Security of and in the cloud

Context, assurance, controls

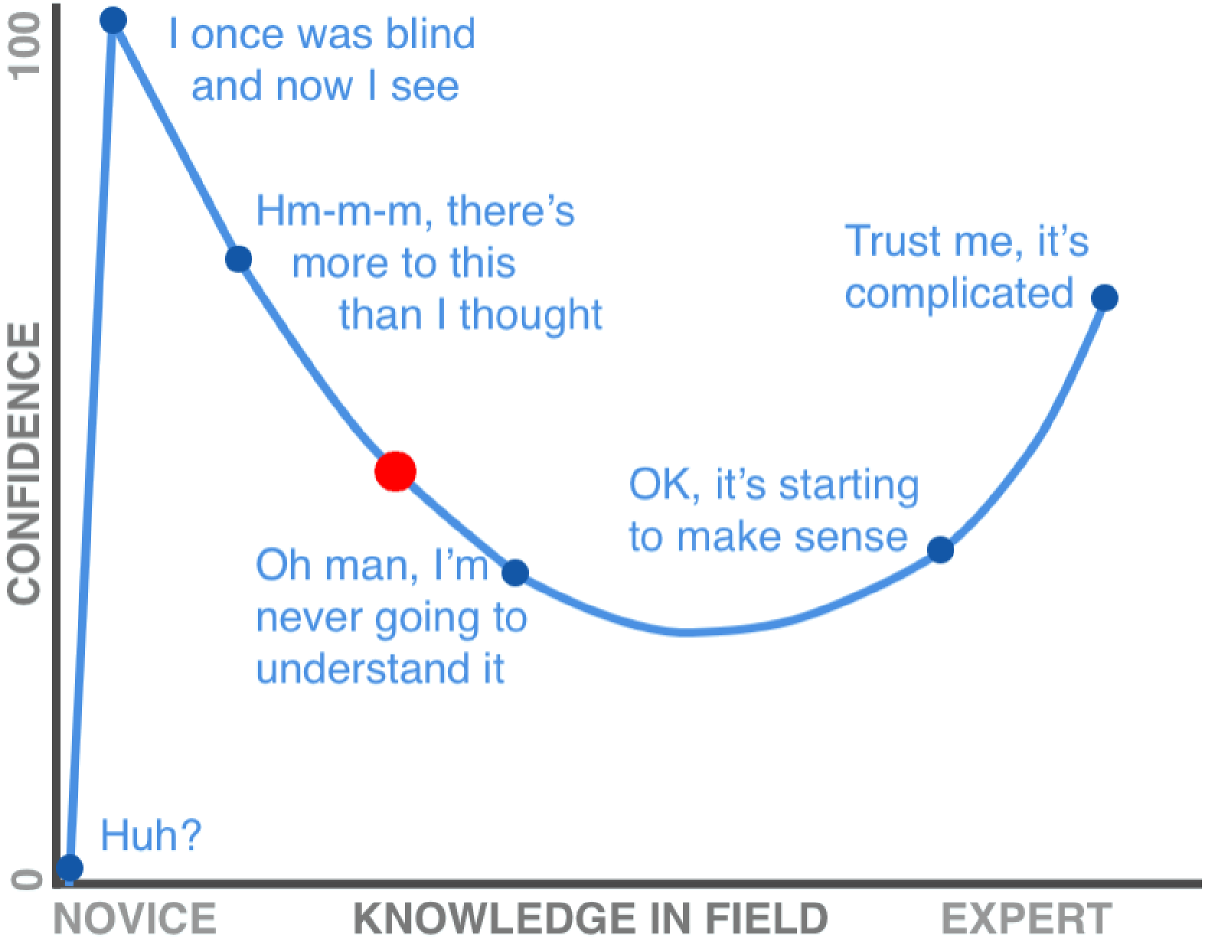
Martin Vliem CISSP, CISA, CCSP
National Security Officer

martin.vliem@microsoft.com
https://www.linkedin.com/in/mvliem

Microsoft

Questions

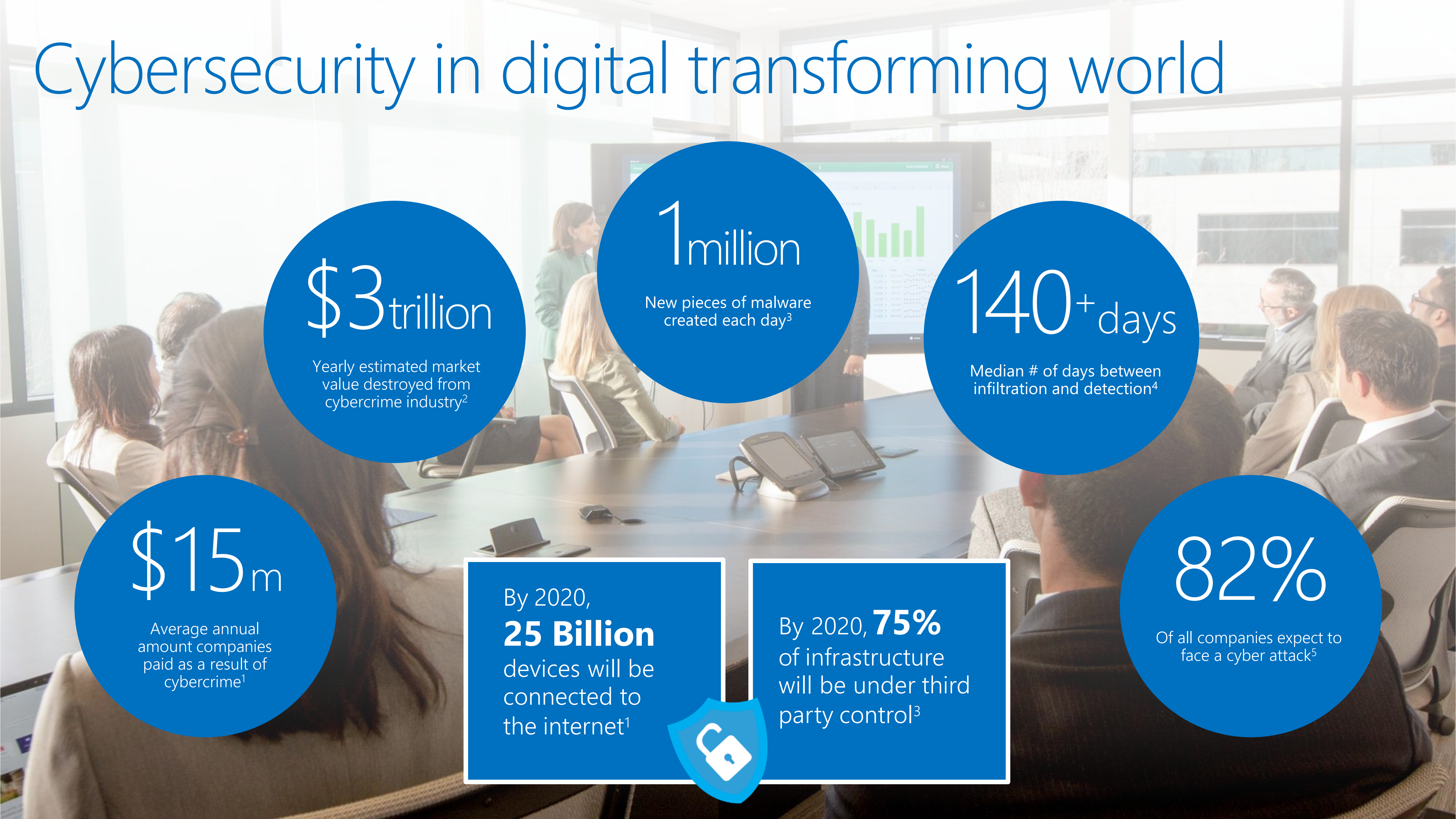
but beware the Dunning-Kruger effect



Digital Transformation

Supported through technology & cloud

Cybersecurity in digital transforming world



$3 trillion

Yearly estimated market value destroyed from cybercrime industry[2]

1 million

New pieces of malware created each day[3]

140+ days

Median # of days between infiltration and detection[4]

$15m

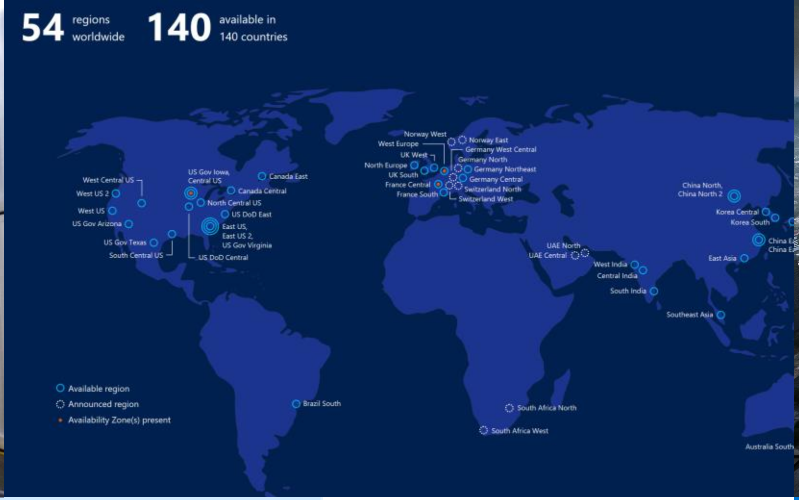
Average annual amount companies paid as a result of cybercrime[1]

By 2020, **25 Billion** devices will be connected to the internet[1]

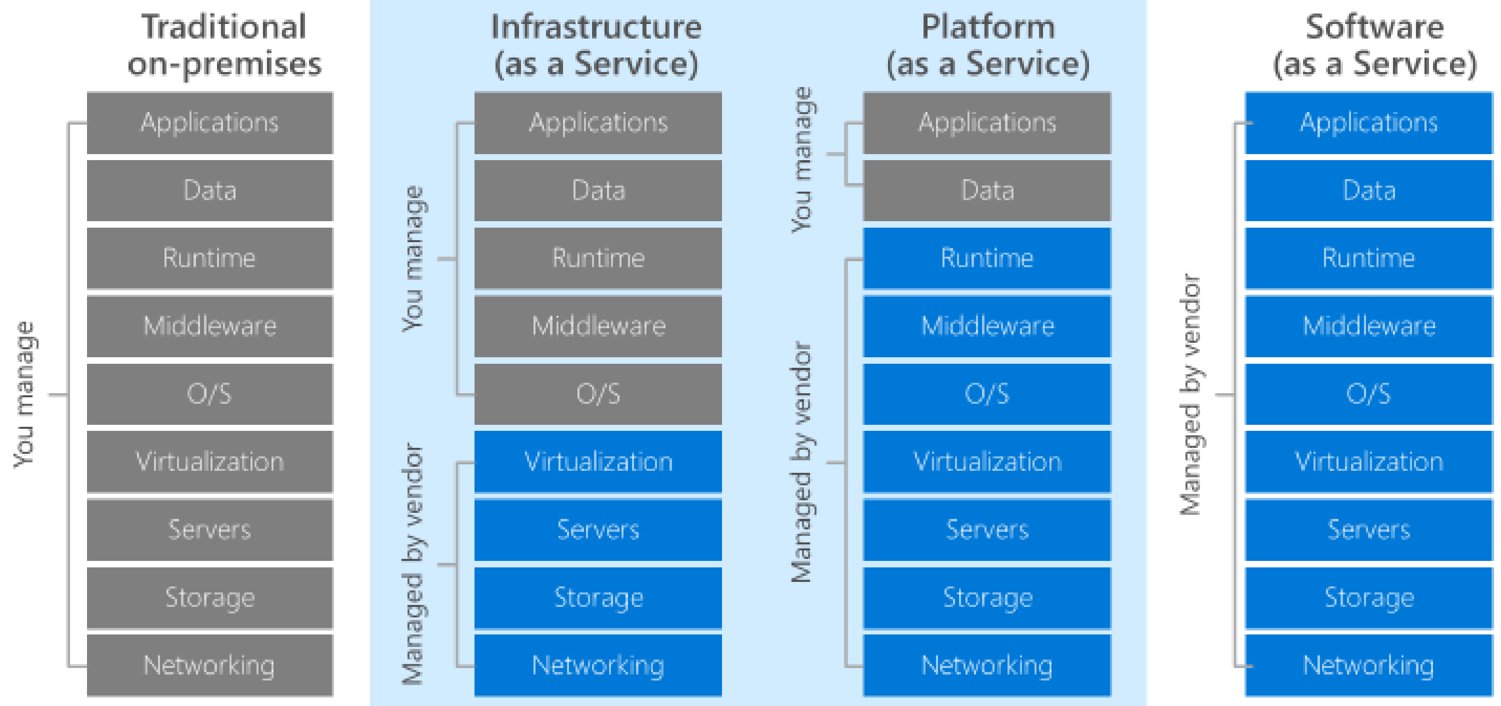
By 2020, **75%** of infrastructure will be under third party control[3]

82%

Of all companies expect to face a cyber attack[5]



Cloud service models



Traditional on-premises

You manage

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Infrastructure (as a Service)

You manage

- Applications
- Data
- Runtime
- Middleware
- O/S

Managed by vendor

- Virtualization
- Servers
- Storage
- Networking

Platform (as a Service)

You manage

- Applications
- Data

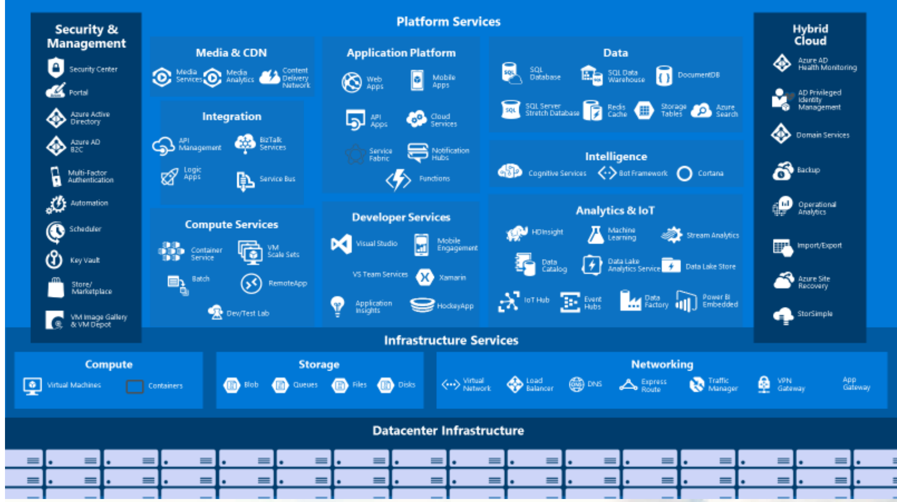
Managed by vendor

- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Software (as a Service)

Managed by vendor

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking



Security & Management

Security Center
Portal
Azure Active Directory
Azure AD B2C
Multi-Factor Authentication
Automation
Scheduler
Key Vault
Store/ Marketplace
VM Image Gallery & VM Depot

Platform Services

Media & CDN

Media Services
Media Analytics
Content Delivery Network

Integration

API Management
BizTalk Services
Logic Apps
Service Bus

Compute Services

Container Service
VM Scale Sets
Batch
RemoteApp
Dev/Test Lab

Application Platform

Web Apps
Mobile Apps
API Apps
Cloud Services
Service Fabric
Notification Hubs
Functions

Developer Services

Visual Studio
Mobile Engagement
VS Team Services
Xamarin
Application Insights
HockeyApp

Data

SQL Database
SQL Data Warehouse
DocumentDB
SQL Server Stretch Database
Redis Cache
Storage Tables
Azure Search

Intelligence

Cognitive Services
Bot Framework
Cortana

Analytics & IoT

HDInsight
Machine Learning
Stream Analytics
Data Catalog
Data Lake Analytics Service
Data Lake Store
IoT Hub
Event Hubs
Data Factory
Power BI Embedded

Hybrid Cloud

Azure AD Health Monitoring
AD Privileged Identity Management
Domain Services
Backup
Operational Analytics
Import/Export
Azure Site Recovery
StorSimple

Infrastructure Services

Compute

Virtual Machines
Containers

Storage

Blob
Queues
Files
Disks

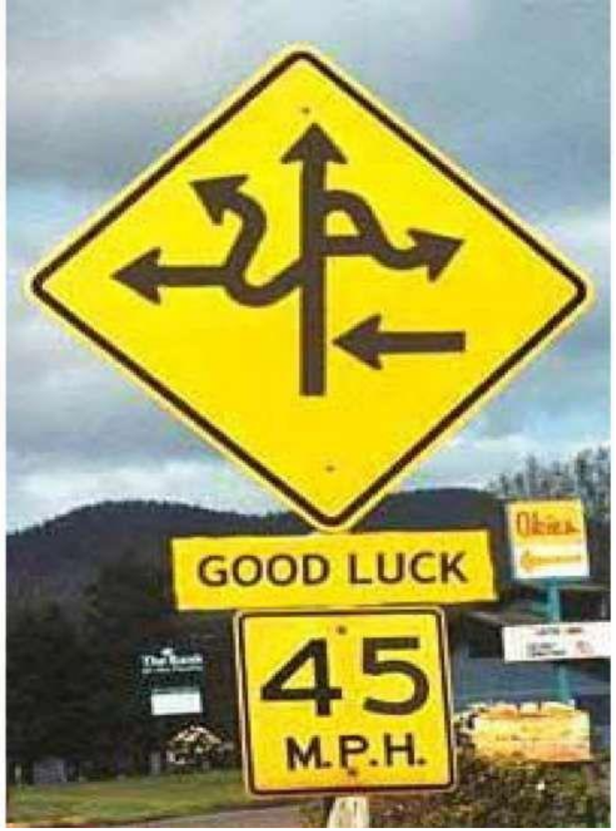
Networking

Virtual Network
Load Balancer
DNS
Express Route
Traffic Manager
VPN Gateway
App Gateway

Datacenter Infrastructure

Fear is a poor advisor

Dutch expression.



A balancing act

Opportunity and concerns

A risk based approach

Agility

Cost

Transformation

Modernization

Privacy & control

Security

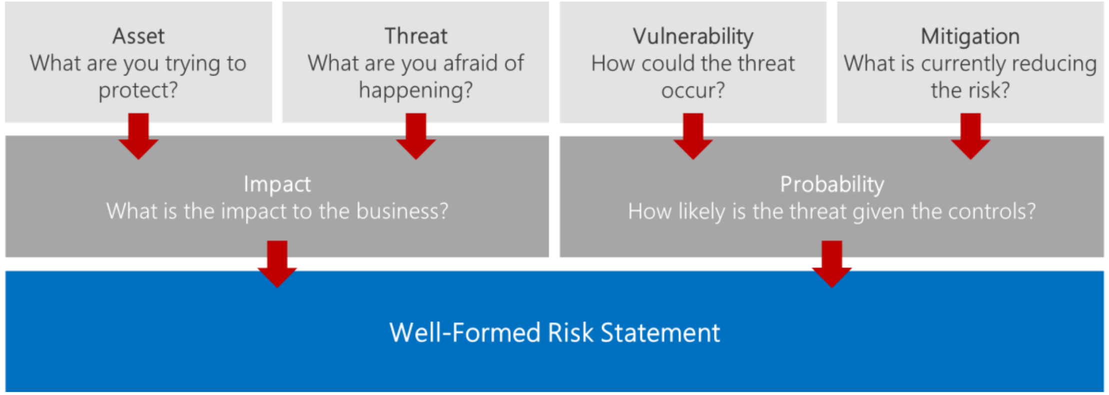
Availability

Compliance

Transparency

Information security & risk management guidelines

- ISO19086 Cloud Due Diligence
- Frameworks & standards & baselines (ISO 27002, NIST 800-53r4, CSA CCM)
- Risk templates (ISO27001, NIST 800-37, NIST CSF/RMF, ENISA)
- GDPR certifications & CoC's, EUCOC & CISPE?
- Data Processing Impact Analysis templates



Asset
What are you trying to protect?

Threat
What are you afraid of happening?

Vulnerability
How could the threat occur?

Mitigation
What is currently reducing the risk?

Impact
What is the impact to the business?

Probability
How likely is the threat given the controls?

Well-Formed Risk Statement

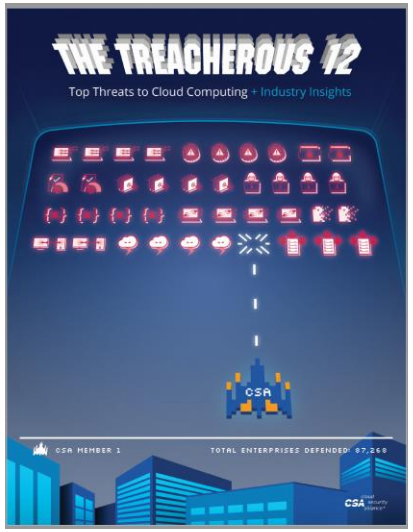
Insights into threats

Cloud Security Alliance, ENISA, threat intelligence (reports), …

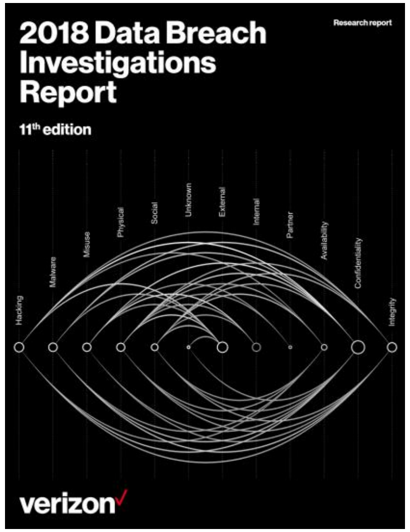
CSA Treacherous 12

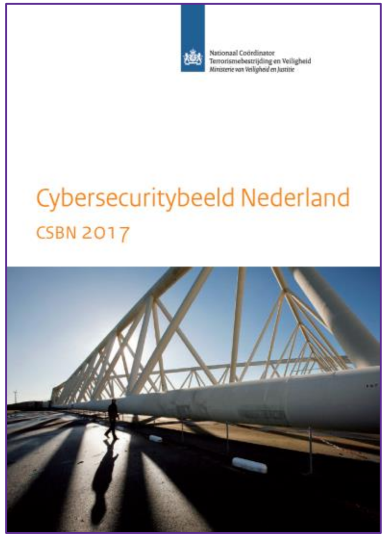
1. Data Breaches
2. Weak Identity, Credential and Access Mgmt
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

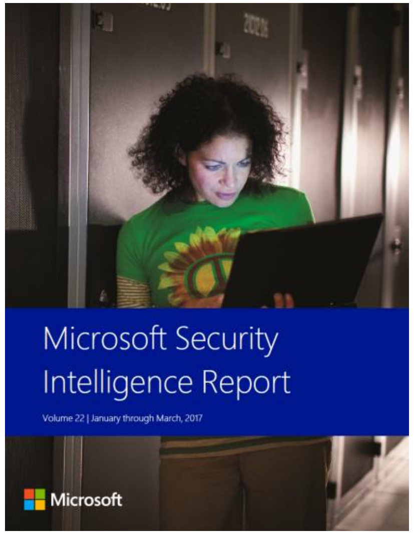
https://cloudsecurityalliance.org/download/top-threats-cloud-computing-plus-industry-insights/
https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
https://www.microsoft.com/en-us/security/Intelligence-report
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2017/1/CSBN2017.pdf


THE TREACHEROUS 12
Top Threats to Cloud Computing + Industry Insights

Cloud Computing
Benefits, risks and recommendations for information security
November 09
enisa

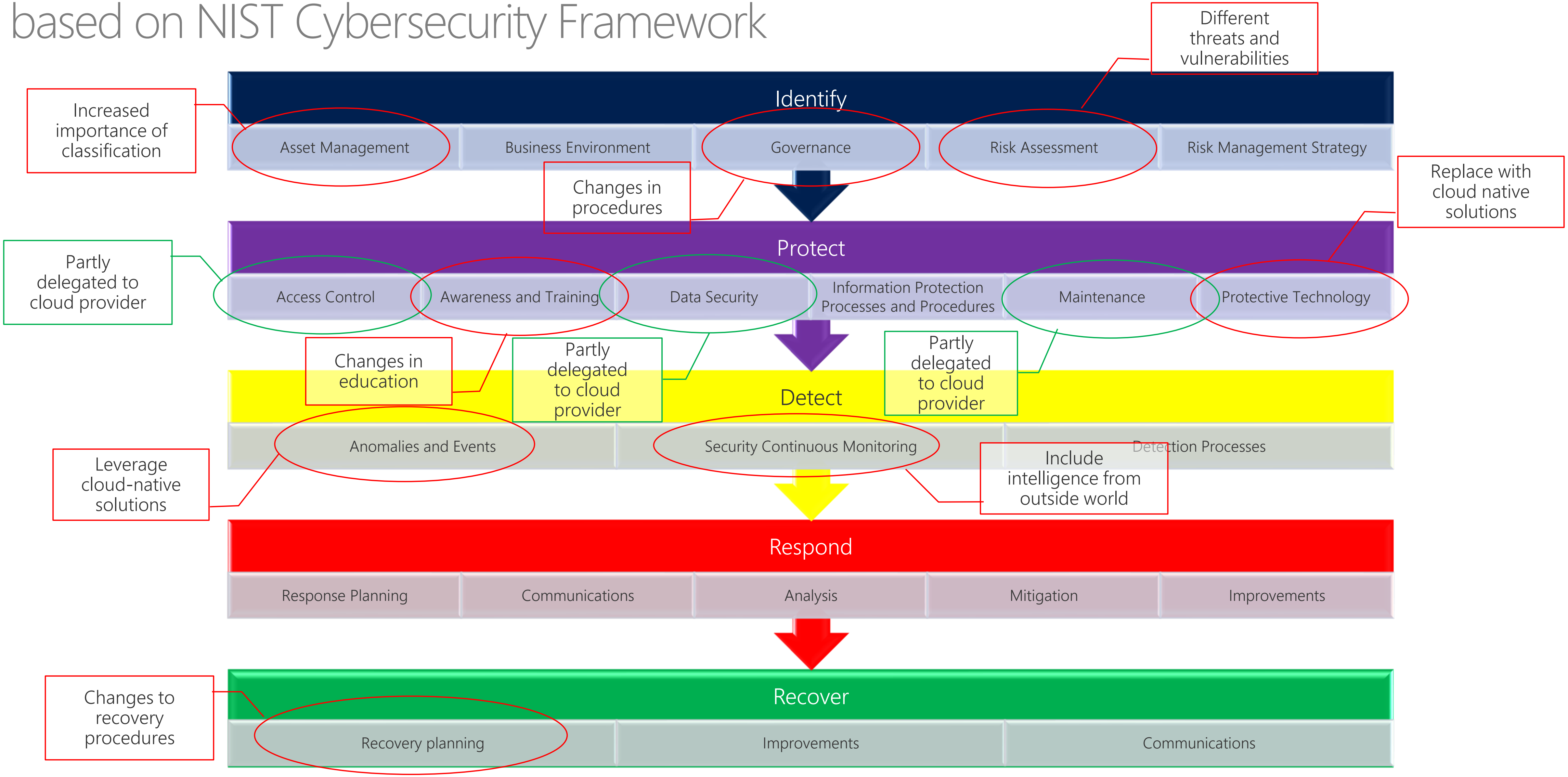

2018 Data Breach Investigations Report
11th edition
Research report
verizon


Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie
Cybersecuritybeeld Nederland
CSBN 2017


Microsoft Security Intelligence Report
Volume 22 | January through March, 2017
Microsoft

Changes in addressing risk

based on NIST Cybersecurity Framework



Identify

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management Strategy

Increased importance of classification

Changes in procedures

Different threats and vulnerabilities

Replace with cloud native solutions

Protect

Access Control

Awareness and Training

Data Security

Information Protection Processes and Procedures

Maintenance

Protective Technology

Partly delegated to cloud provider

Changes in education

Partly delegated to cloud provider

Partly delegated to cloud provider

Detect

Anomalies and Events

Security Continuous Monitoring

Detection Processes

Leverage cloud-native solutions

Include intelligence from outside world

Respond

Response Planning

Communications

Analysis

Mitigation

Improvements

Recover

Recovery planning

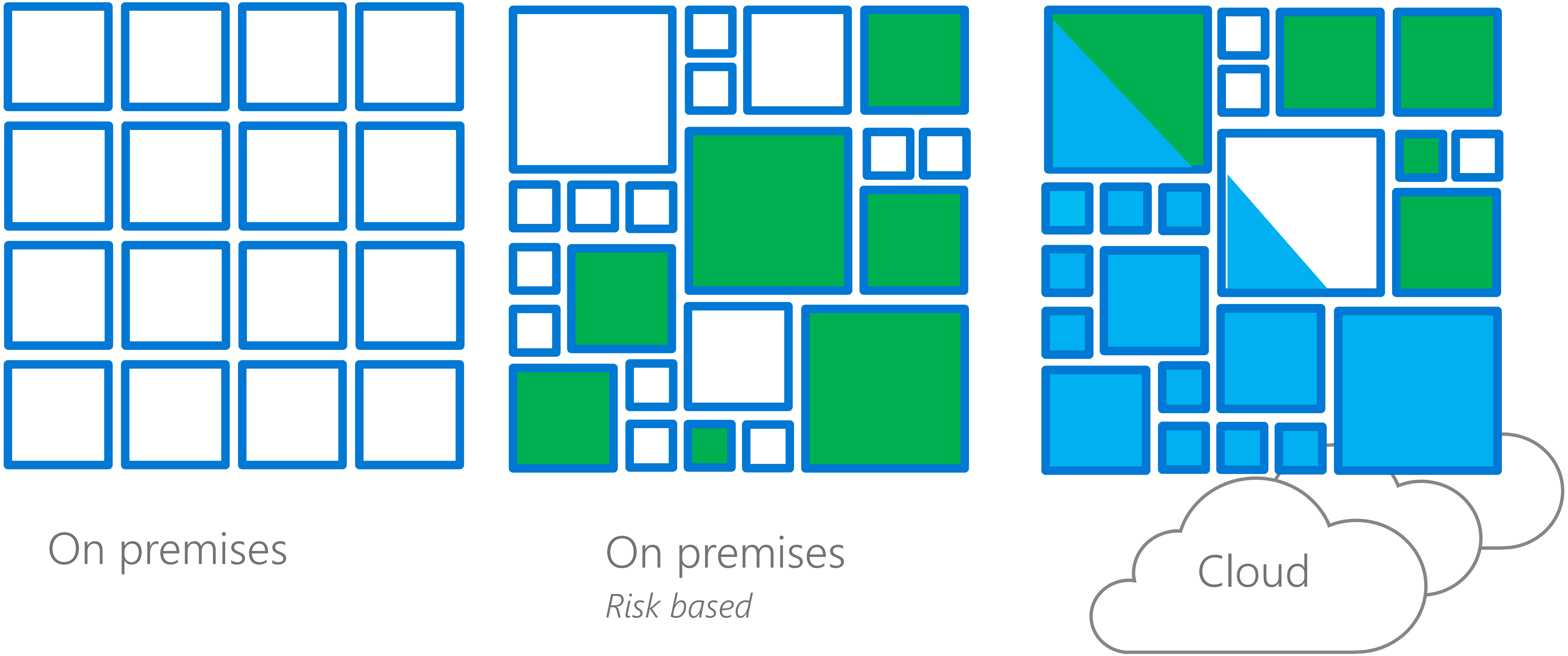
Improvements

Communications

Changes to recovery procedures

Cloud enabled security

Risk management and computing models



On premises

On premises
Risk based

Cloud

A partnership…

Doveryai, no proveryai

Your responsibility for security is based on the type of cloud service. The chart summarizes the balance of responsibility for both Microsoft and the customer.

⬜ Customer

▨ Customer and Microsoft

■ Microsoft

Responsibility	SaaS	PaaS	IaaS	On-Prem
Data governance and rights management	⬜	⬜	⬜	⬜
Client endpoints	⬜	⬜	⬜	⬜
Account and Access management	⬜	⬜	⬜	⬜
Identity and directory infrastructure	▨	▨	⬜	⬜
Application	■	▨	⬜	⬜
Network controls	■	▨	⬜	⬜
Operating system	■	▨	⬜	⬜
Physical hosts	■	■	■	⬜
Physical network	■	■	■	⬜
Physical datacenter	■	■	■	⬜

Cloud service provider, Microsoft operates

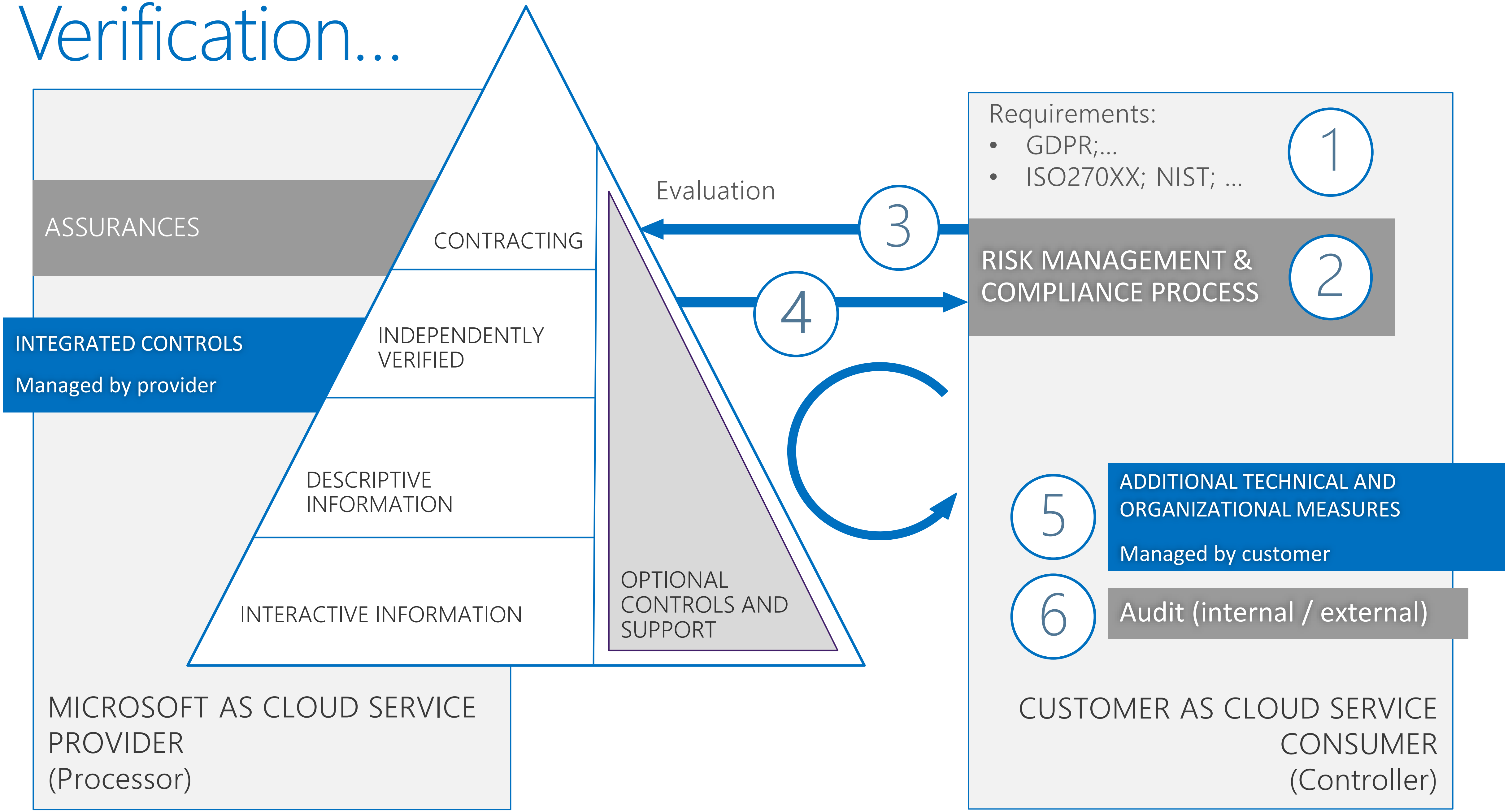
Customer, Microsoft & Partner helps

Source available here: Microsoft Cloud Security for Legal and Compliance Professional

Trust = *“hope with assurance”*

Van Dale (Dutch dictionary)

Verification…

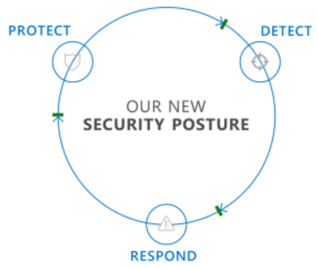


Cloud service provider assurance

Microsoft managed controls

Security

Cloud Service Provider controls



- ✓ Secure hypervisor, code signing, strong isolation, VM Shielding, Threat protection/AV, intelligence based threat protection, detection and response
- ✓ GEO resilience, DDOS protection, isolated networking options
- ✓ 24 hour monitoring, multi-factor authentication, biometric scanning. Cyber Defense Operations Center (CDOC)
- ✓ Audited at least once every 12 months by 3rd party, compliant with international standards (ISO 27001, SOC2 AT 101, …)
- ✓ Build in and optional high availability mechanisms, memory preserving updates
- ✓ Secure Development mandatory following SDL (ISO/IEC 27034). Operational Security Assurance approach (OSA – NIST 800-53, ISO 27001 …)
- ✓ Built in advanced encryption options, VM Disk encryption, homomorphic encryption in SQL DB

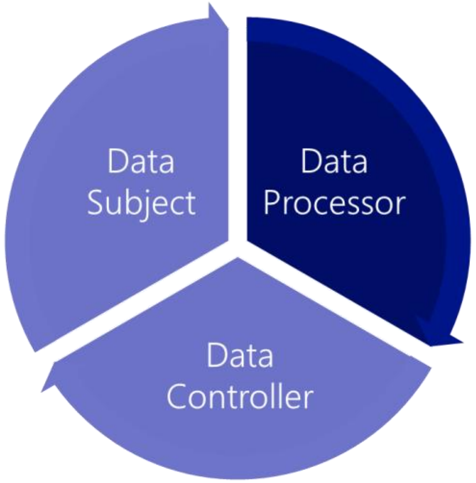
Privacy

Key principles from ISO27018

Cloud providers must:

Not use data for advertising or marketing unless express **consent** is obtained	Be **accountable** to determine if customer data was impacted by a breach of information security
Be **transparent** about data location and how data is handled	**Communicate** to customers and regulators in the event of a breach
Provide customers with **control** over how their data is used	Have services **independently audited** for compliance with this standard

Part of Microsofts control framework BSI certified under ISO 27001



Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments

Compliance

Compliance coverage

GLOBAL: ISO 27001, ISO 27018, ISO 27017, ISO 22301, ISO 9001, SOC 1 Type 2, SOC 2 Type 2, SOC 3, CSA STAR Self-Assessment, CSA STAR Certification, CSA STAR Attestation

US GOV: Moderate JAB P-ATO, High JAB P-ATO, DoD DISA SRG Level 2, DoD DISA SRG Level 4, DoD DISA SRG Level 5, SP 800-171, FIPS 140-2, Section 508 VPAT, ITAR, CJIS, IRS 1075

INDUSTRY: PCI DSS Level 1, CDSA, MPAA, FACT UK, Shared Assessments, FISC Japan, HIPAA / HITECH Act, HITRUST, GxP 21 CFR Part 11, MARS-E, IG Toolkit UK, FERPA, GLBA, FFIEC

REGIONAL: Argentina PDPA, EU Model Clauses, UK G-Cloud, China DJCP, China GB 18030, China TRUCS, Singapore MTCS, Australia IRAP/CCSL, New Zealand GCIO, Japan My Number Act, ENISA IAF, Japan CS Mark Gold, Spain ENS, Spain DPA, India MeitY, Canada Privacy Laws, Privacy Shield, Germany IT Grundschutz workbook

Transparency

You have visibility into our practices

Microsoft believes that you have a right to as much information as possible about how we handle your customer data in the cloud.

We provide you with clear explanations about where your data is stored and how we help secure it, as well as who can access it and under what circumstances. And you don't have to take our word for it. You can review a wide range of evidence, including independent audit reports and certifications for most of our business cloud services, to confirm that we meet the standards we set.

How we work to secure your data

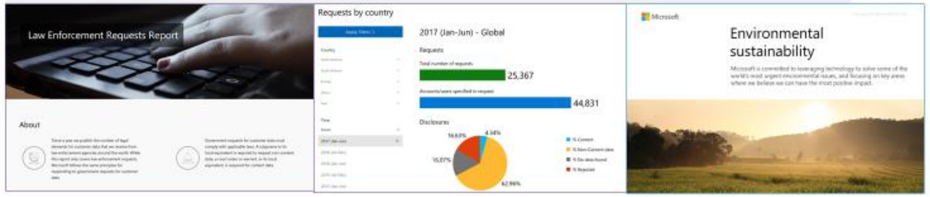
Where your data is stored

How we manage your data

Who can access your data and on what terms

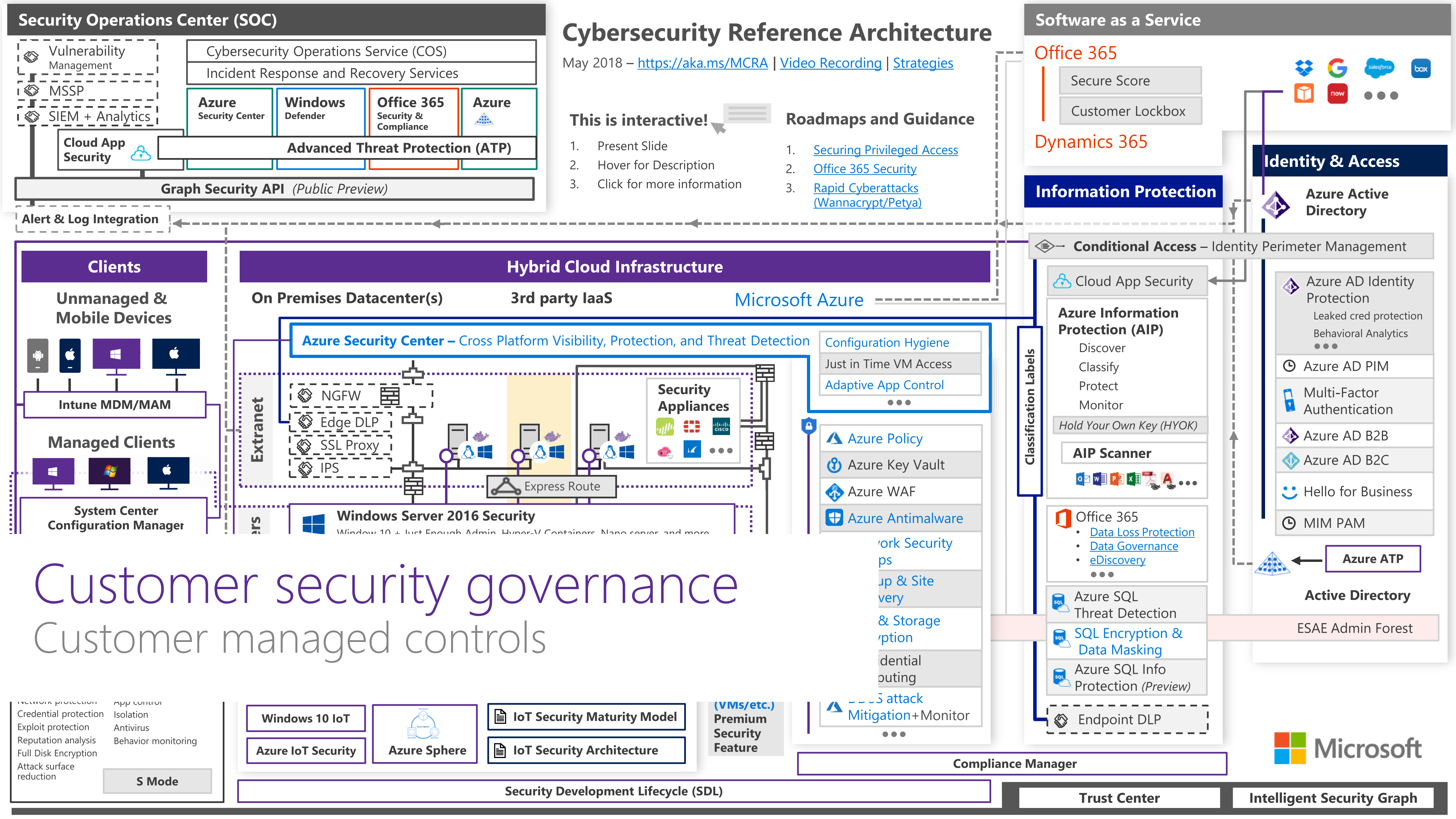
How we respond to government requests for your data

How we help you meet compliance requirements



Customer security governance

Customer managed controls



Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Vulnerability Management

MSSP

SIEM + Analytics

Cloud App Security

Cybersecurity Operations Service (COS)

Incident Response and Recovery Services

Azure Security Center

Windows Defender

Office 365 Security & Compliance

Azure

Advanced Threat Protection (ATP)

Graph Security API *(Public Preview)*

Alert & Log Integration

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

salesforce

box

now

•••

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

•••

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Classification Labels

Cloud App Security

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

•••

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

•••

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection *(Preview)*

Endpoint DLP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

•••

Extranet

NGFW

Edge DLP

SSL Proxy

IPS

Security Appliances

cisco

•••

Express Route

Windows Server 2016 Security

Windows 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

…ork Security

…ps

…up & Site …very

… & Storage …yption

…idential …outing

…DoS attack Mitigation+Monitor

•••

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

(VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft

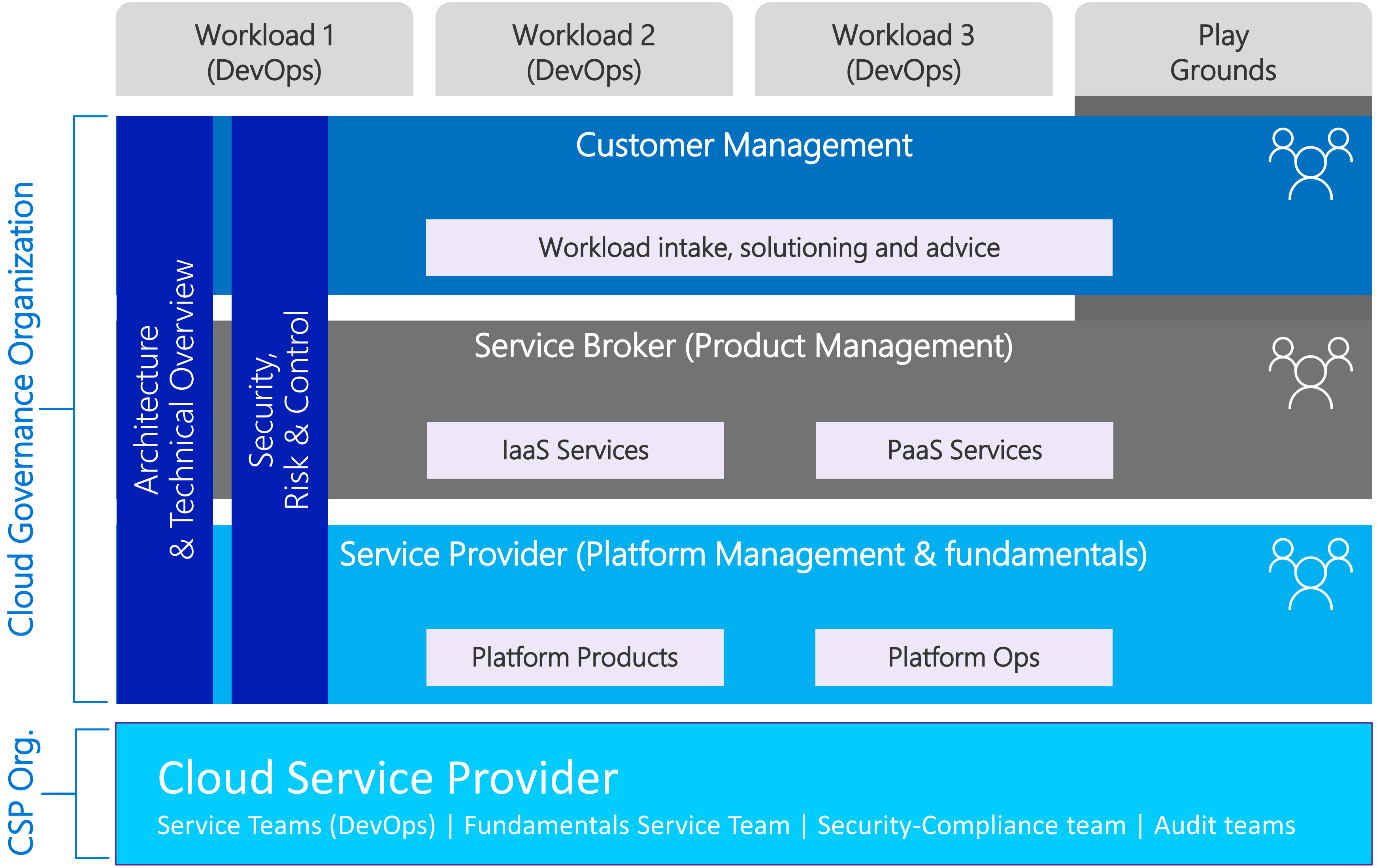
Cloud security operations

Customer managed controls

From central control to agile security…

Organization Model managing customer controls

facilitate protect, detect, respond conditions



Workload 1 (DevOps)
Workload 2 (DevOps)
Workload 3 (DevOps)
Play Grounds
Cloud Governance Organization
Architecture & Technical Overview
Security, Risk & Control
Customer Management
Workload intake, solutioning and advice
Service Broker (Product Management)
IaaS Services
PaaS Services
Service Provider (Platform Management & fundamentals)
Platform Products
Platform Ops
CSP Org.
Cloud Service Provider
Service Teams (DevOps) | Fundamentals Service Team | Security-Compliance team | Audit teams

1. Provide the foundation controls (network, Identity, crypto)
2. Provide service building blocks with preconfigured controls to DevOps teams. And enforce technical policies.
3. Enable detection: Instrument, Monitor and verify
4. Regular risk assessment (trust but verify)

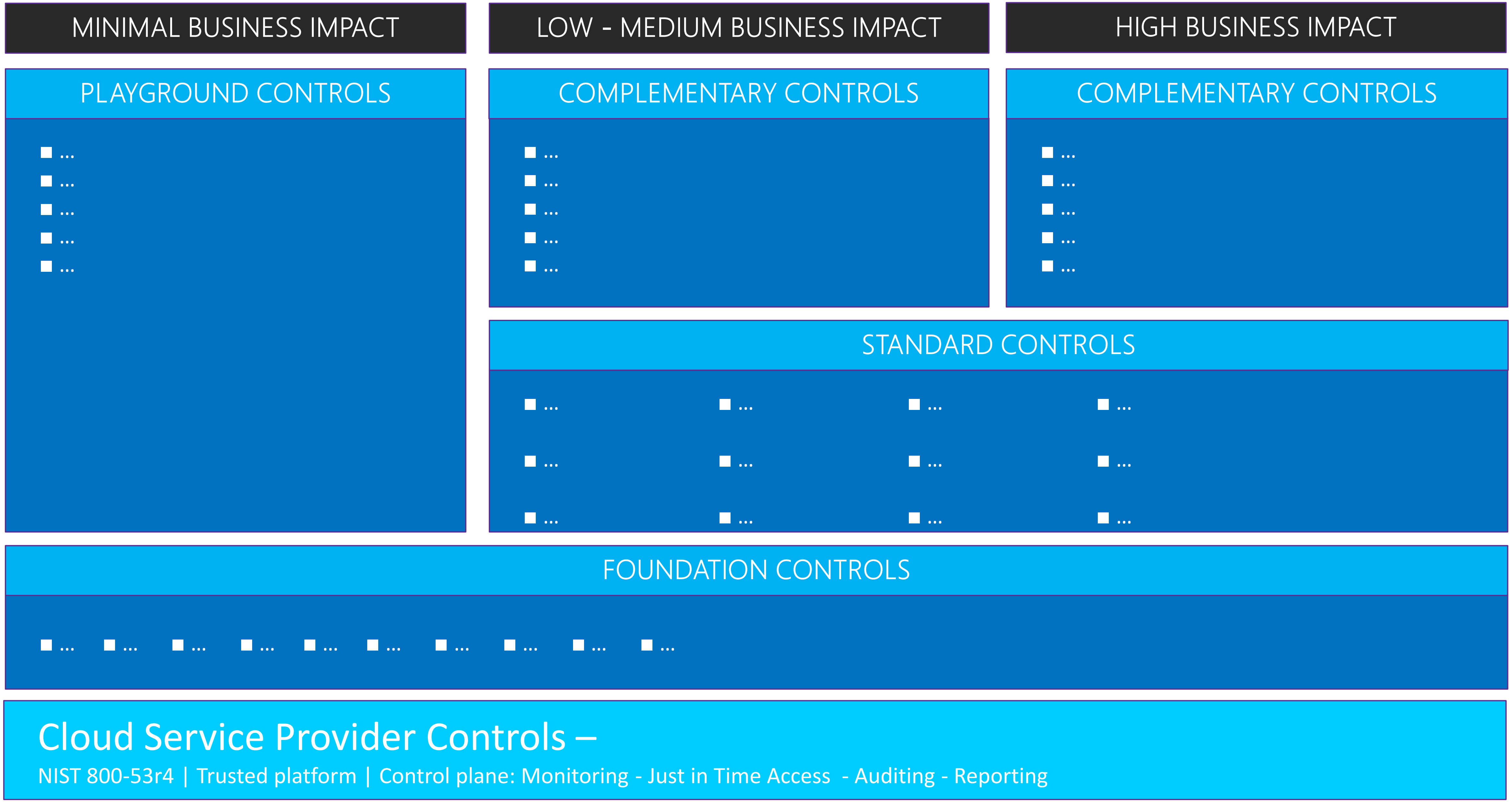
Sample Technical Security controls

connecting to a service security classification through risk assessment

- Control routing path for traffic from Azure private to Azure public and Internet
- Automatically clean/purge playground environments
- Automated & enforced Update Management
- Azure provided Key Management
- Connectivity controls on public end-points
- Control network protocols from Internet to Azure Private
- Monitor outbound traffic from Azure Private to Azure Public and Internet
- Monitor traffic from Azure to on-premises networks
- Monitor traffic from Azure private to Azure public and Internet
- Monitor traffic from Azure private to Azure public and Internet with SSL termination
- Vulnerability Management
- Declarative configuration management
- Encrypt data at rest for services with public endpoints
- Encrypt data at rest for services with public endpoints that lack IAM controls
- Encrypt data in transit over private interconnections
- Encrypt data in transit over public interconnections
- IAM on all accounts
- IAM on all resources
- Identity Threat Protection
- Infrastructure as Code (central repository, code review and approval, SDL, etc.)
- MFA on all user accounts

- Network segmentation and containment
- Network segmentation on application tier level
- No direct inbound traffic from Internet to Azure Private
- No network connectivity between playground and production workloads
- No outbound network connectivity to on-premises networks
- Assess and approve cloud services prior to deployment
- OS hardening
- OS Threat Protection
- Owner tagging (resource groups, resources)
- Monitor and assess updated Azure Service Terms and Audit Reports
- Platform Audit Logs
- Platform Security Monitoring
- Prescribe minimum OS levels
- Define Primary Application security layers (Data, IAM, Application)
- Customer provided Key Management
- Secure web publishing (network virtual appliance, Application Gateway. ...)
- Platform native security management and threat protection with on-prem SIEM integration
- Terms of use for isolated Playground environments (e.g. development and test purposes are prohibited)
- End-point protection
- End-point Detection and Response
- Web Application Firewall (WAF)
- **Data Leakage Prevention**

Security Control Framework: connect risk analysis to controls framework



MINIMAL BUSINESS IMPACT

PLAYGROUND CONTROLS

- ...
- ...
- ...
- ...
- ...

LOW - MEDIUM BUSINESS IMPACT

COMPLEMENTARY CONTROLS

- ...
- ...
- ...
- ...
- ...

HIGH BUSINESS IMPACT

COMPLEMENTARY CONTROLS

- ...
- ...
- ...
- ...
- ...

STANDARD CONTROLS

- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...

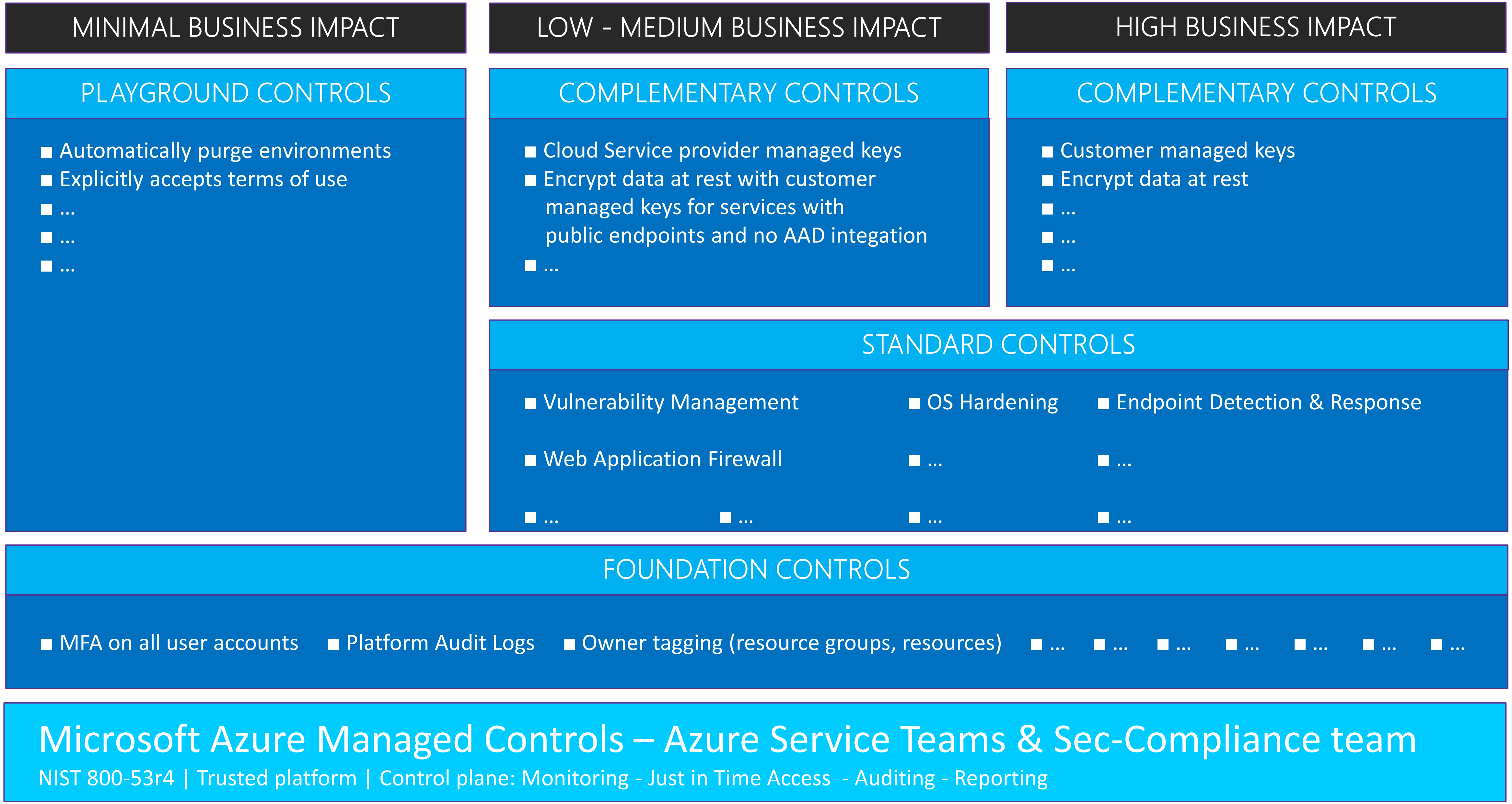
FOUNDATION CONTROLS

- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...

Cloud Service Provider Controls –

NIST 800-53r4 | Trusted platform | Control plane: Monitoring - Just in Time Access - Auditing - Reporting

Security Control Framework – Some Example Controls



MINIMAL BUSINESS IMPACT

PLAYGROUND CONTROLS

- Automatically purge environments
- Explicitly accepts terms of use
- …
- …
- …

LOW - MEDIUM BUSINESS IMPACT

COMPLEMENTARY CONTROLS

- Cloud Service provider managed keys
- Encrypt data at rest with customer managed keys for services with public endpoints and no AAD integration
- …

HIGH BUSINESS IMPACT

COMPLEMENTARY CONTROLS

- Customer managed keys
- Encrypt data at rest
- …
- …
- …

STANDARD CONTROLS

- Vulnerability Management
- OS Hardening
- Endpoint Detection & Response
- Web Application Firewall
- …
- …
- …
- …
- …
- …

FOUNDATION CONTROLS

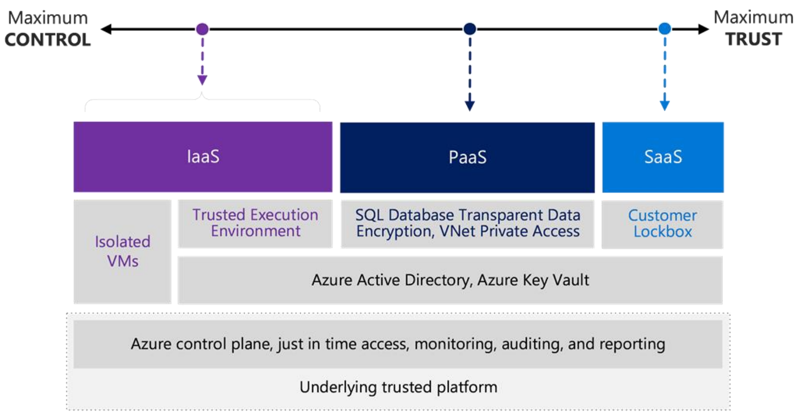
- MFA on all user accounts
- Platform Audit Logs
- Owner tagging (resource groups, resources)
- …
- …
- …
- …
- …
- …
- …

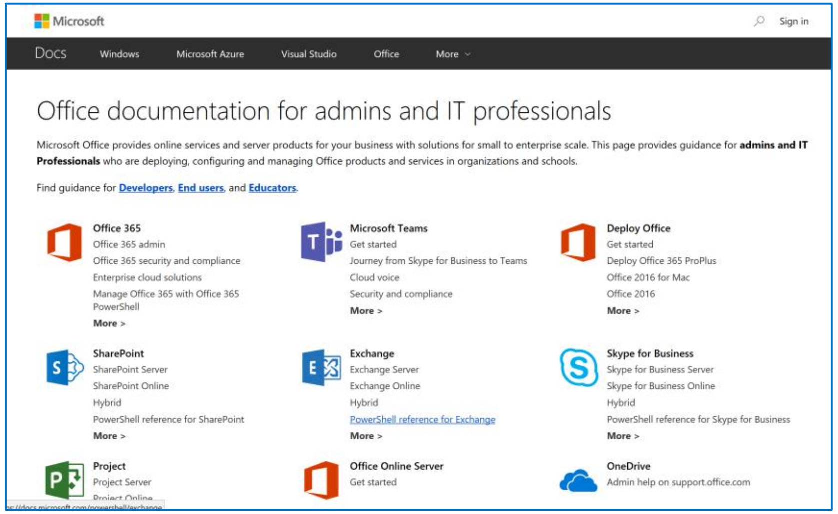
Microsoft Azure Managed Controls – Azure Service Teams & Sec-Compliance team

NIST 800-53r4 | Trusted platform | Control plane: Monitoring - Just in Time Access - Auditing - Reporting

Getting started…

Cloud requires knowledge and understanding


Maximum CONTROL
Maximum TRUST
IaaS
PaaS
SaaS
Isolated VMs
Trusted Execution Environment
SQL Database Transparent Data Encryption, VNet Private Access
Customer Lockbox
Azure Active Directory, Azure Key Vault
Azure control plane, just in time access, monitoring, auditing, and reporting
Underlying trusted platform



Office documentation for admins and IT professionals

Microsoft Office provides online services and server products for your business with solutions for small to enterprise scale. This page provides guidance for **admins and IT Professionals** who are deploying, configuring and managing Office products and services in organizations and schools.

Find guidance for Developers, End users, and Educators.

Office 365
Office 365 admin
Office 365 security and compliance
Enterprise cloud solutions
Manage Office 365 with Office 365 PowerShell
More >

Microsoft Teams
Get started
Journey from Skype for Business to Teams
Cloud voice
Security and compliance
More >

Deploy Office
Get started
Deploy Office 365 ProPlus
Office 2016 for Mac
Office 2016
More >

SharePoint
SharePoint Server
SharePoint Online
Hybrid
PowerShell reference for SharePoint
More >

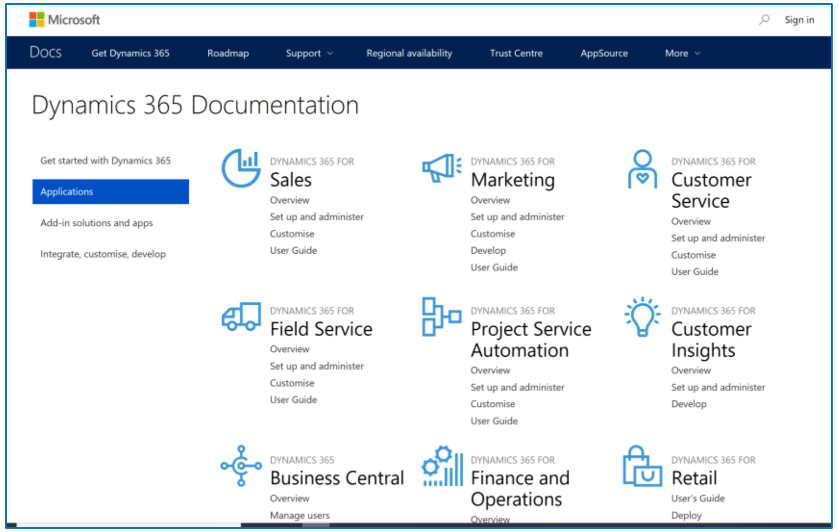
Exchange
Exchange Server
Exchange Online
Hybrid
PowerShell reference for Exchange
More >

Skype for Business
Skype for Business Server
Skype for Business Online
Hybrid
PowerShell reference for Skype for Business
More >

Project
Project Server
Project Online

Office Online Server
Get started

OneDrive
Admin help on support.office.com



Dynamics 365 Documentation

Get started with Dynamics 365
Applications
Add-in solutions and apps
Integrate, customise, develop

DYNAMICS 365 FOR
Sales
Overview
Set up and administer
Customise
User Guide

DYNAMICS 365 FOR
Marketing
Overview
Set up and administer
Customise
Develop
User Guide

DYNAMICS 365 FOR
Customer Service
Overview
Set up and administer
Customise
User Guide

DYNAMICS 365 FOR
Field Service
Overview
Set up and administer
Customise
User Guide

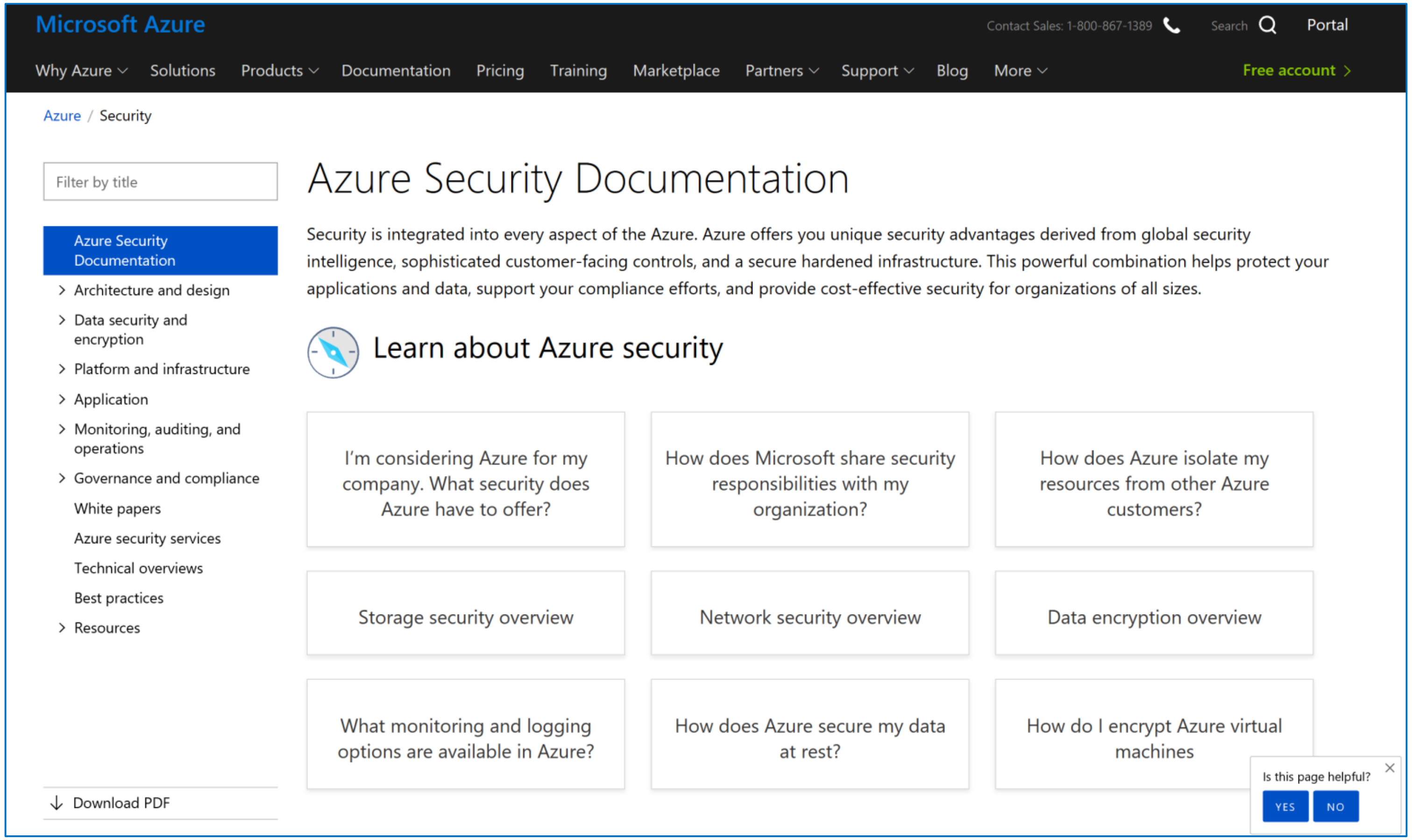
DYNAMICS 365 FOR
Project Service Automation
Overview
Set up and administer
Customise
User Guide

DYNAMICS 365 FOR
Customer Insights
Overview
Set up and administer
Develop

DYNAMICS 365
Business Central
Overview
Manage users

DYNAMICS 365 FOR
Finance and Operations
Overview

DYNAMICS 365 FOR
Retail
User's Guide
Deploy



Azure Security Documentation
Architecture and design
Data security and encryption
Platform and infrastructure
Application
Monitoring, auditing, and operations
Governance and compliance
White papers
Azure security services
Technical overviews
Best practices
Resources

Azure Security Documentation

Security is integrated into every aspect of the Azure. Azure offers you unique security advantages derived from global security intelligence, sophisticated customer-facing controls, and a secure hardened infrastructure. This powerful combination helps protect your applications and data, support your compliance efforts, and provide cost-effective security for organizations of all sizes.

Learn about Azure security

I'm considering Azure for my company. What security does Azure have to offer?

How does Microsoft share security responsibilities with my organization?

How does Azure isolate my resources from other Azure customers?

Storage security overview

Network security overview

Data encryption overview

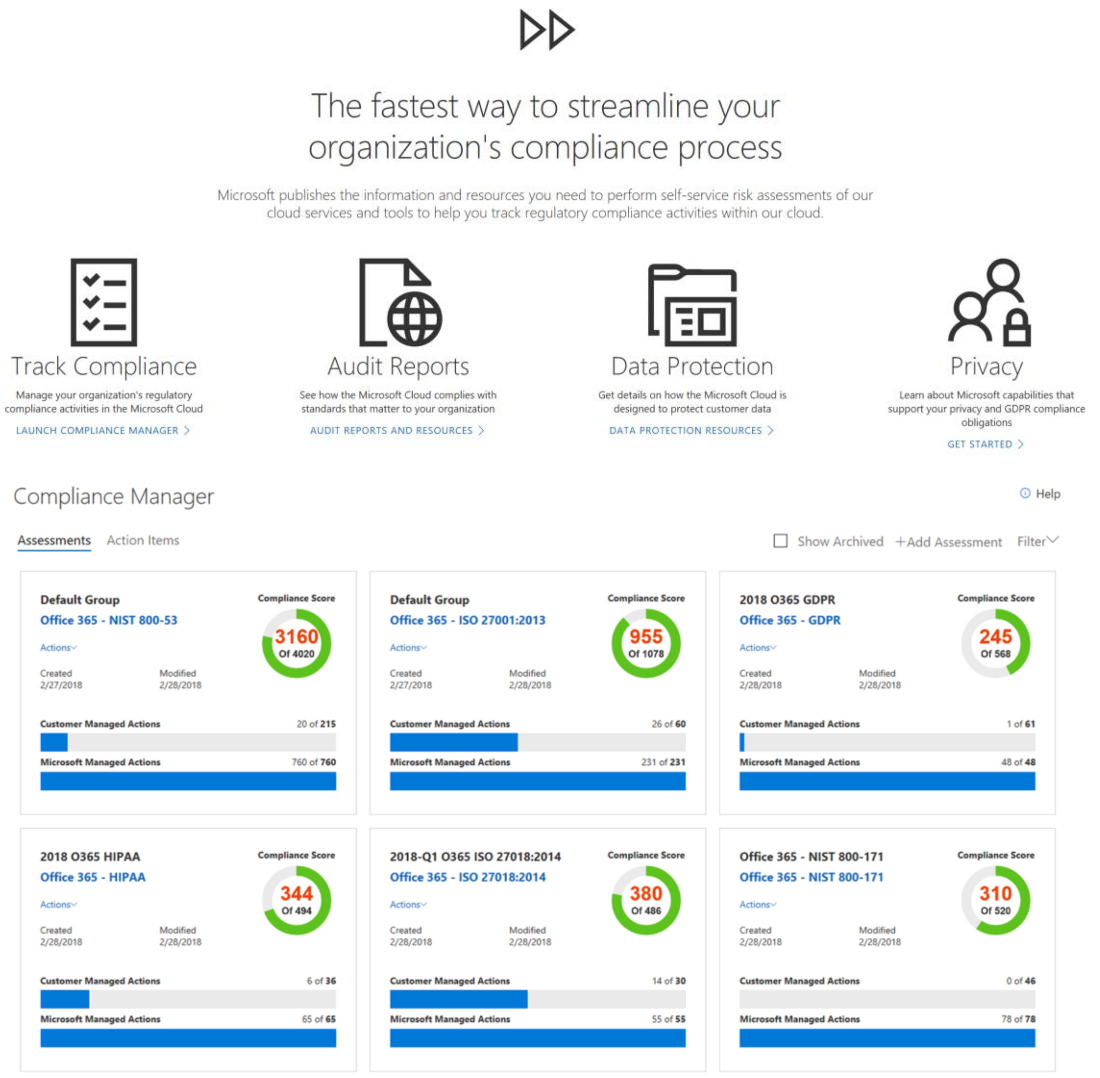
What monitoring and logging options are available in Azure?

How does Azure secure my data at rest?

How do I encrypt Azure virtual machines

Assurance & tooling

https://aka.ms/stp (GDPR example)



The fastest way to streamline your organization's compliance process

Microsoft publishes the information and resources you need to perform self-service risk assessments of our cloud services and tools to help you track regulatory compliance activities within our cloud.

Track Compliance

Manage your organization's regulatory compliance activities in the Microsoft Cloud

LAUNCH COMPLIANCE MANAGER >

Audit Reports

See how the Microsoft Cloud complies with standards that matter to your organization

AUDIT REPORTS AND RESOURCES >

Data Protection

Get details on how the Microsoft Cloud is designed to protect customer data

DATA PROTECTION RESOURCES >

Privacy

Learn about Microsoft capabilities that support your privacy and GDPR compliance obligations

GET STARTED >

Compliance Manager

Default Group
Office 365 - NIST 800-53
Actions
Created 2/27/2018 Modified 2/28/2018
Compliance Score 3160 Of 4020
Customer Managed Actions 20 of 215
Microsoft Managed Actions 760 of 760

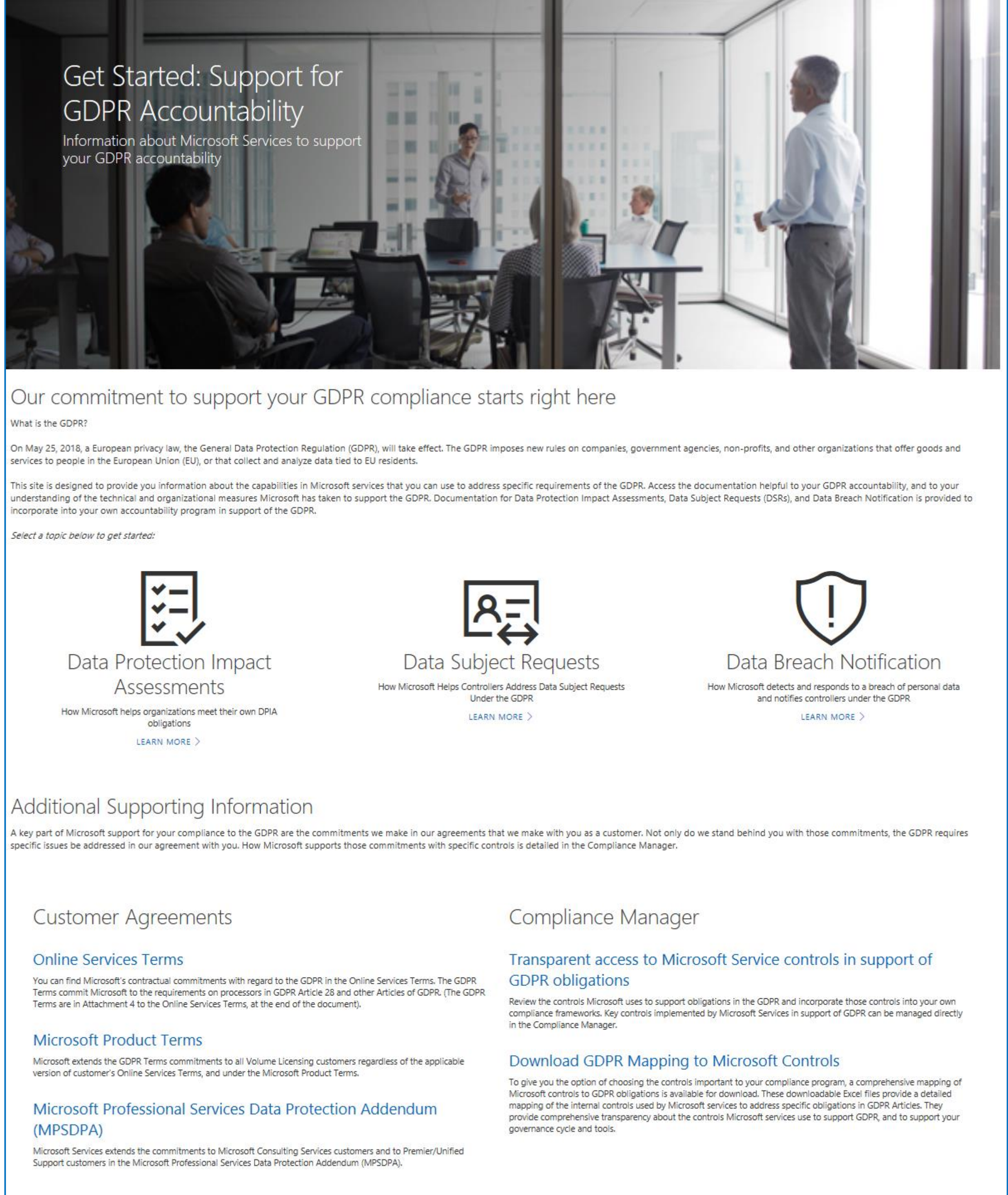
Default Group
Office 365 - ISO 27001:2013
Actions
Created 2/27/2018 Modified 2/28/2018
Compliance Score 955 Of 1078
Customer Managed Actions 26 of 60
Microsoft Managed Actions 231 of 231

2018 O365 GDPR
Office 365 - GDPR
Actions
Created 2/28/2018 Modified 2/28/2018
Compliance Score 245 Of 568
Customer Managed Actions 1 of 61
Microsoft Managed Actions 48 of 48

2018 O365 HIPAA
Office 365 - HIPAA
Actions
Created 2/28/2018 Modified 2/28/2018
Compliance Score 344 Of 494
Customer Managed Actions 6 of 36
Microsoft Managed Actions 65 of 65

2018-Q1 O365 ISO 27018:2014
Office 365 - ISO 27018:2014
Actions
Created 2/28/2018 Modified 2/28/2018
Compliance Score 380 Of 486
Customer Managed Actions 14 of 30
Microsoft Managed Actions 55 of 55

Office 365 - NIST 800-171
Office 365 - NIST 800-171
Actions
Created 2/28/2018 Modified 2/28/2018
Compliance Score 310 Of 520
Customer Managed Actions 0 of 46
Microsoft Managed Actions 78 of 78



Get Started: Support for GDPR Accountability

Information about Microsoft Services to support your GDPR accountability

Our commitment to support your GDPR compliance starts right here

What is the GDPR?

On May 25, 2018, a European privacy law, the General Data Protection Regulation (GDPR), will take effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

This site is designed to provide you information about the capabilities in Microsoft services that you can use to address specific requirements of the GDPR. Access the documentation helpful to your GDPR accountability, and to your understanding of the technical and organizational measures Microsoft has taken to support the GDPR. Documentation for Data Protection Impact Assessments, Data Subject Requests (DSRs), and Data Breach Notification is provided to incorporate into your own accountability program in support of the GDPR.

Select a topic below to get started:

Data Protection Impact Assessments

How Microsoft helps organizations meet their own DPIA obligations

LEARN MORE >

Data Subject Requests

How Microsoft Helps Controllers Address Data Subject Requests Under the GDPR

LEARN MORE >

Data Breach Notification

How Microsoft detects and responds to a breach of personal data and notifies controllers under the GDPR

LEARN MORE >

Additional Supporting Information

A key part of Microsoft support for your compliance to the GDPR are the commitments we make in our agreements that we make with you as a customer. Not only do we stand behind you with those commitments, the GDPR requires specific issues be addressed in our agreement with you. How Microsoft supports those commitments with specific controls is detailed in the Compliance Manager.

Customer Agreements

Online Services Terms

You can find Microsoft's contractual commitments with regard to the GDPR in the Online Services Terms. The GDPR Terms commit Microsoft to the requirements on processors in GDPR Article 28 and other Articles of GDPR. (The GDPR Terms are in Attachment 4 to the Online Services Terms, at the end of the document).

Microsoft Product Terms

Microsoft extends the GDPR Terms commitments to all Volume Licensing customers regardless of the applicable version of customer's Online Services Terms, and under the Microsoft Product Terms.

Microsoft Professional Services Data Protection Addendum (MPSDPA)

Microsoft Services extends the commitments to Microsoft Consulting Services customers and to Premier/Unified Support customers in the Microsoft Professional Services Data Protection Addendum (MPSDPA).

Compliance Manager

Transparent access to Microsoft Service controls in support of GDPR obligations

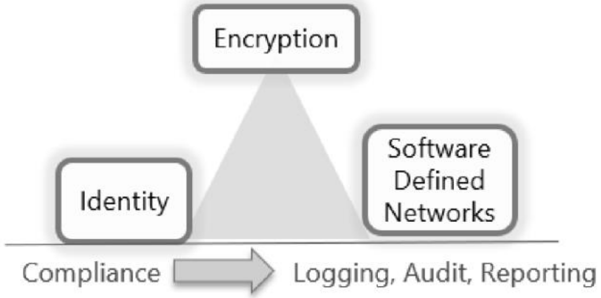
Review the controls Microsoft uses to support obligations in the GDPR and incorporate those controls into your own compliance frameworks. Key controls implemented by Microsoft Services in support of GDPR can be managed directly in the Compliance Manager.

Download GDPR Mapping to Microsoft Controls

To give you the option of choosing the controls important to your compliance program, a comprehensive mapping of Microsoft controls to GDPR obligations is available for download. These downloadable Excel files provide a detailed mapping of the internal controls used by Microsoft services to address specific obligations in GDPR Articles. They provide comprehensive transparency about the controls Microsoft services use to support GDPR, and to support your governance cycle and tools.

Key activities and essential controls

to address risk



Governance & Risk management & Policies

- Develop policies for how to evaluate, adopt, and use cloud services to minimize creation of inconsistencies and vulnerabilities that attackers can exploit.
- Identity policies
- Data policies
- Compliance policies and documentation

Administrative Privilege Management

- IT administrators are a dependency for cloud security. The privileged accounts, credentials, and workstations where the accounts are used must be protected and monitored.

Identity Systems and Identity Management

- Secure identity systems at or above the level of cloud services.

Data Protection

- You own your data. Classify your sensitive data and ensure it is protected and monitored wherever it is stored.

Monitoring, Threat awareness and Incident Response

- Evaluate the threats that apply to your organization and put them into context by leveraging resources like threat intelligence and Information Sharing and Analysis Centers (ISACs).
- Implementing continuous monitoring & detection capabilities

Security in and of the cloud

agility & change is the new normal...

Microsoft

Thank you!

References

Microsoft assurance information

1. **Descriptive:**

   Microsoft trustcenter: https://www.microsoft.com/en-us/TrustCenter/default.aspx

2. **Independently verified:**

   Microsoft Service Trust portal: https://servicetrust.microsoft.com

3. **Contractual:**

   Microsoft online service terms & SLA: https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx

- Microsoft On the Issues: https://blogs.microsoft.com/on-the-issues/
- Microsoft Data & Law: https://blogs.microsoft.com/datalaw/
- Microsoft Transparency reports: https://www.microsoft.com/en-us/about/corporate-responsibility/reports-hub
- Microsoft Cloud IT Architecture resources: https://docs.microsoft.com/en-us/office365/enterprise/microsoft-cloud-it-architecture-resources
- Cloud Services Due Diligence Checklist (ISO 19086 based): https://www.microsoft.com/en-us/trustcenter/Compliance/Due-Diligence-Checklist
- SAFE Handbook: http://aka.ms/safehandbook
- Microsoft Cyber Trust Blog: https://blogs.microsoft.com/cybertrust
- Microsoft Secure: https://www.microsoft.com/en-us/security/default.aspx
- A Data driven security defense: https://gallery.technet.microsoft.com/Fixing-the-1-Problem-in-2e58ac4a
- Enterprise Cloud strategy e-book: https://info.microsoft.com/enterprise-cloud-strategy-ebook.html
- Microsoft Security Intelligence Report: https://www.microsoft.com/security/sir/default.aspx