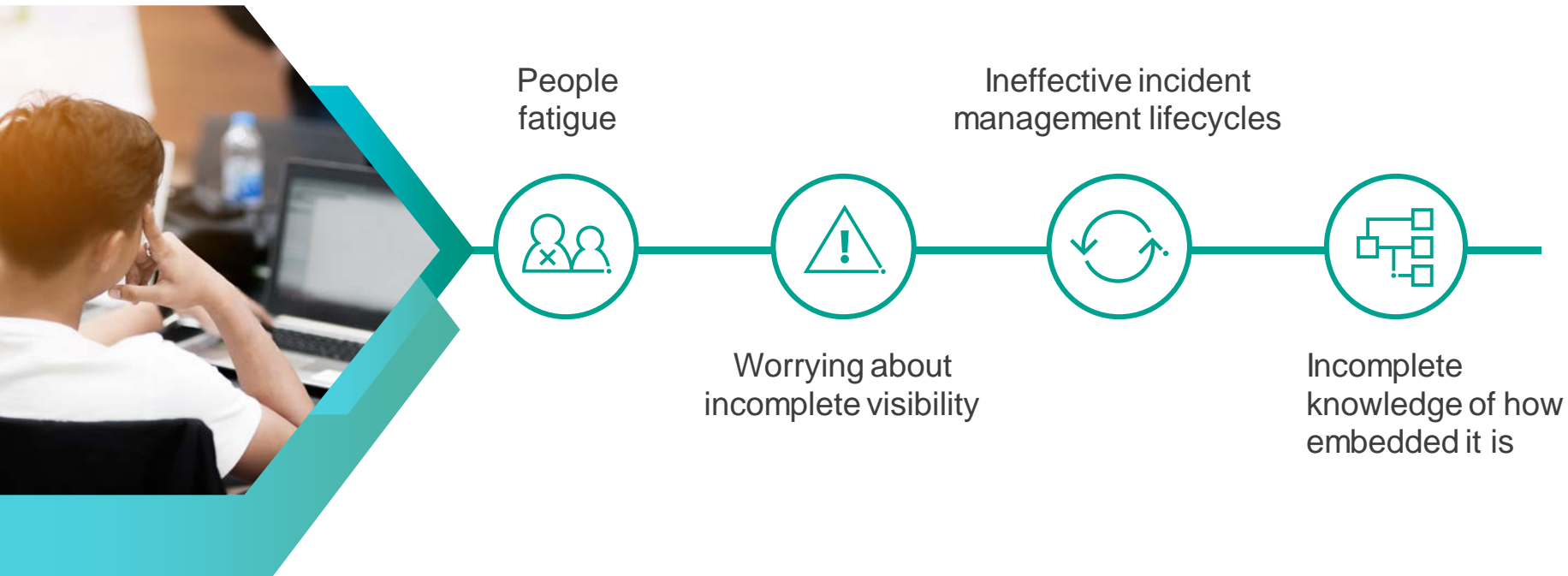
Source: [What Is the SolarWinds Hack and Why Is It a Big Deal?](https://www.businessinsider.com/solarwinds-hack-why-it-is-a-big-deal) (businessinsider.com)

Source: [SolarWinds says dealing with hack fallout cost at least \\$18 million](https://www.yahoo.com/news/solarwinds-says-dealing-with-hack-fallout-cost-at-least-18-million-123456789.html) (yahoo.com)

Source: [Massive SolarWinds hack has big businesses on high alert](https://www.cnn.com/2020/12/23/tech/solarwinds-hack/index.html) - CNN

# OUTCOMES OF NEW SUPPLY CHAIN ATTACKS

#ProtivitiTech



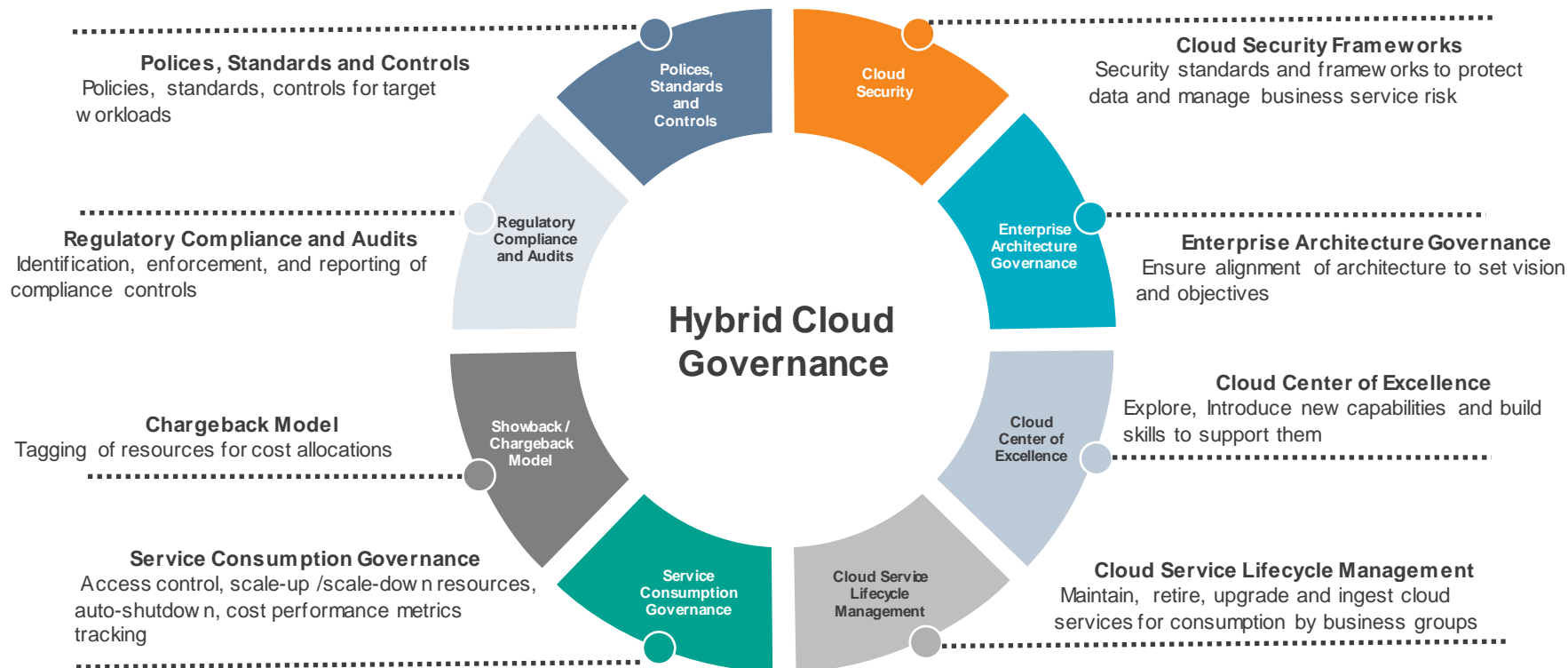
# Update GRC Processes

Include Cloud Supply Chain in GRC






# START WITH CLOUD GOVERNANCE

#ProtivitiTech



# ADAPTED PEOPLE, PROCESS & TECHNOLOGIES TO ADDRESS RISK

#ProtivitiTech

	<b>Shared Responsibility Model and Knowledge</b>	<ul style="list-style-type: none"><li>• Define how Shared Responsibility Model impacts structure and operational models for your organization<ul style="list-style-type: none"><li>– Formalize and Communicate</li><li>– Update Governance policies, RACI's</li><li>– Measure and Monitor</li></ul></li><li>• Train employees</li><li>• Provide incentives and paths to certifications where relevant</li></ul>
	<b>Frameworks and Benchmarks</b>	<ul style="list-style-type: none"><li>• Use established frameworks to holistically address environment<ul style="list-style-type: none"><li>– Example: CSA Cloud Security Guidance, STAR and AZURE Well-Architected Framework</li></ul></li><li>• Compliance and Regulatory concerns</li><li>• Align CIS Benchmarks, CCM and others to approved standards and governance policies</li></ul>
	<b>Technical Capabilities and Tools</b>	<ul style="list-style-type: none"><li>• Implement technical capabilities to enable real-time understanding of what is going on in the environment</li><li>• Use tools to reduce or remove human error, which increases speed of response and allows security controls to be automated</li><li>• Key considerations:<ul style="list-style-type: none"><li>– Open Source vs. Enterprise</li><li>– Platform Agnostic vs. Platform Specific vs. Cloud Native</li></ul></li></ul>

# TOOLS TO ADDRESS TPRM GOVERNANCE – CSA CLOUD SECURITY GUIDANCE & ATTESTATIONS

#ProtivitiTech



## Frameworks and Benchmarks

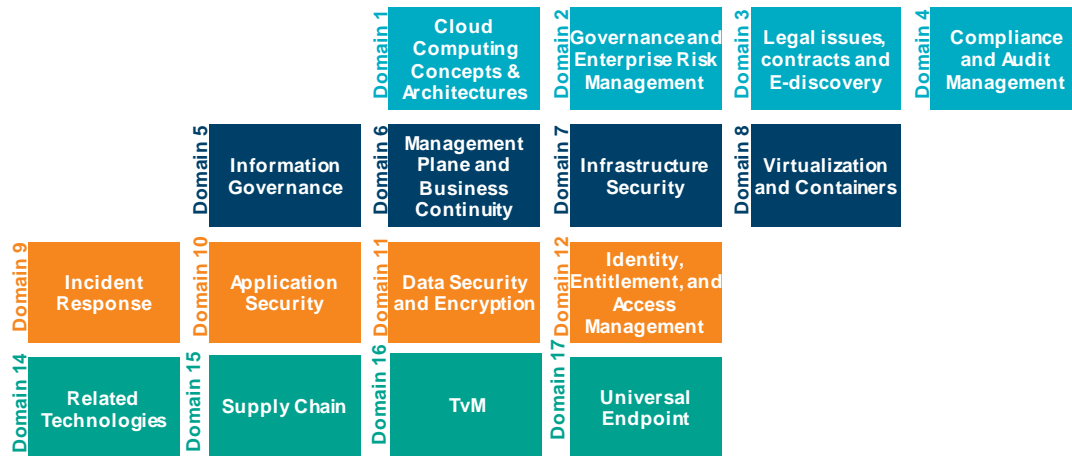
- Use established frameworks to holistically address environment
  - CSA Cloud Security Guidance and **CSP Well-Architected Frameworks**
- Compliance and Regulatory concerns
  - Example: CSA CCM
  - CIS, Azure Security Center, Azure/AWS/GCP Compliance FAQ
- Compliance and Regulatory concerns
  - Example: CSA CCM
  - CIS, Azure Security Center, Azure/AWS/GCP Compliance FAQ's
- Join ISAC's and Peer Sharing Groups

## CSA STAR Registry

- CSA STAR (Security, Trust and Assurance Registry)
- Public Registry of Cloud Provider self assessments
- Based on Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
  - Provider may elect to provide assessments from third parties.
- Available October 2011



CSA Domains establish a stable, secure baseline for cloud operations and **should become a part of your Standards library. Cloud Polices can be built from Domains** which emphasize security, stability, and privacy in a multi-tenant environment.



# HAVE CONTINGENCY PLANS FOR DEPRECIATED/OBSOLETE SERVICES



## Start using Conditional Access in Azure Active Directory by 30 January 2021

Sign Up to Be Notified

Please fill out the form below with an email address to be notified of any changes to the list on the [AWS Sub-processors webpage](#). If a change occurs, you will receive an email to the email address provided below.

\* Business Email Address:

Submit

***...this email because you use the preview of configurable token lifetimes in Azure Active Directory (Azure AD).***

Conditional Access in Azure AD provides granular controls for sign-in frequency, and the preview of configurable token lifetimes for refresh and session tokens on **30**

you need to use Conditional Access to manage sign-in frequency. Conditional Access is a new feature of Azure AD—read complete [pricing details](#).

### Recommended action

To continue managing sign-in frequency, [start using Conditional Access](#) in Azure AD by 30 January 2021.

# ADD CSP SUPPLY CHAIN MONITORING TO YOUR GRC DASHBOARDS



## Microsoft Top 100 Production Suppliers

Based on FY20 spend for commercially available hardware products

AAC ACOUSTIC TECHNOLOGIES  
AAVID THERMALLOY LLC  
ADVANCED MICRO DEVICES, INC.  
ALLEGRO MICROSYSTEMS, LLC  
ALPS ALPINE CO. LTD  
ASIA VITAL COMPONENTS CO., LTD  
AVARY HOLDING (SHENZHEN) CO., LTD.  
AVX CORPORATION  
BEST EVER INDUSTRIES LIMITED  
CAM PLAS (H.K.) LTD.  
CASETEK COMPUTER (SUZHOU) CO. LTD.

MONOLITHIC POWER SYSTEMS, INC  
MULTI-FINELINE ELECTRONIX INC  
MURATA MANUFACTURING CO., LTD  
NEXPERIA USA, INC.  
NIDEC SEIMITSU  
NINGBO SANHUAN  
NIPPON MEKTRON  
NORDIC SEMICONDUCTOR  
NVIDIA SINGAPORE  
NXP SEMICONDUCTOR  
ON SEMICONDUCTOR

The screenshot shows the Google Cloud Platform Subprocessors page. The header includes the Google Cloud logo and navigation links: Why Google, Solutions, Products, Pricing, Getting Started. There are also links for Docs, Support, Language, and Sign in. A 'Contact Us' link and a 'Get started for free' button are visible. The main heading is 'Google Cloud Platform Subprocessors'. Below it, there is a section titled 'Third-Party Subprocessors' with a blue arrow icon. The text explains that Google and its affiliates engage third-party entities to perform limited activities in connection with Google Cloud Platform Services. It mentions that the table shows what activity each entity performs and indicates if an entity is only relevant to a specific Service or Region. More information about each activity is provided directly below. This explains the limited processing of Customer Data the entity is authorized to perform. A 'Data Labeling' section mentions that human labelers apply labels to datasets submitted by Customer based on instructions provided by Customer. It refers to the AI Platform Data Labeling Service page, Document AI Service page, and Human-in-the-Loop AI Service page for more information.

The screenshot shows the AWS Sub-processors page. The header includes the AWS logo and navigation links: Products, Solutions, Pricing, Documentation, Learn, Partner Network. Below the header, there is a section titled 'AWS Cloud Security' with sub-links: Overview, Security Services, Compliance Offerings, and Data Protection. The main heading is 'AWS Sub-processors'.

# MONITOR CSA STAR REGISTRY-EXAMPLE: AZURE ATTESTATIONS

The first screenshot shows the CSA STAR Registry search results for 'microsoft'. It includes a search bar with 'microsoft' entered, a filter section for 'View Only' (CSA Trusted Cloud Providers) and 'By STAR Level' (All (default), Level One: Self Assessment), and a list of providers including Microsoft and VMware. The second screenshot shows the detailed profile for 'Microsoft Azure', which is a STAR Level One provider. It lists submissions for CAIQ, CCM, Attestation, and Certification. The third screenshot shows the 'Level 2: Third-Party Audit' section for Microsoft Azure, detailing STAR Attestation (SOC 2) and STAR Certification (ISO/IEC 27001:2013) with download links.

cloudsecurityalliance.org/star/registry/

Find a provider with the right level of security and data privacy for your organization.

Submit to the Registry →  
Ask a provider to submit to the registry

Search: microsoft

Filter Your Results ▲

Reset all filters

View Only

☒ CSA Trusted Cloud Providers

By STAR Level

☒ All (default)

☒ Level One: Self Assessment

☒ CAIQ

☒ CCM

Microsoft

Microsoft Azure is a cloud computing platform for building, deploying and managing applications through a global network of Microsoft and third-party managed da...

Listed Since: 12/02/2011

STAR LEVEL ONE

Submissions: CAIQ 1, CCM 1

STAR LEVEL TWO

Submissions: Attestation 1, Certification 1

Trusted Cloud Provider CSA

Microsoft Azure

Azure is a multi-tenant hyperscale cloud platform that is available or announced to customers in 60+ regions worldwide. Most Azure services enable customers to s...

Listed Since: 04/05/2016

STAR LEVEL ONE

Submissions: CAIQ 1

STAR LEVEL TWO

Submissions: Attestation 1, Certification 1

Trusted Cloud Provider CSA

cloudsecurityalliance.org/star/registry/services/microsoft-azure

Level 2: Third-Party Audit

Organizations looking for a third-party audit can choose from one or more of the security and privacy audits and certifications.

STAR Attestation: SOC 2

A technology-neutral certification leveraging the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix (CCM).

STAR Attestation 1

Download Attestation

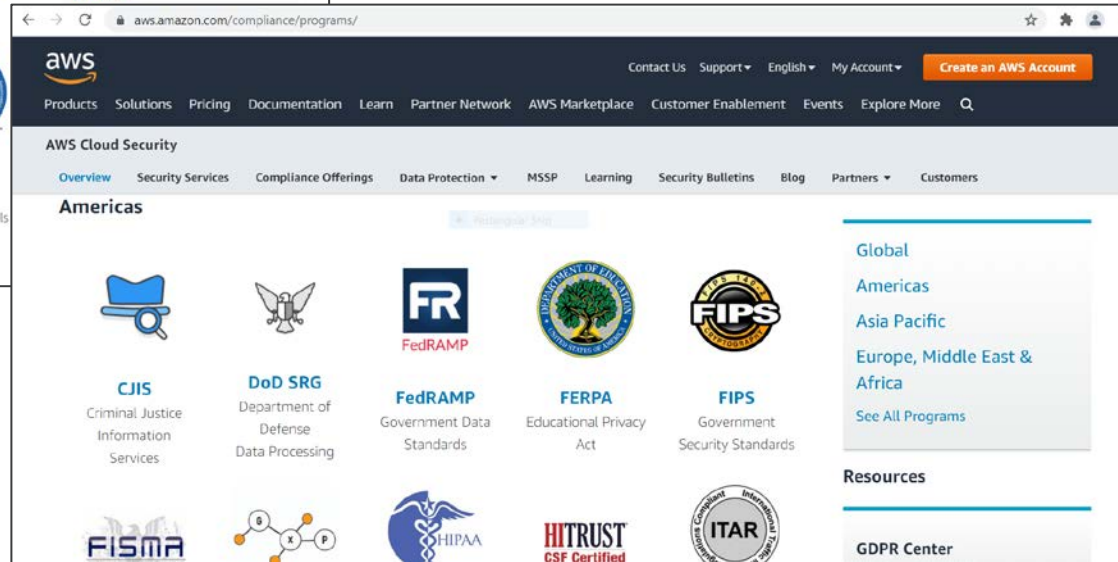
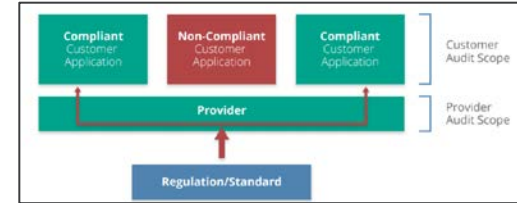
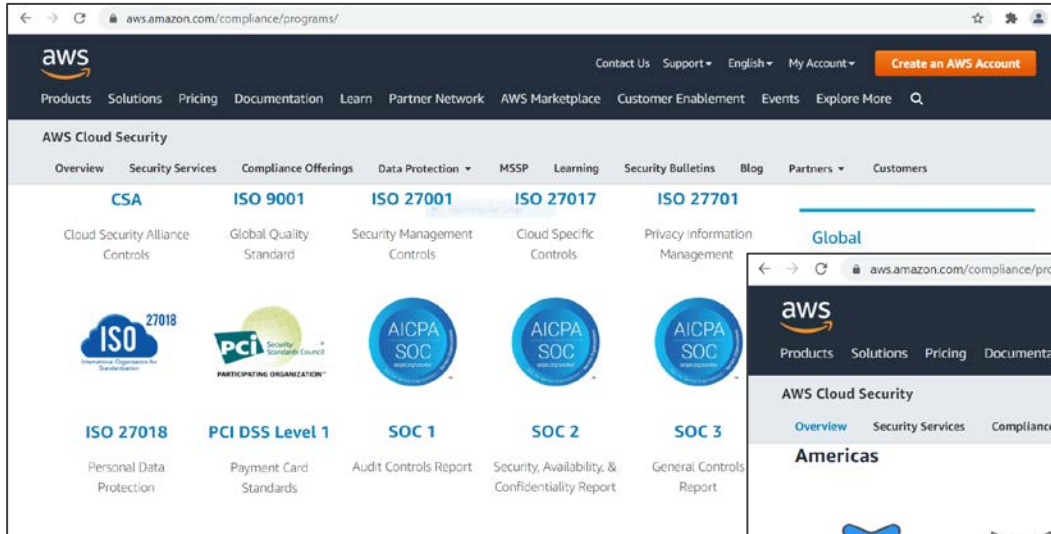
STAR Certification: ISO/IEC 27001:2013

A technology-neutral certification leveraging the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix (CCM).

STAR Certification 1

Download Certification Supporting Asset

# MONITOR FOR CERTIFICATIONS AGAINST LEADING STANDARDS – EXAMPLE: AWS



# FINAL THOUGHTS



Consider the cloud ecosystem as part of the organization



Evolve the TPRM program



Include cloud in everything you do for GRC



Stay vigilant in monitoring for updates from your cloud providers



Q&A

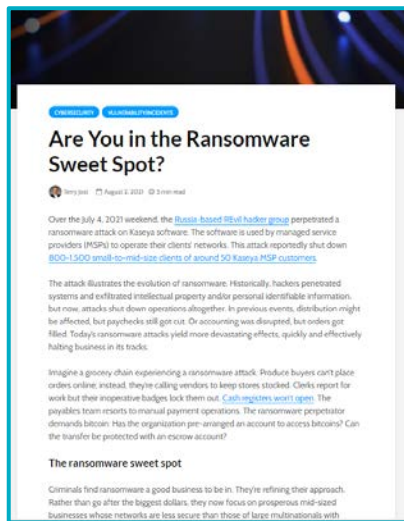
# RECOMMENDED RESOURCES

#ProtivitiTech

## Recover: The NIST Cybersecurity Framework's Outlier



## Are You in the Ransomware Sweet Spot?



## Key Strategies to Mitigate Ransomware Impact



## Ransomware Crisis: 11 Actions to Secure Critical Infrastructure



Looking for more? Check out our Tech Insights Blog

# CONNECT WITH THE SPEAKERS

#ProtivitiTech

Reach out to the speakers and learn more about their background



## John Stevenson

Protiviti

Managing Director Security & Privacy – Cloud Security

[john.stevenson@protiviti.com](mailto:john.stevenson@protiviti.com)

<https://www.linkedin.com/in/john-stevenson-8790077/>



## Joe Burkard

Protiviti

Director Security & Privacy – Cloud Security

[joseph.burkard@protiviti.com](mailto:joseph.burkard@protiviti.com)

<https://www.linkedin.com/in/josephburkard/>



## Siobhan Moran

Protiviti

Security & Privacy – Cloud Security

[siobhan.moran@protiviti.com](mailto:siobhan.moran@protiviti.com)

<https://www.linkedin.com/in/siobhanmoransecurty6942203/>



*Face the Future with Confidence*