# Security < cloud < security

Martin Vliem, CISSP, CISA
National Security Officer
Microsoft

martin.vliem@microsoft.com

Microsoft

# Digital transformation

CVRIA

European Council
Council of the European Union

Language selection

Search

The European Council | The Council of the EU | Topics | Policies | Meetings | Documents & Publications | Press | Contact

Home > Press > Press releases and statements > EU-wide cybersecurity rules adopted by the Council

About this site | Legal notice | Contact | Search | English (EN)

EAN COMMISSION

ease Database

lease details

RSS

Login | Subscribe

U.S. Privacy Shield: stronger protection for transatlantic data flows

he EU-U.S. Privacy Shield.

ights of anyone in the EU whose personal data is transferred to the United States as well as
ransatlantic data transfers.

De economische en maatschappelijke noodzaak van meer

CYBER SECURITY

Nederland digitaal droge voeten

Zuidelij
Stille Zui

NIEUW-
ZEELAND

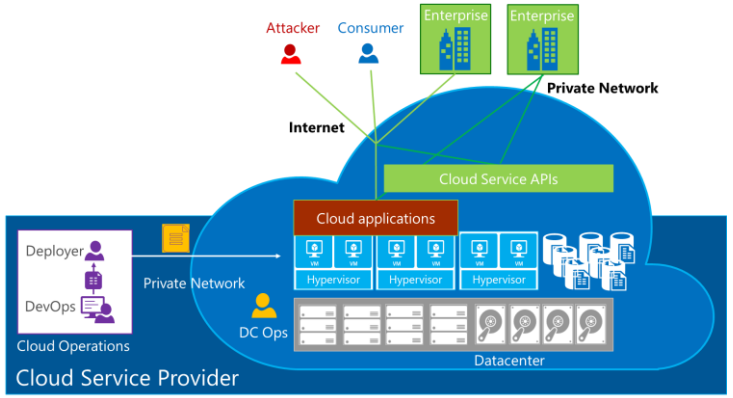
# The CSA Treacherous 12

## Top threat 2016

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

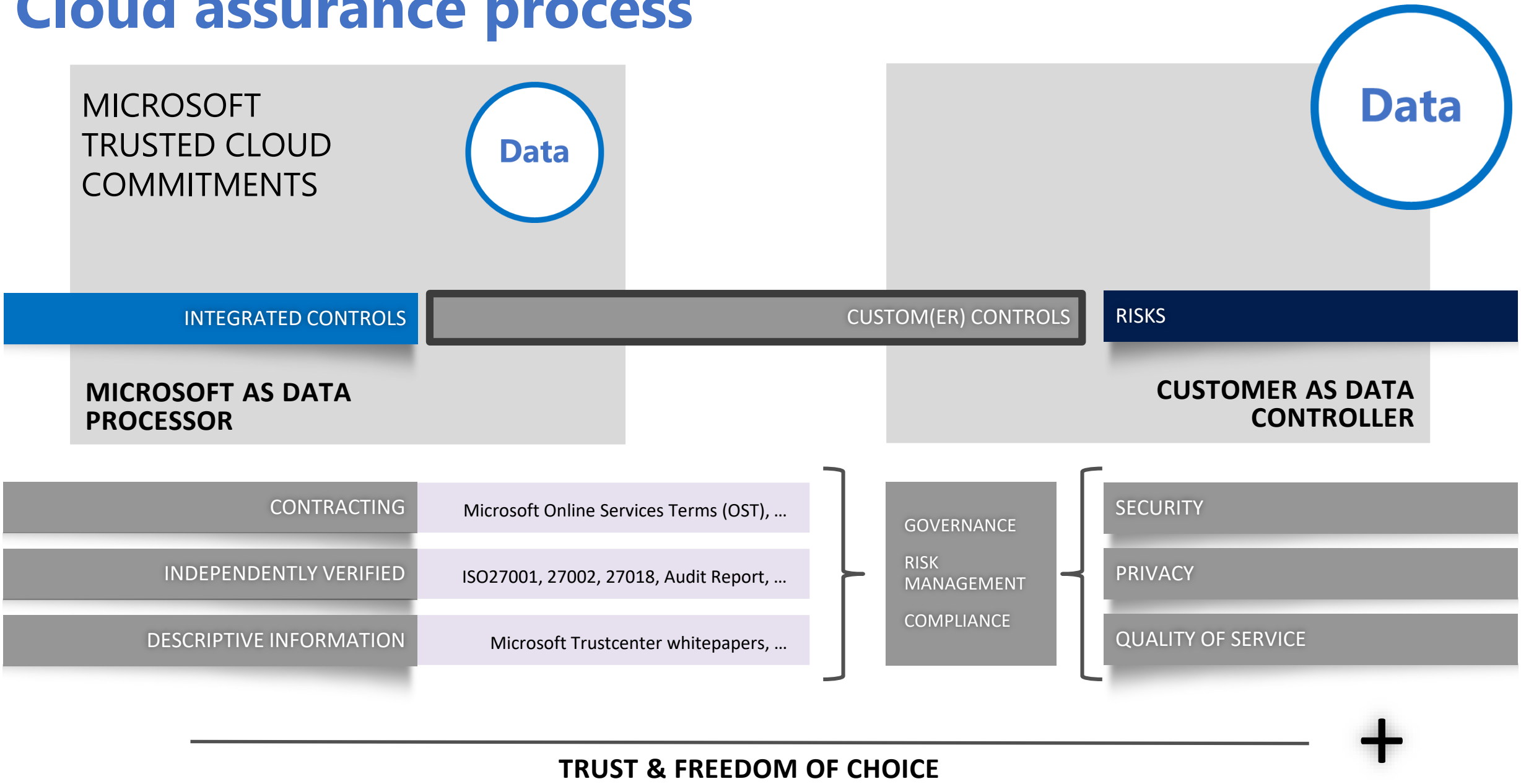
## Notorious nine 2013

1. Data breaches
2. Data loss
3. Account or service traffic hijacking
4. Insecure interfaces and APIs
5. Denial of service
6. Malicious insiders
7. Abuse of cloud services
8. Insufficient due diligence
9. Shared technology vulnerabilities




https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/

# Cloud assurance process



# Cloud assurance process

1 Legal/policy compliance requirements to customer

MICROSOFT TRUSTED CLOUD COMMITMENTS

Data

INTEGRATED CONTROLS

CONTRACTING

INDEPENDENTLY VERIFIED

DESCRIPTIVE INFORMATION

**MICROSOFT AS DATA PROCESSOR**

2 Customer starts assessment

GOVERNANCE, RISK & COMPLIANCE

3 Customer requests assurances from Cloud vendor

4 Microsoft provides attestations, certifications and legal commitments

RISKS

CLOUD PROVIDER CLAIMS

CUSTOM(ER) CONTROLS & PROCESSES

5 Customer evaluates claims and adds additional controls

6 Customer demonstrates compliance. Optionally requests third party audit or certification

**CUSTOMER AS DATA CONTROLLER**

The DNB Sjabloon coverage report helps customers to map and evaluate Microsoft's assurances to the DNB sjabloon

# Trusted cloud principles
## Microsoft commitments

SECURITY

PRIVACY & CONTROL

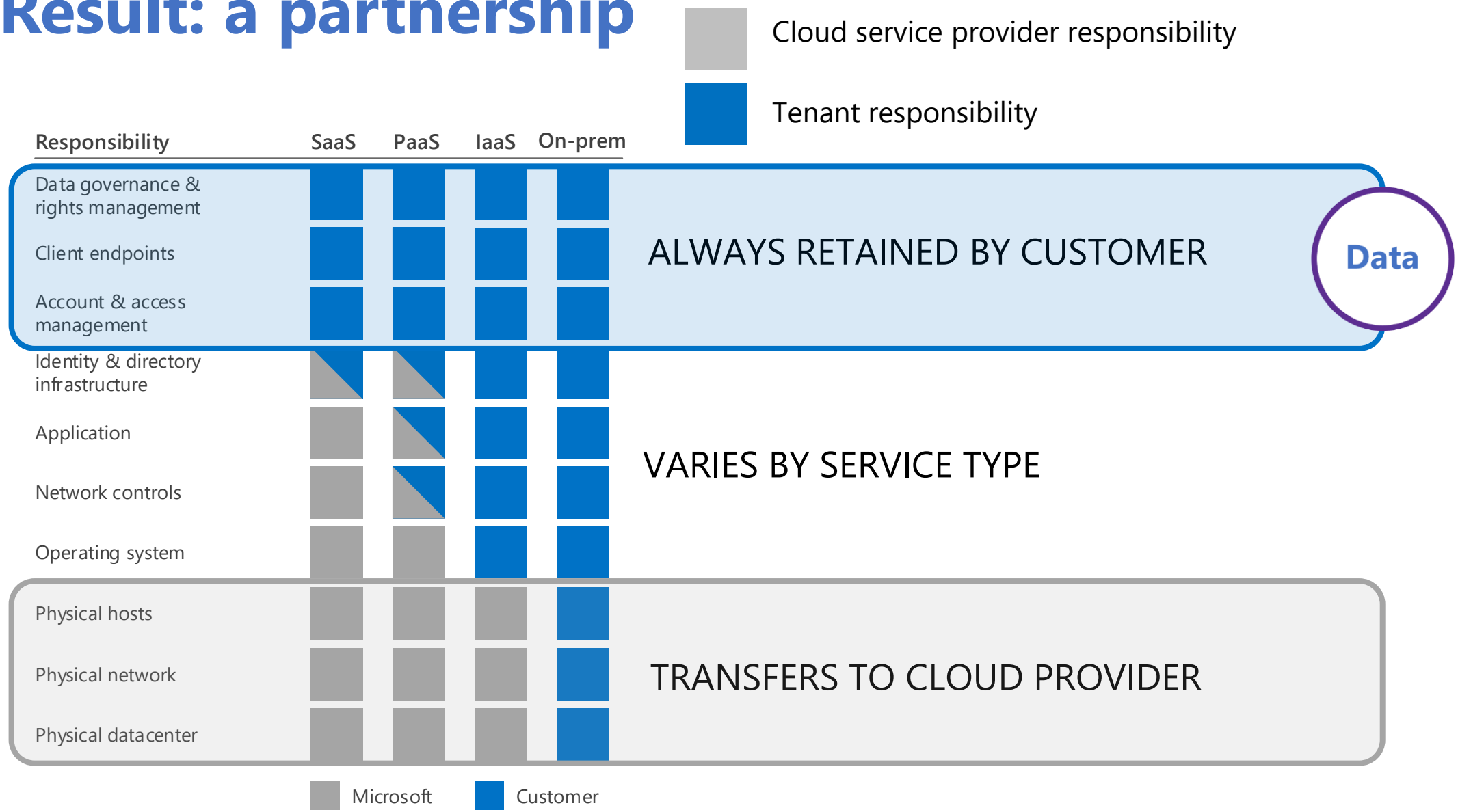
COMPLIANCE

TRANSPARENCY

RELIABILITY

OUR COMMITMENT
TO **YOU**

# Result: a partnership



3759
KINGMAN,
ARIZONA.
3759
SANTA FE
3759

# Customer responsibilities

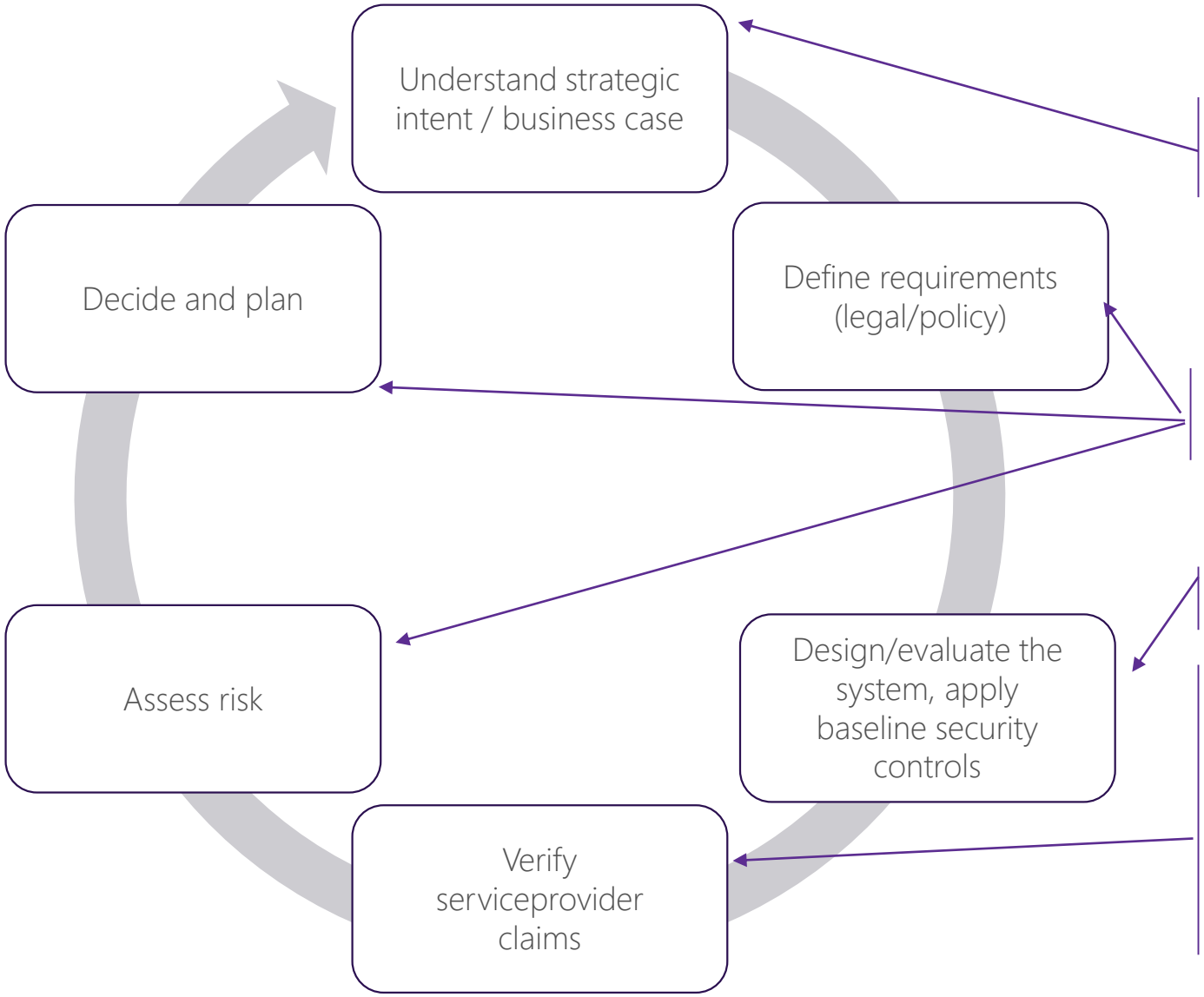
## Empowerment through Microsoft Secure

| Software as a Service<br>Office 365 - SaaS | Platform as a Service<br>Azure - PaaS | Infrastructure as a Service<br>Azure - IaaS | On Premises<br>Security Dependencies |
|---|---|---|---|
| 1. Security strategy, governance, and operationalization: Provide clear vision, standards, and guidance for your organization | | | |
| 2. Administrative control: Defend against the loss of control of your cloud services and on-premises systems | | | |
| 3. Data: Identify and protect your most important information assets | | | |
| 4. User identity and device security: Strengthen protection for accounts and devices | | | |
| | 5. Application security: Ensure application code is resilient to attacks | | |
| | 6. Network: Ensure connectivity, isolation, and visibility into anomalous behavior | | |
| | | 7. Operating system and middleware: Protect integrity of hosts | |
| | | | 8. Private or on-premises environments: Secure the foundation |

Microsoft Secure

Cinderella

# Cloud assurance approach




Microsoft
Cyber Trust Blog
Cloud Computing · Cybersecurity · Data Privacy · Tips & Talk · Topics

Microsoft publishes guide for secure and efficient integration of cloud services into government operations

- Value proposition, business case
- Best practices, guidelines, frameworks- CSA
- Architecture diagram, solution guidance
- Assurances:
  - ✓ Descriptive
  - ✓ 3rd party validated
  - ✓ Contractural
- Control mapping support
- Q&A specialist sessions

# **Discussion**
## top questions

DATA
**CONTROLLER**

1. HOW SECURE IS MY DATA?
2. CAN I CONTROL MY DATA?
3. HOW CAN I STAY COMPLIANT?
4. WHAT HAPPENS WITH MY DATA?

DATA
**PROCESSOR**

# The World
is digital

Location of Customer Data at Rest
Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows:

Office 365 Services. If Customer provisions its tenant in Australia, the European Union, India, Japan or the United States (each of the foregoing a Geo), Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments) and (2) SharePoint Online site content and the files stored within that site.
(...)

**Microsoft Online Service Terms (OST)**

CONTRACTUAL

# The World
is sovereign

Our search warrant case: An important decision for people everywhere

Today the United States Court of Appeals for the Second Circuit ruled in a case brought by Microsoft addressing the global application of U.S. search warrants for people's email. The court ruled in favor of Microsoft overturning an earlier ruling from a lower court.

We obviously welcome today's decision by the United States Court of Appeals for the Second Circuit. The decision is important for three reasons: it ensures that people's privacy rights are protected by the laws of their own countries (...)

**Legal court case against USA Government**

MICROSOFT SEARCH WARRANT CASE

# Government access to data

## Law Enforcement Request report

Only 28 requests for Enterprise Accounts for the same period!

- 12 Rejected, withdrawn or redirected
- 11 Compelled to respond non-content only
- 5 Compelled to respond some content

These numbers include mostly consumer services requests (hotmail/outlook, Skype)

Requests received for all Microsoft Services from January - June 2016

| | Total Requests | | Some Customer Data Disclosed | | | | No Customer Data Disclosed | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Total Number of Law Enforcement Requests | Accounts / Users Specified in Requests | Law Enforcement Requests Resulting in Disclosure of Content | | Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data | | Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found) | | Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements) | |
| | # | # | % | # | % | # | % | # | % | # |
| **TOTAL** | **35.572** | **60.367** | **2,65%** | **943** | **65,91%** | **23.445** | **18,66%** | **6637** | **12,78%** | **4547** |
| Turkey | 7.364 | 7.907 | 0,00% | - | 70,27% | 5.175 | 26,41% | 1.945 | 3,31% | 244 |
| United States | 5.168 | 13.755 | 9,31% | 481 | 56,44% | 2.917 | 16,85% | 871 | 17,40% | 899 |
| France | 5.045 | 7.068 | 0,00% | - | 57,24% | 2.888 | 15,62% | 788 | 27,14% | 1.369 |
| United Kingdom | 4.731 | 8.249 | 0,00% | - | 75,10% | 3.553 | 17,99% | 851 | 6,91% | 327 |
| Germany | 4.167 | 7.307 | 0,00% | - | 68,56% | 2.857 | 15,96% | 665 | 15,48% | 645 |
| Brazil | 1.251 | 2.077 | 36,61% | 458 | 40,37% | 505 | 20,06% | 251 | 2,96% | 37 |
| Australia | 1.000 | 1.154 | 0,00% | - | 71,50% | 715 | 18,00% | 180 | 10,50% | 105 |
| Argentina | 866 | 1.061 | 0,00% | - | 79,68% | 690 | 14,43% | 125 | 5,89% | 51 |
| Italy | 663 | 1.247 | 0,00% | - | 64,71% | 429 | 16,14% | 107 | 19,16% | 127 |
| Spain | 623 | 946 | 0,00% | - | 65,49% | 408 | 19,42% | 121 | 15,09% | 94 |
| Portugal | 522 | 595 | 0,00% | - | 71,07% | 371 | 13,98% | 73 | 14,94% | 78 |
| India | 507 | 1.117 | 0,00% | - | 69,43% | 352 | 14,20% | 72 | 16,37% | 83 |
| Taiwan | 393 | 1.299 | 0,00% | - | 66,92% | 263 | 25,45% | 100 | 7,63% | 30 |
| Netherlands | 385 | 441 | 0,00% | - | 82,34% | 317 | 14,03% | 54 | 3,64% | 14 |
| Belgium | 351 | 453 | 0,00% | - | 71,51% | 251 | 16,24% | 57 | 12,25% | 43 |
| Mexico | 347 | 708 | 0,00% | - | 71,18% | 247 | 21,33% | 74 | 7,49% | 26 |
| Japan | 224 | 285 | 0,00% | - | 58,04% | 130 | 19,20% | 43 | 22,77% | 51 |
| Norway | 200 | 1.060 | 0,00% | - | 79,50% | 159 | 11,00% | 22 | 9,50% | 19 |
| Sweden | 185 | 257 | 0,00% | - | 77,30% | 143 | 11,89% | 22 | 10,81% | 20 |
| Colombia | 134 | 234 | 0,00% | - | 83,58% | 112 | 9,70% | 13 | 6,72% | 9 |
| Chile | 127 | 147 | 0,00% | - | 75,59% | 96 | 14,17% | 18 | 10,24% | 13 |
| Luxembourg | 109 | 494 | 2,75% | 3 | 65,14% | 71 | 22,94% | 25 | 9,17% | 10 |
| Hong Kong | 106 | 110 | 0,00% | | 58,49% | 62 | 12,26% | 13 | 29,25% | 31 |

SOURCE: http://www.microsoft.com/about/csr/transparencyhub/lerr/

# Freedom of choice
# **cloud services**

| CUSTOMER | PARTNER | MICROSOFT CLOUD GLOBAL | | MICROSOFT CLOUD SOVEREIGN |
|---|---|---|---|---|
| Customer Datacenter | Partner Datacenter | Microsoft Datacenters Europe | Microsoft Datacenters UK | Microsoft Cloud Germany |
| Deployed on customer-dedicated resources with Microsoft products and technologies. Benefit from cloud experiences on your own premises. | Cloud services deployed on dedicated resources, hosted or operated by a Microsoft partner. Provides integrated or industry-specific service offerings. | Hyper-scale, globally connected cloud services deployed from regional Microsoft datacenters. | Local datacenters enable customers to address local data residency requirements. | Rare, non-standard deployment of Microsoft cloud resources that meet the unique requirements of certain markets |

# Summary
## key approach and activities

1. Cloud security is a partnership, governance is key
   - Business case and Risk management is foundational
   - Implement flexible goverance processes
   - Design security requirements & policies
2. Request cloud provider assurances on integrated security capabilities
   - Many operational & security responsibilities can be transferred to the service provider.
3. Additional customer controls & requirements, empowered by cloud platforms
   - Administrative Privilege Management
   - Identity Systems and Identity Management
   - Threat Awareness & monitoring
   - Data Protection

# References

## Microsoft trust

- Microsoft trustcenter: http://www.microsoft.com/en-us/TrustCenter/default.aspx
- Microsoft Service Trust portal: http://aka.ms/STP
- Microsoft online service terms: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31
- Microsoft Cloud IT Architecture resources: https://technet.microsoft.com/en-us/library/dn919927.aspx
- 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

Thank you.

Microsoft