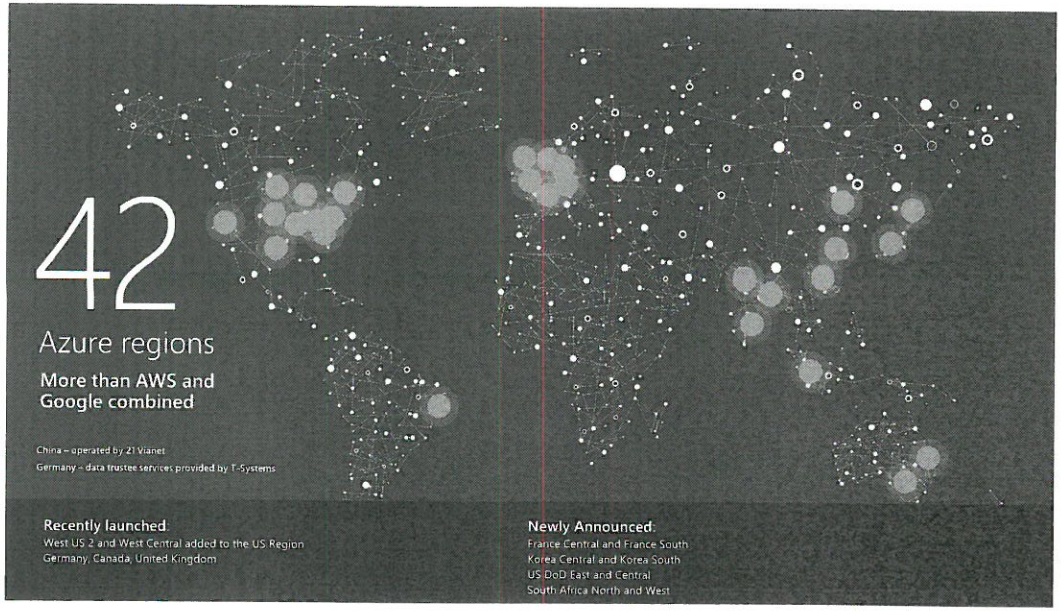
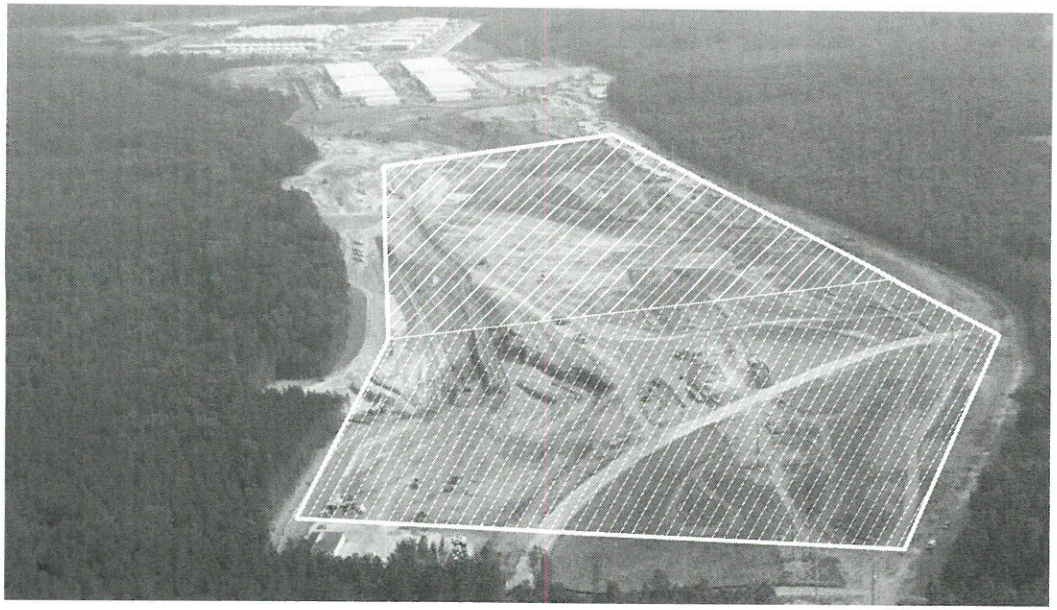
Microsoft

Leveraging Opportunity without Compromising Security

Robert Dring, FSI Audit Lead, Office 365

Hyperscale Cloud



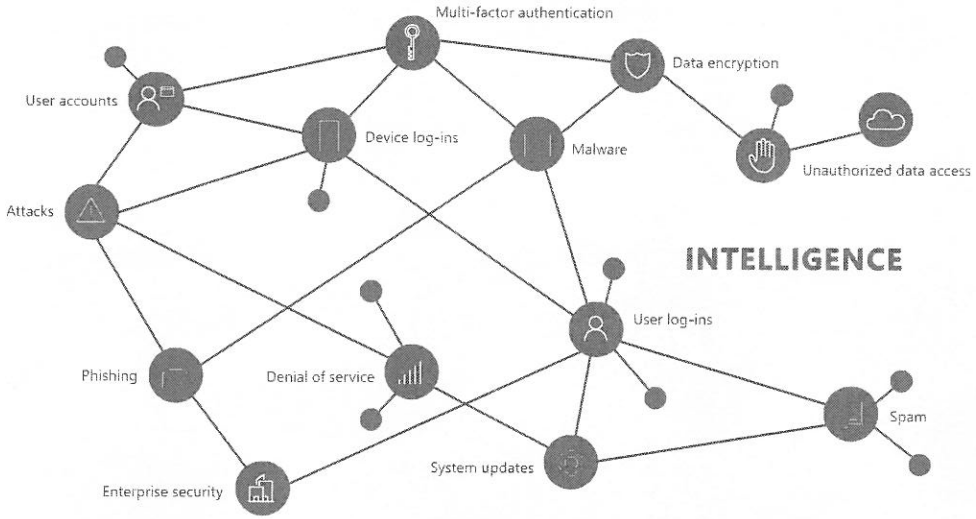


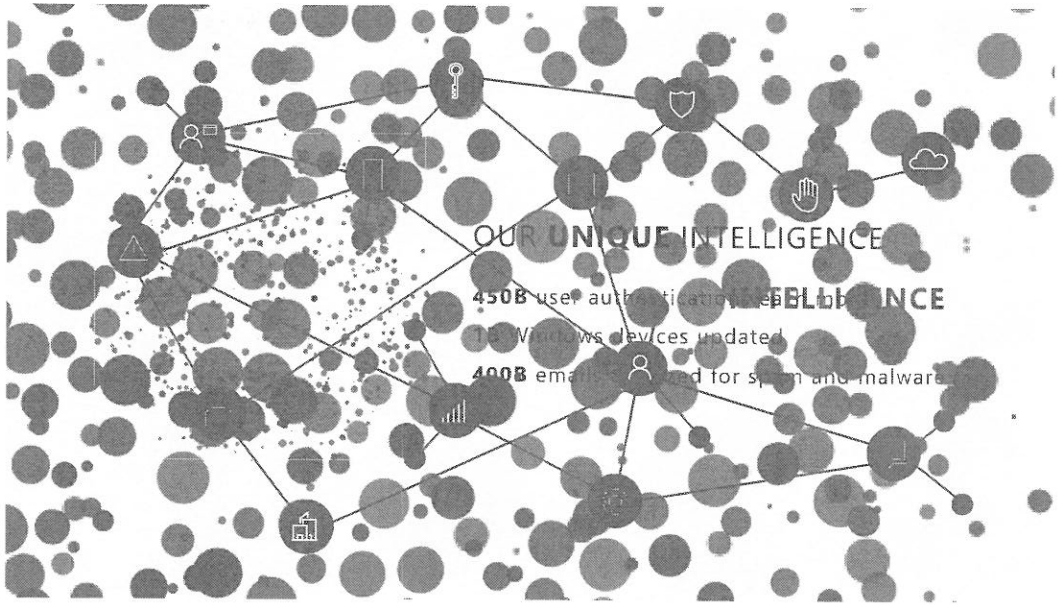
OUR **UNIQUE** APPROACH

Platform

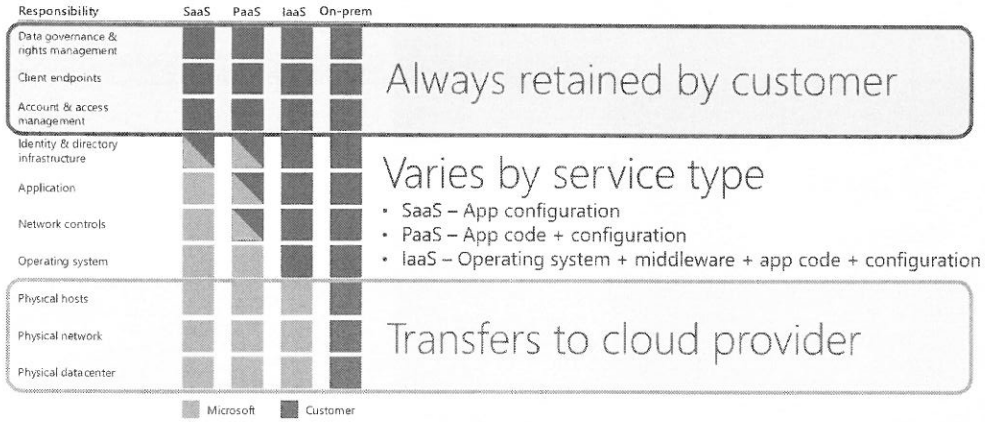
Intelligence

Features

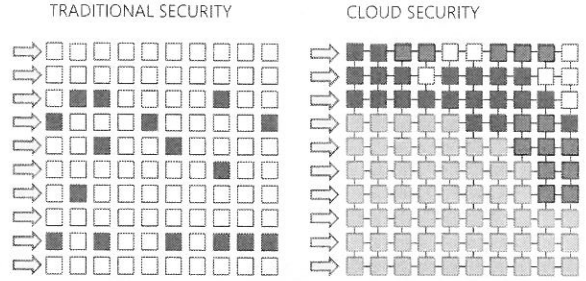




Shared Responsibility for Workloads



Security Advantages of Cloud



Security is a challenging and under-resourced function

- Prioritized and addressed by limited resources
- Many unmet responsibilities
- *Attackers exploiting vulnerabilities at all layers*

Cloud Technology enables security to:

- Shift responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use Cloud intelligence improve detection/response/time

Hyperscale Cloud Security

Prevent Breach

- Vulnerability and Update Management
- Isolation (Data, Network, Trust)
- Least Privileged/JIT Access
- Security development lifecycle (SDL)

Assume Breach

- Red vs Blue
- Live Site Penetration Testing
- Breach Hunt
- Centralized security logging & monitoring

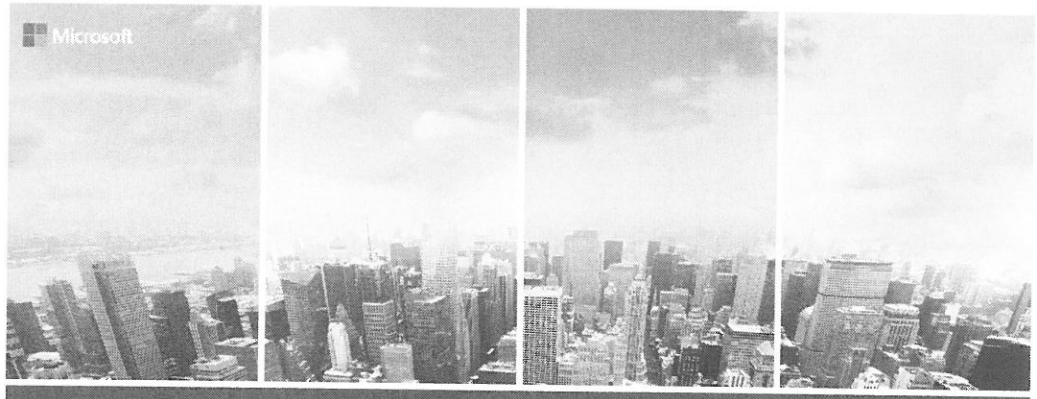
Assume breach identifies & addresses significant gaps:

- Detect attack & penetration
- Respond to attack & penetration
- Recover from data leakage or tampering

Scope **ongoing live site** testing of security response plans to drastically improve **mean time to detection & recovery**

Reduce exposure to **internal attack** (once inside, attackers have broad access)

Periodic environment **post breach assessment & clean state**



Actionable Insights Driven by Scale

Microsoft Azure Security Center

Unify security management and enable advanced threat protection for hybrid cloud workloads

Unified visibility and control

Adaptive threat prevention

Intelligent detection and response

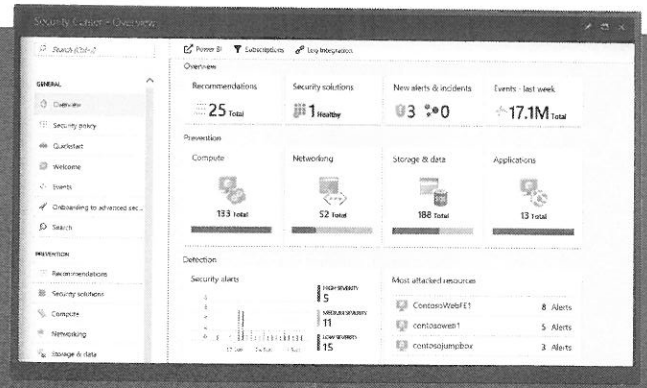
Understand security state across hybrid workloads

Built-in Azure, no setup required

- Automatically discover and monitor security of Azure resources

Gain insights for hybrid resources

- Easily onboard resources running in other clouds and on-premises



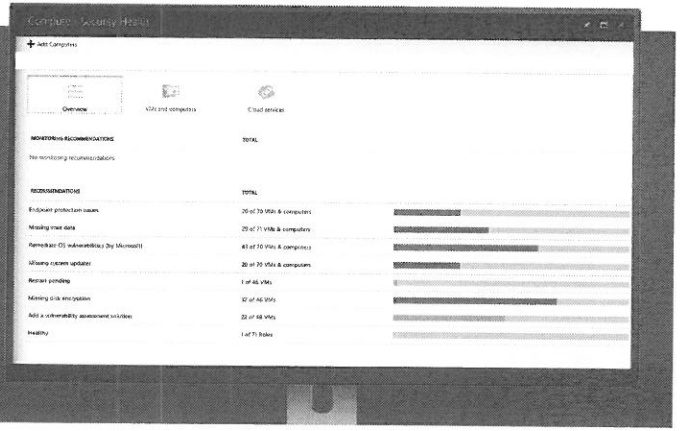
Identify and remediate vulnerabilities quickly

Continuous assessment of machines, networks, and Azure services

- Hundreds of built-in security assessments, or create your own

Fix vulnerabilities quickly

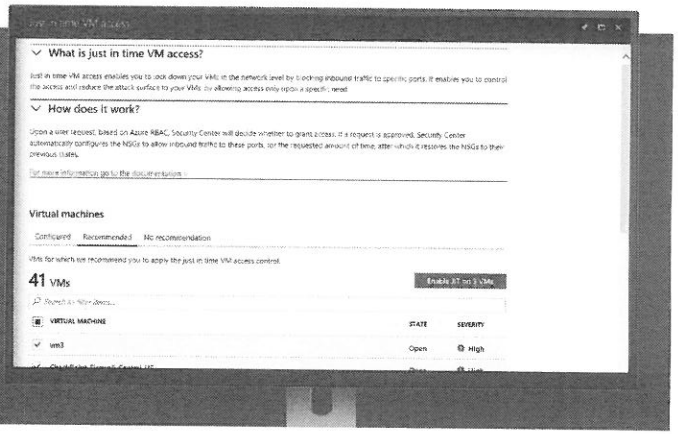
- Prioritized, actionable security recommendations



Limit exposure to brute-force attacks

Lock down ports on virtual machines

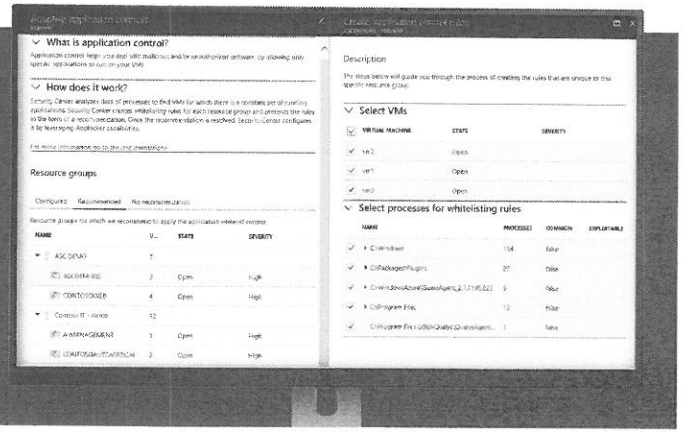
- Enable just-in-time access to virtual machines
- Access automatically granted for limited time



Block malware and other unwanted applications

Allow safe applications only

- Adaptive whitelisting learns application patterns
- Simplified management with recommended whitelists



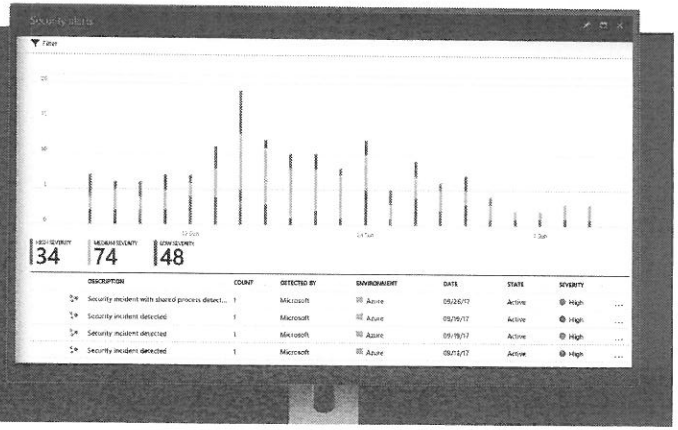
Focus on the most critical threats

Get prioritized security alerts

- Details about detected threats and recommendations

Detect threats across the kill chain

- Alerts that conform to kill chain patterns are fused into a single incident



Office 365 Advanced Threat Protection

Hackers around the globe launch increasingly sophisticated attacks

Organizations seek tools that provide advanced protection

Office 365 Advanced Threat Protection provides additional protection against specific types of advanced threats

Protection against unknown malware/viruses
- Behavioral analysis with machine learning
- Admin alerts

Time-of-click protection
- Real-time protection against malicious URLs
- Growing URL coverage

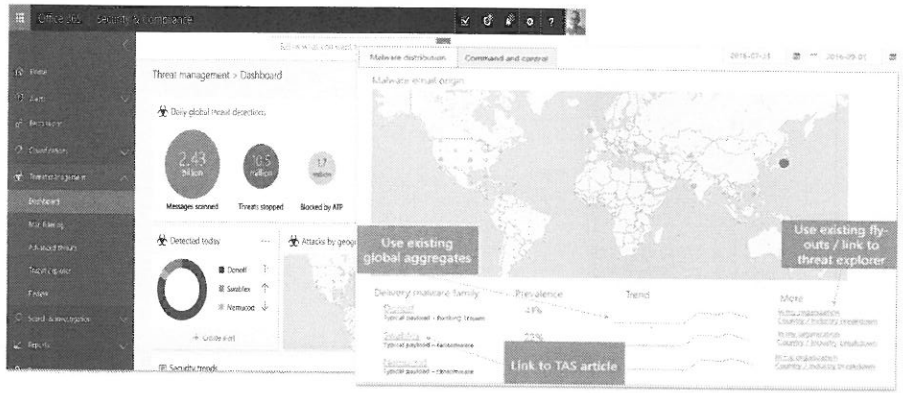
Rich reporting and tracing
- Built-in URL trace
- Reports for advanced threats

Threat Intelligence

Rich insights – Identify and correlate threats before they impact your organization

Proactive defense – Dynamic policies to protect against rapidly evolving threats

Seamless integration – Intuitive interface with connectivity to existing security systems



Threat Explorer

Trending threats, technical details, global targeting context

Advanced Compliance Capabilities

Advanced Data Governance

Leverage intelligence to automate data retention and deletion

Automatic Classification

Classify data based on automatic analysis

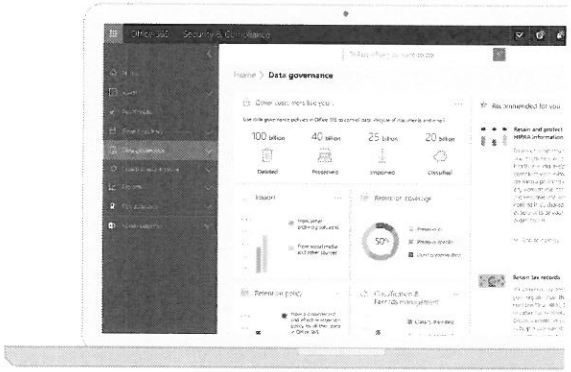
(age, user, type, sensitive data and user provided fingerprints)

Intelligent Policies

Policy recommendations based on machine learning and cloud intelligence

Take Action

Apply actions to preserve high value data in-place and purge what's redundant, trivial or obsolete



Advanced eDiscovery

Intelligently explore and analyze unstructured data to quickly identify what's relevant

Identify relevant documents

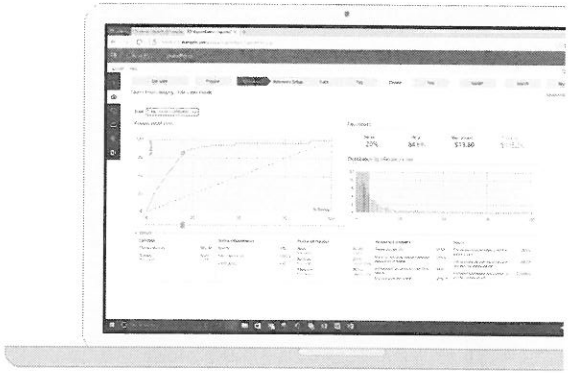
Predictive coding enables you to train the system to automatically distinguish between likely relevant and non-relevant documents

Identify data relationships

Use clustering technology to look at documents in context and identify relationships between them

Organize, reduce data prior to review

Use near duplicate detection to organize the data and reconstruct email threads from unstructured data to reduce what's sent to review



COMPLIANCE AND EDISCOVERY ECOSYSTEM

Work with Partners to help to ensure the success, usage and adoption of all O365 Compliance capabilities

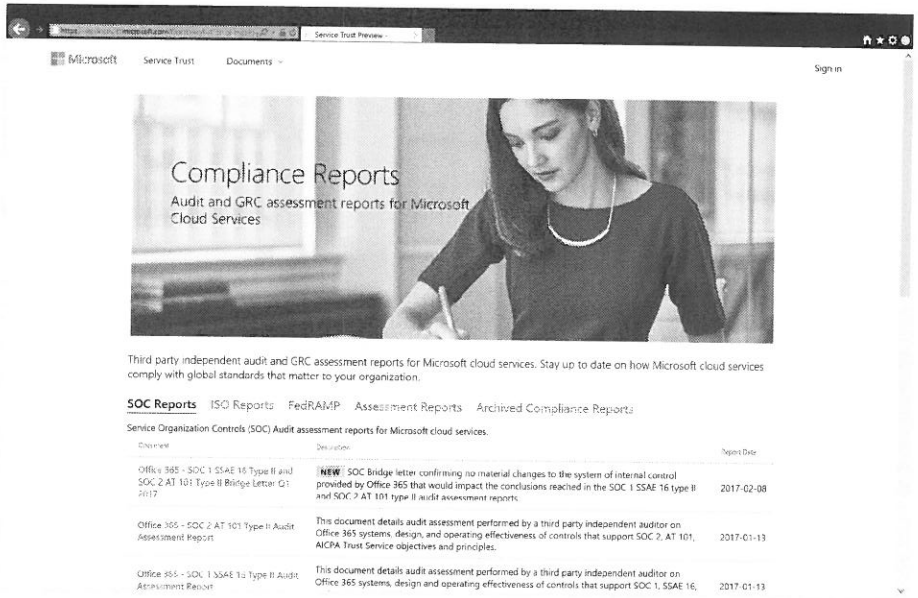
KPMG cutting through complexity
Lighthouse eDiscovery
DTI
EDGRAVE
discover ready
CONTROLO
Kroll Ontrack.
FTI CONSULTING | TECHNOLOGY
epiq SYSTEMS
The Discovery Companies
FIVE STAR LEGAL
RVM
D4 powered by people
bluesource
ADVANCED DISCOVERY
NightOwlDiscovery
WINSTON & STRAWN LLP
BRAINSTORM
Discovia Managed eDiscovery
Altep
NAVIGANT

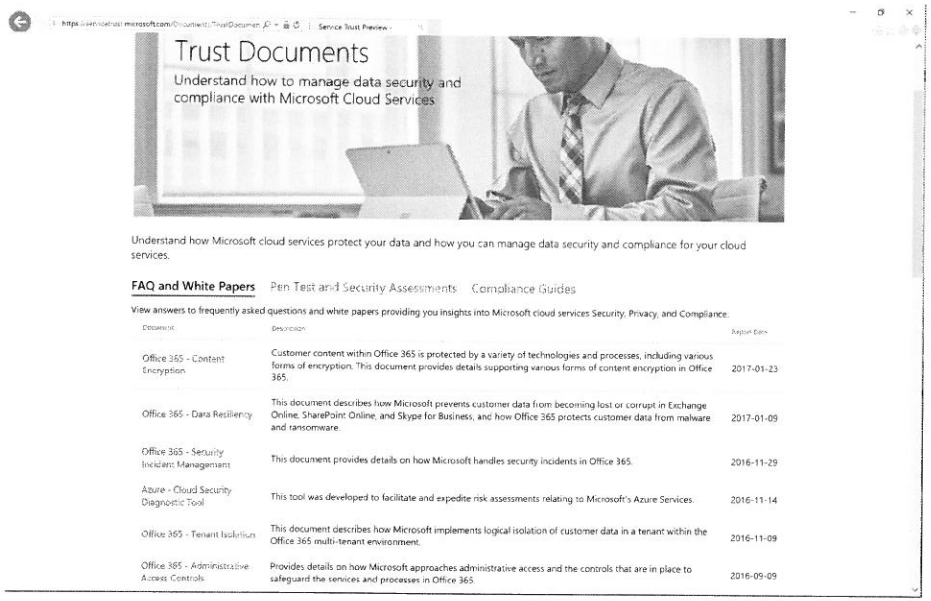
Self-Service Audit

Microsoft Online Services – Service Trust Portal

Assess
- Relevant content
- Easily discoverable
- 3rd party audits
- Responses to standard frameworks
- Deep explanation

Examine
- Browse controls
- See audit details
- Review evidence

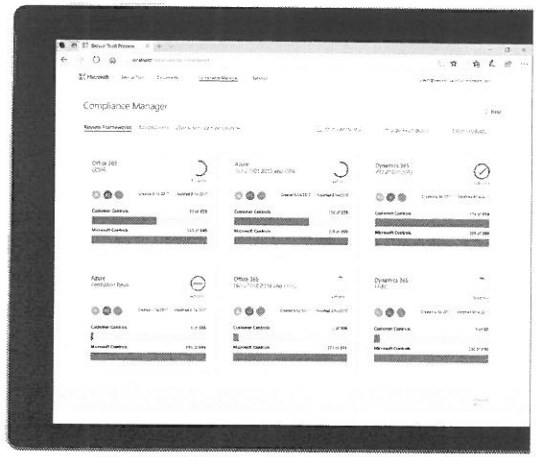


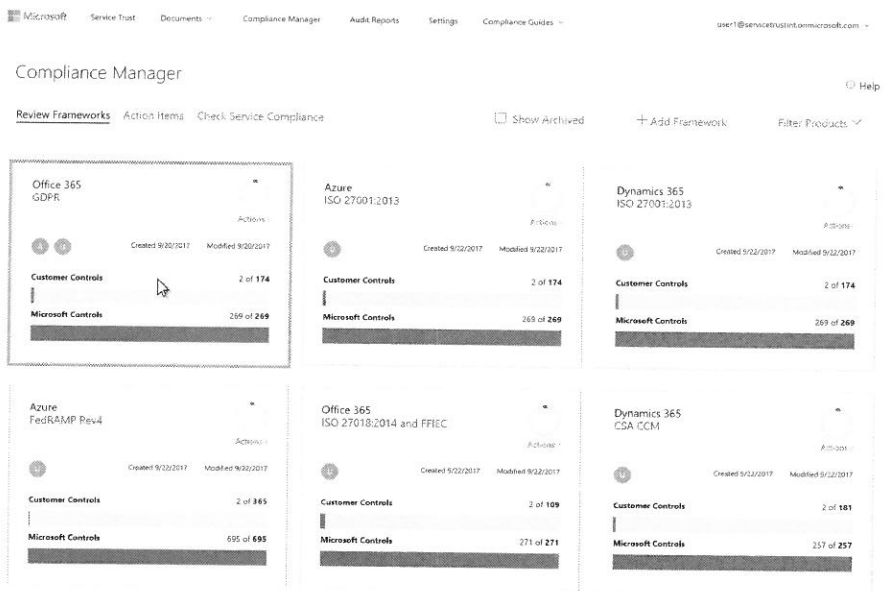


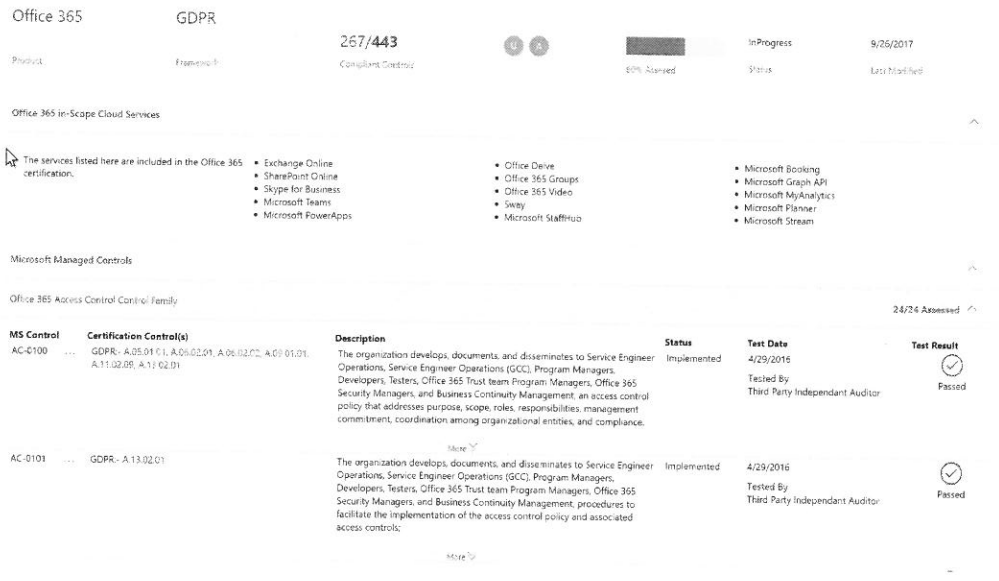
Compliance manager

Manage your compliance from one place

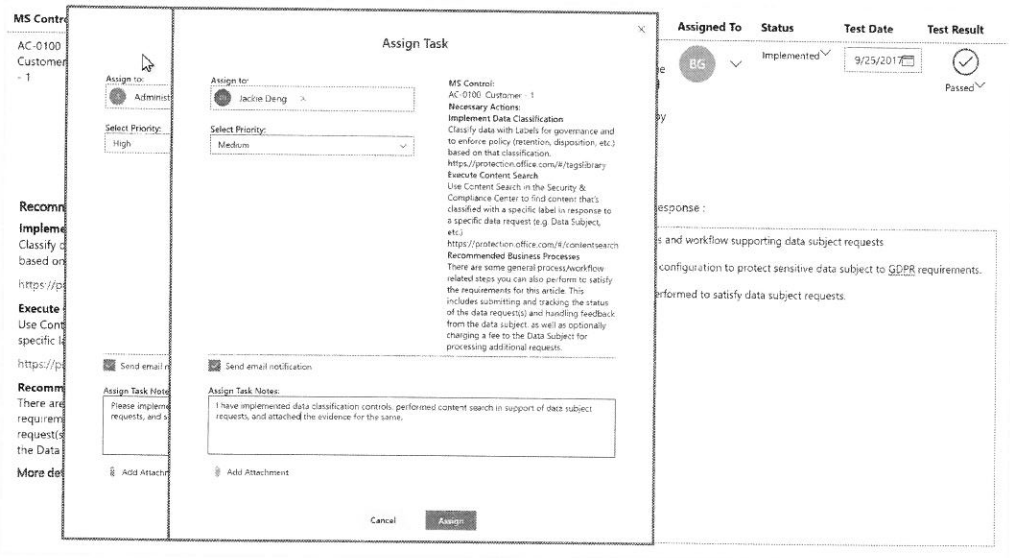
- **Real-time risk assessment**
  An intelligent score shows your compliance posture against evolving regulations
- **Actionable insights**
  Recommended actions to improve your data protection capabilities
- **Simplified compliance**
  Streamlined workflow and audit-ready reports

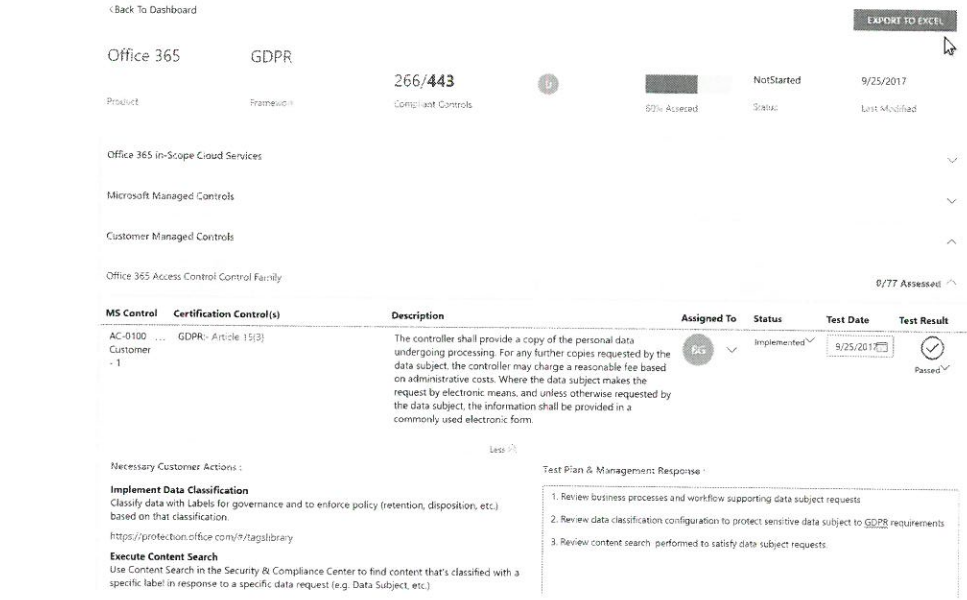



Microsoft
Service Trust
Documents
Compliance Manager
Audit Reports
Settings
Compliance Guides
user1@servicetrustint.onmicrosoft.com
Compliance Manager
Help
Review Frameworks
Action Items
Check Service Compliance
Show Archived
+ Add Framework
Filter Products
Office 365
GDPR
Created 9/20/2017
Modified 9/20/2017
Customer Controls
2 of 174
Microsoft Controls
269 of 269
Azure
ISO 27001:2013
Created 9/22/2017
Modified 9/22/2017
Customer Controls
2 of 174
Microsoft Controls
269 of 269
Dynamics 365
ISO 27001:2013
Created 9/22/2017
Modified 9/22/2017
Customer Controls
2 of 174
Microsoft Controls
269 of 269
Azure
FedRAMP Rev4
Created 9/22/2017
Modified 9/22/2017
Customer Controls
2 of 365
Microsoft Controls
695 of 695
Office 365
ISO 27018:2014 and FFIEC
Created 9/22/2017
Modified 9/22/2017
Customer Controls
2 of 109
Microsoft Controls
271 of 271
Dynamics 365
CSA CCM
Created 9/22/2017
Modified 9/22/2017
Customer Controls
2 of 181
Microsoft Controls
257 of 257


Office 365
GDPR
267/443
Compliant Controls
InProgress
9/26/2017
Status
Last Modified
Office 365 In-Scope Cloud Services
The services listed here are included in the Office 365 certification.
Exchange Online
SharePoint Online
Skype for Business
Microsoft Teams
Microsoft PowerApps
Office Delve
Office 365 Groups
Office 365 Video
Sway
Microsoft StaffHub
Microsoft Booking
Microsoft Graph API
Microsoft MyAnalytics
Microsoft Planner
Microsoft Stream
Microsoft Managed Controls
Office 365 Access Control Control Family
24/24 Assessed
MS Control
Certification Control(s)
Description
Status
Test Date
Test Result
AC-0100
GDPR:- A.05.01.01, A.05.02.01, A.06.02.02, A.09.01.01, A.11.02.09, A.13.02.01
The organization develops, documents, and disseminates to Service Engineer Operations, Service Engineer Operations (GCC), Program Managers, Developers, Testers, Office 365 Trust team Program Managers, Office 365 Security Managers, and Business Continuity Management: an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
Implemented
4/29/2016
Tested By
Third Party Independent Auditor
Passed
More
AC-0101
GDPR:- A.13.02.01
The organization develops, documents, and disseminates to Service Engineer Operations, Service Engineer Operations (GCC), Program Managers, Developers, Testers, Office 365 Trust team Program Managers, Office 365 Security Managers, and Business Continuity Management, procedures to facilitate the implementation of the access control policy and associated access controls;
Implemented
4/29/2016
Tested By
Third Party Independent Auditor
Passed
More


More
AC-0153
FedRAMP Rev4:- AC-06(10)
The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
Implemented
4/29/2016
Tested By
Third Party Independent Auditor
Passed
More
AC-0154
FedRAMP Rev4:- AC-07(a)
The information system enforces a limit of 5 consecutive invalid login attempts by a user during a 15-minute period.
Implemented
4/29/2016
Tested By
Third Party Independent Auditor
Failed-Low Risk
Less
Microsoft Implementation Details :
Microsoft has implemented an account lockout for Office 365 of 5 failed attempts in 15 minutes, rather than the FedRAMP value of 3 failed attempts in 15 minutes, using Active Directory Group Policy. Microsoft has adopted this alternative implementation as an operational requirement of Office 365 in order to ensure system availability, especially during non-business hours.
Microsoft believes that the more restrictive value of 3 attempts exposes a risk to the availability of the system. Operational experience has shown that on-call personnel may inadvertently lock themselves out during non-business hours, resulting in delayed service response times.
Microsoft's internal risk evaluations found that account lockout after 5 failed attempts in 15 minutes provides the best balance of risk from the threat of account breaches against risk of delayed service response times. Also, allowing 3
Read More
Test Plan Details :
Examined the Microsoft Office 365 Multitenant System Security Plan Version 3.01, dated May 13, 2016 and determined that Microsoft defines the organizational value as 10 failed attempts in 15 minutes, rather than the FedRAMP value of 3 failed attempts in 15 minutes, using Active Directory Group Policy. Microsoft has adopted this alternative implementation as an operational requirement of Office 365 in order to ensure system availability, especially during non-business hours.
Examined the Microsoft Office 365 Multitenant System Security Plan Version 3.01, dated May 13, 2016 and determined that Microsoft defines the organizational value as 10 failed attempts in 15 minutes, rather than the FedRAMP value of 3 failed attempts in 15 minutes, using group policy. Microsoft has adopted this alternative implementation as an operational requirement of Office 365 in order to ensure system availability, especially during non-business hours.
Read More
Management Response :
The FedRAMP Organizational Defined Values require accounts to be locked after three failed access attempts within fifteen minutes. Workload threat modeling indicates that the risk of a denial-of-service that negatively affects system availability as a result of locking admin accounts exceeds the risk of loss of system confidentiality due to multiple failed login attempts. Workloads log and alert off of excessive failed login attempts and can take manual actions to prevent brute force access attempts even if the account does not automatically lock.
Microsoft believes that the more restrictive value of 3 attempts exposes a risk to the availability of the system. Operational experience has shown that on-call personnel may inadvertently lock themselves out during non-business hours, resulting in delayed service response times.
Microsoft's internal risk evaluations found that account lockout after up to 10 failed attempts in 15 minutes provides
Read More
AC-0155
FedRAMP Rev4:- AC-07(b)
The information system automatically locks the account for 30 minutes; locks the account/node until released by an administrator; delays next login prompt according to Active Directory group policy when the maximum number of unsuccessful attempts is exceeded.
Implemented
4/29/2016
Tested By
Third Party Independent Auditor
Passed
More


MS Contro
AC-0100
Customer
- 1
Assign Task
Assign to:
Administ
Select Priority:
High
Assign to:
Jackie Deng
Select Priority:
Medium
MS Control:
AC-0100 Customer - 1
Necessary Actions:
Implement Data Classification
Classify data with Labels for governance and to enforce policy (retention, disposition, etc.) based on that classification.
https://protection.office.com/#/tagslibrary
Execute Content Search
Use Content Search in the Security & Compliance Center to find content that's classified with a specific label in response to a specific data request (e.g. Data Subject, etc.)
https://protection.office.com/#/contentsearch
Recommended Business Processes
There are some general process/workflow related steps you can also perform to satisfy the requirements for this article. This includes submitting and tracking the status of the data request(s) and handling feedback from the data subject as well as optionally charging a fee to the Data Subject for processing additional requests.
Send email notification
Assign Task Notes:
I have implemented data classification controls, performed content search in support of data subject requests, and attached the evidence for the same.
Add Attachment
Cancel
Assign
Assigned To
Status
Test Date
Test Result
BG
Implemented
9/25/2017
Passed
esponse :
s and workflow supporting data subject requests
configuration to protect sensitive data subject to GDPR requirements.
erformed to satisfy data subject requests.

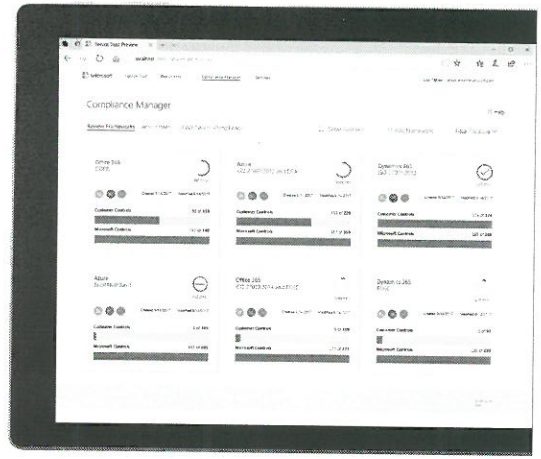


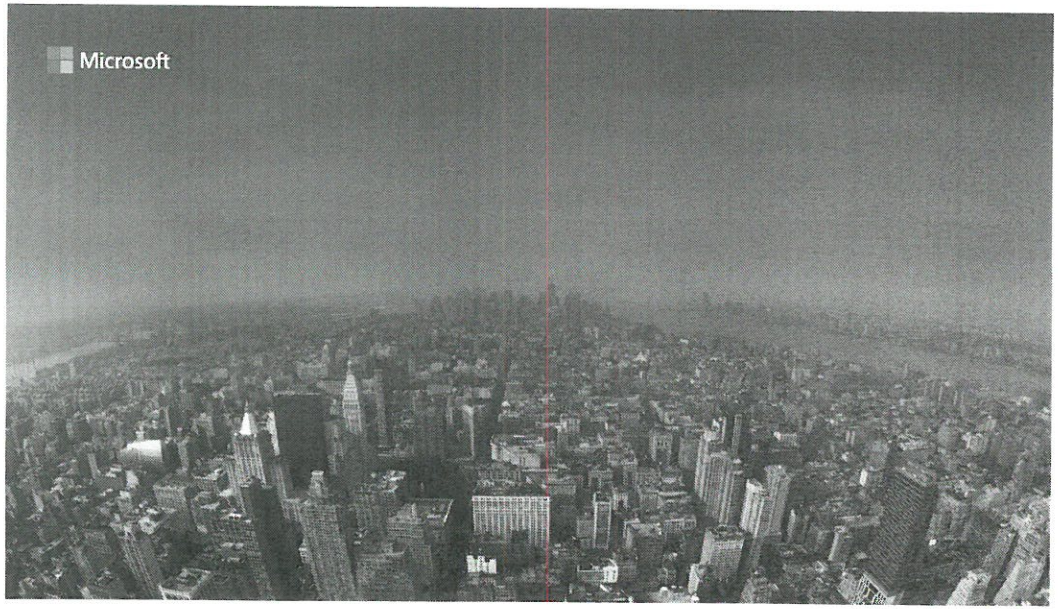
Compliance manager

Manage your compliance from one place

- **Real-time risk assessment**
  An intelligent score shows your compliance posture against evolving regulations
- **Actionable insights**
  Recommended actions to improve your data protection capabilities
- **Simplified compliance**
  Streamlined workflow and audit-ready reports

Compliance Manager Preview is a dashboard that provides a summary of your data protection and compliance posture and recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate its effectiveness in your regulatory environment prior to implementation. Recommendations from Compliance Manager Preview should not be interpreted as a guarantee of compliance.



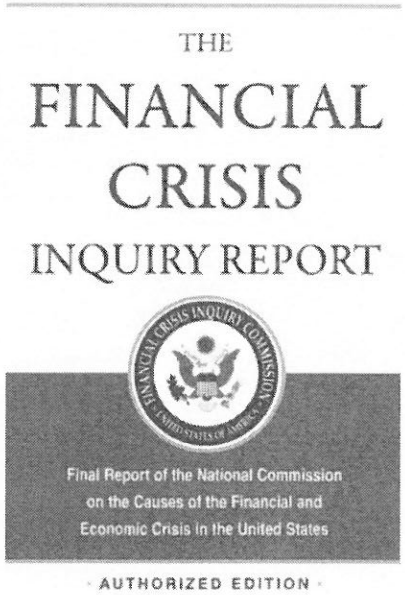


What are Challenges in Cloud Adoption

- Fear of no control
- Uncertainty about regulation
- Doubts about Assurance

- Educate on controls
- Clarity on regulation
- Transparency on assurance

TRUST



Learnings from the Great Recession

- Financial institutions highly leveraged subprime mortgages leading to economic collapse
- Lack of regulation spurred undue risk
- Corporate governance, controls and risk assurance did not adequately address warning signs
- Minimal transparency contributed to crisis
- Information technology played no contributing role
- Key regulators saved the world economy from utter destruction

Cloud and Risk Management

Cloud Can Improve Risk Assurance and Compliance

"The cloud makes it possible to do things analytical, related to cybersecurity that were never before possible" David Burg, Global Cybersecurity Leader at PwC

Cloud solutions

- Anti-Money Laundering
- Immutability
- Document Retention/Holds
- Block Chain
- Risk Modeling
- Payments/Open APIs
- Artificial Intelligence
- Hybrid

Managing risk

- Multi-Factor Authentication
- RBAC
- Geo Footprint and Infrastructure
- Data Resiliency
- Continuous Innovation
- Cybersecurity Investments
- Transparency
- Data Portability/Interop

Regulatory Approaches: Enabling Compliance Based on Existing Frameworks

Risk Assurance Framework

Security	Privacy	Compliance	Transparency
Service provider reputation and competence	Limits on data use and access	Confidentiality	Audit & inspection
Resilience and business continuity	Conditions on subcontracting	Security standards	Data location
Data segregation/isolation	Conditions on termination	Review, monitoring & control	Documentation

Compliance

Regulator Right to Inspect

Regulators need full visibility into all the services used and operated by their supervised institutions

Financial institutions compliance

Financial institutions must assess and manage the services they use – they cannot outsource their accountability

Contractually committed

These capabilities need to be mirrored in contracts meeting their unique compliance requirements

Addressing compliance requirements in the

Benefits of Scale

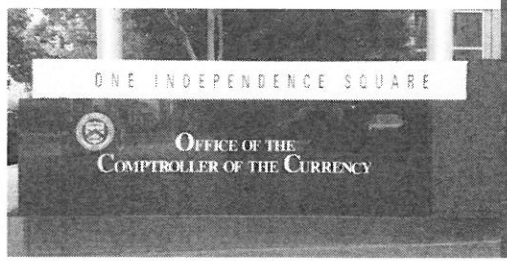
For all Customers	For all FSIs	Optional Program for FSIs	On Demand
▪ Privacy, Security, and Data Processing commitments including EU Model Clauses ▪ Access to Audit Reports ▪ Commit to location of customer data at rest ▪ Protections against unauthorized access ▪ Compliance with industry standards	▪ Regulator Right to Examine ▪ Contractual Right to the Compliance Program ▪ Regulatory Changes and Termination Rights ▪ Business Continuity	▪ Additional access to information: - Audit Webcasts & Annual Summit - Risk Register & Control Framework - Advanced Roadmap - Security Incident Reviews ▪ Access to Microsoft compliance and security experts & external auditors ▪ Ability to influence via future audit scope	▪ Right to Audit ▪ Physical Data Centers ▪ Interview Engineers and Engineering Leadership ▪ Inspect Audit Evidence ▪ Request New Evidence
Online Service Terms	FSI Amendment	Compliance Program	Audit

Regulatory Trends in Adapting to the Cloud

Regulatory trends: cybersecurity & vendor management

"Responsible innovation among banks should help them fulfill their public purpose by promoting fair access to financial services and fair treatment of consumers."

– Office of the Comptroller of Currency March, 2016



Regulatory themes

- Openness to cloud
- Support of innovation
- Improvements in transparency
- Accountability
- Oversight of cloud vendors

Comparative Approaches – Rules v. Principles

Rules – Focused on the How

- Prescriptive on managing risk
- Favor legacy systems
- Data localization prescribed
- Restricted in time

Examples:

- Bangladesh – Fire extinguisher placement "shall be placed..."
- Brazil – Data storage "forbidden" abroad (DRAFT)

Principles -- Focused on the What

- Outcomes on managing risk
- Technology neutral
- Offshoring measured by risk
- Adaptive and flexible

Examples:

- FFIEC – Fire suppression "should address risks"
- Singapore – Offshoring "should take into account risks"

Cloud Considerations

1. Prescriptive Guidance

Cloud Technology is very different and is moving rapidly. Key to focus on Outcomes rather than Methods.

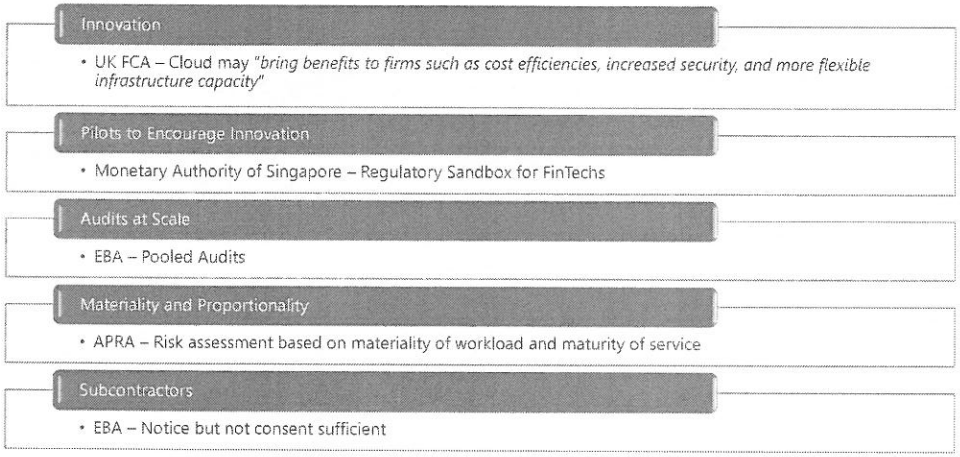
2. Data Localization

Data localization limits innovation as datacenters won't be in every country. Key is security, not where data is stored.

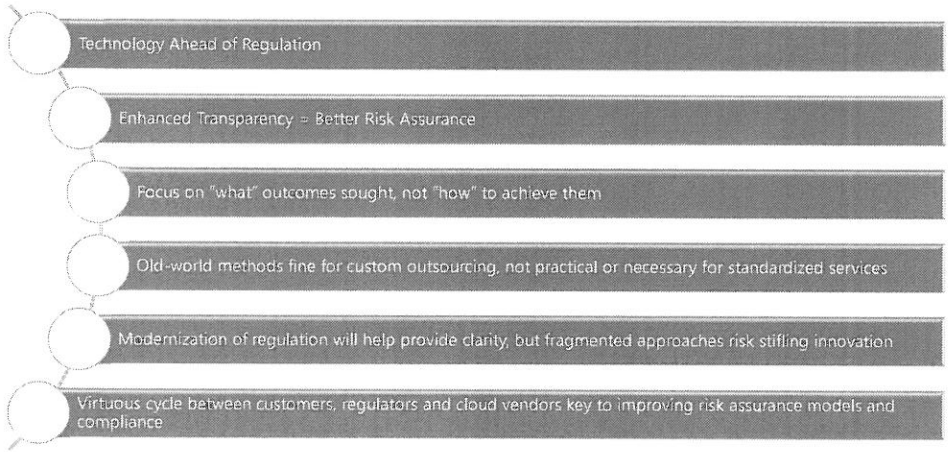
3. Compliance cannot be manual

Compliance can be accomplished through automation and self-help tools. Audit, evidence and assurance needs to be available at scale.

Adapting to the Cloud without Compromising on Risk Assurance



Learnings Designed to Improve Risk Assurance



A Path Forward to Modernization

Adapting Principles for the Cloud

Risk Assessments and Due Diligence

FIs must carry out, and CSPs must assist in facilitating, a risk assessment and due diligence on the CSP to ensure that the CSP and its Cloud Services meet the legal, regulatory, contractual and business requirements. FIs should have in place a risk management plan that includes measures to address the risks associated with the use of Cloud Services. **Need: Standardized approach on risk assessments.**

Review, Monitoring, and Control (Audit)

CSPs must provide FIs and applicable Financial Regulators with audit rights. CSPs must provide regular reporting and information to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the contract. Self-help tools and underlying evidence available through dashboards and portals should be sufficient to help address supervisory needs at scale.. The contract must provide for an effective mechanism for remedial actions arising from any issues that emerge concerning non-compliance. **Need: Monitoring at Scale.**

Confidentiality and Certified Security Standards

CSPs must be certified to have and maintain robust security measures and comprehensive security policies that meet or exceed international standards (ISO27001 accreditation should be a minimum). CSPs should use encryption technology that meets or exceeds international standards to protect and secure the FI's Data at all times.

The Trusted Cloud Principles for FSI

Resilience and Business Continuity

The Cloud Service must be reliable. CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives and with regularly tested and updated procedures and systems in place to meet those objectives. The risks of downtime should be minimized through good planning and a high degree of system resilience.

Data Location and Transparency

CSPs must provide transparency in which regions Data will be located. FIs should ensure that the government policies, economic and legal conditions of the identified locations are safe and stable. **Need: Clarity on regulation concerning data location.**

Limits on Data Use

CSPs should not use FI's Data for any purpose other than that which is necessary to provide the Cloud Service, such as advertising. Using telemetry data to improve the service, including enhancing security is consistent with permissible uses.

Data Isolation

FI Customer Data must be isolated from other Data held by the CSPs. .

The Trusted Cloud Principles for FSI

Conditions on Subcontracting

CSPs may only use subcontractors if the subcontractors are subject to privacy and security requirements with contractual commitments that are no less protective than provided by the CSP. **Need: Assurance through CSP and flow-down of commitments to subcontractor.**

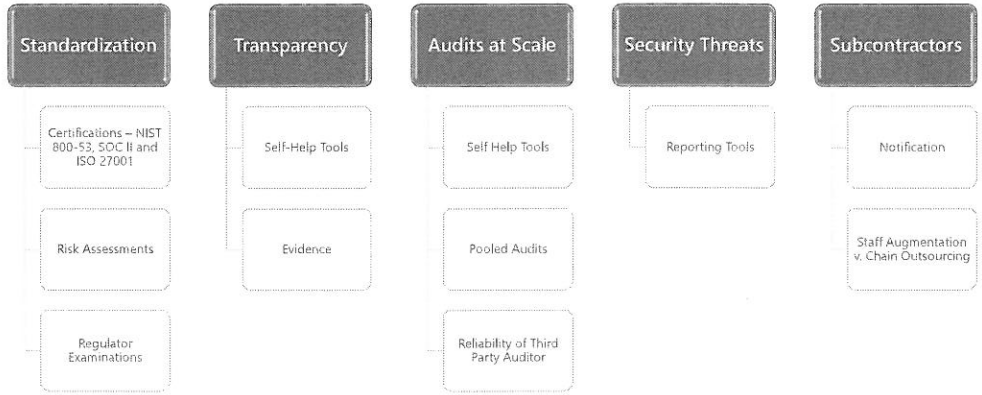
Conditions on Termination

FIs must have appropriate exit provisions in the contract with the CSP. To the extent that the FI requires, on termination, the CSP must work with the FI to return the FI's Data to the FI and then the CSP must permanently delete the Data from the CSP's systems. Any Data that does not need to be returned to the FI must be permanently deleted by the CSP.

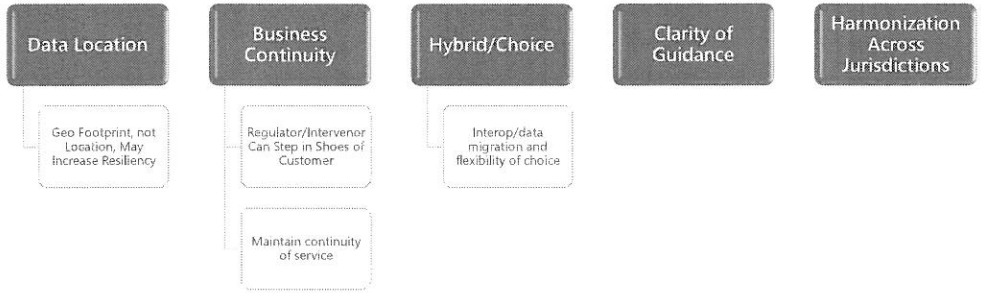
Flexibility and Hybrid Solutions

CSPs must provide appropriate flexibility for FIs to house workloads on premise or in the cloud as necessitated by data classification, business policy and regulatory requirements.

Principles Adaptive to Cloud but Consistent with Risk Assurance Obligations and Standards



Principles adaptive to cloud but consistent with risk assurance obligations



A Path Forward – Working Together

- Role of CSPs?
  - Education
  - Tools and Self-Help Resources
  - Standardized Risk Assessments
- Role of Industry?
  - Governance Councils/Pooled Audits
  - Standardized Risk Assessments
- Role of Regulators?
  - Harmonization
  - Clarity of Guidance
  - Consistent/Standardized/Pooled Examinations
  - Education

Resources

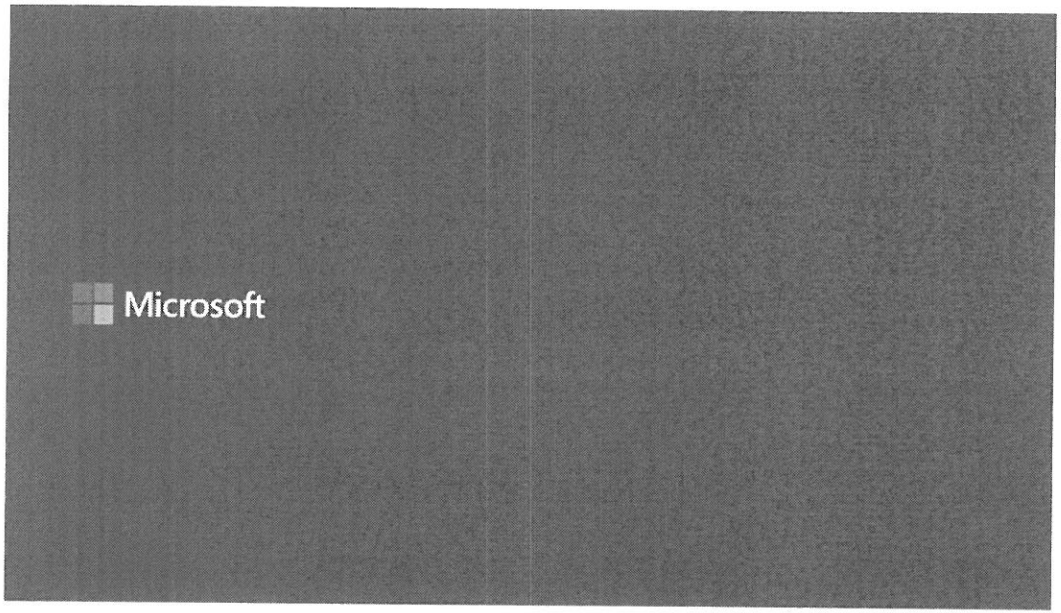
- Australian Prudential Regulation Authority - Information Paper - Outsourcing involving shared computing services (including cloud)
- Monetary Authority of Singapore - Guidelines on Outsourcing Risk Management
- Financial Conduct Authority - FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third-party IT services
- European Banking Authority - Guidance for the use of cloud computing

FCA FINANCIAL CONDUCT AUTHORITY

APRA Australian Prudential Regulation Authority

EBA European Banking Authority

MAS Monetary Authority of Singapore



Risk assessment: Questions we expect banks to ask

Accountability	Partnership with cloud vendor	Reputation	Audits	Security Controls
Legal and regulatory compliance Clarity of commitments on responsibility of parties	Managing the relationship Transparency of controls, SLAs, and commercial commitments Due diligence (including appropriate documentation) Board review	Capability Enterprise ready History	ISO 27001 SOC 1 and 2/SSAE16 ISO 27018 Frequency of audits Commit on audits	Authentication Access controls Physical security Strict limits on use of data Security incident management Encryption Logical separation of data Security policies

Risk assessment: Questions we expect banks to ask

Contingency Plans	Transparency	Supervision	Control	Flexibility
Disaster recovery Business continuity Termination and exit plan Data deletion and retention	Data location Subcontractors Audit reports FS-ISAC cybersecurity threat information sharing Penetration test reports	Documentation and reports Regulator examination rights Customer examination rights Access to subject matter experts	Admin controls Influence controls Penetration testing Remediation	Private Hybrid Public Cloud

Commitments: Consumer v. Enterprise

Commitment	Consumer	Enterprise
Privacy and Control	No ISO 27018 Use of data -- ads Law enforcement – no notice	ISO 27018 Use of data – no ads Law enforcement -- redirect & notice
Terms of Use	IP --Data ownership and use Financial Liability-- none Termination– Any time Change to Terms of Service – No notice Data deletion -- none Data retention – none SLA -- None	IP – Ownership by customer Financial Liability -- Significant Termination: Transition & Notice Change to Terms of Service – None Data deletion – 180 days Data retention – 90 days SLA – Commit with financial backing
Security	Basic encryption	ISO 27001, SOC 1 and SOC 2 Security policies Security Incident Notification Access control & authorization
Compliance	None	Access to audit reports Commitment on audit cycle (annually) Regulatory – Financial Services
Transparency	Basic	Subcontractors Data location

A Brazilian Financial Regulatory Approach to Information Technology Outsourcing Services / Cloud Based Services

Carlos André de Melo Alves
carlos.demelo@bcb.gov.br

Committee on Credit Rating Agencies (Committee 6)
December – 2017 - Rio de Janeiro - Brazil

Note

- All opinions expressed in this presentation must be credited to the author and do not necessarily reflect the institutional position of the Banco Central do Brasil.

Index

- Introduction (Brazilian Financial System and Banco Central do Brasil).
- Examples of Selected International Recommendations About Information Technology (IT) Outsourcing Services / Cloud Based Services.
- Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell).
- Concluding Remarks.

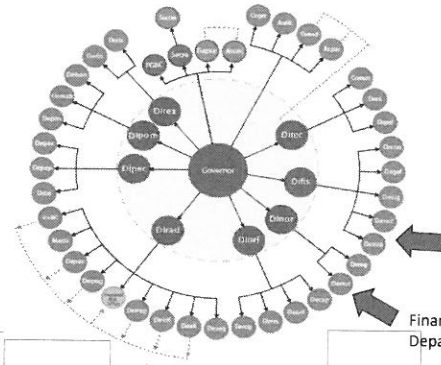
Brazilian Financial System – An Overview

- In October, 2017, the National Financial System was composed of 1.754 institutions:
  - 560 institutions (coverign banking financial institutions - FIs, non banking FIs and payment institutions);
  - 1.037 credit unions; and
  - 157 consortium managers.

Banco Central do Brasil (BCB) - Mission

- To ensure the stability of the currency's purchasing power and a solid and efficient financial system.
- The mission to ensure a solid and efficient financial system is accomplished through:
  - Regulation activities; and
  - Supervision activities (covering banking FIs, non banking FIs and credit unions).

BCB – Organization Chart



Source: BCB (2017)

Examples of International Recommendations about IT Outsourcing Services / Cloud Based Services

- IT outsourcing services and cloud based services can offer a lot of benefits to the FIs (cost reduction, for example).
- However, IT outsourcing services and cloud based services can bring new sources of risks to the FIs (for example, the high dependence of a third-party provider).
- Considering these issues as a part of international financial regulatory agenda, it is necessary to verify examples of international recommendations addressing IT outsourcing services / cloud based services.

Examples of International Recommendations about IT Outsourcing Services / Cloud Based Services

- ***Outsourced Cloud Computing***
  - Issued by Federal Financial Examination Council - FFIEC (2012);
- ***Technology Risk Management Guidelines***
  - Issued by Monetary Authority of Singapore – MAS (2013);
- ***Secure Use of Cloud Computing in the Finance Sector***
  - Issued by European Union Agency For Network And Information Security - ENISA (2015);

Examples of International Recommendations about IT Outsourcing Services / Cloud Based Services

- ***Guidelines on Outsourcing***
  - Issued by Monetary Authority of Singapore – MAS (2016); and
- ***Cross Industry Guidance in Respect of Information Technology and Cybersecurity Risks***
  - Issued by the Central Bank of Ireland (2016).

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- The issues related to IT outsourcing services / cloud based services are treated in a generic way, based on financial regulation that discipline operational risk management.
- Considering the mentioned international recommendations about IT outsourcing services and cloud based services, the relevance of cybersecurity issues in an international context and BCB internal discussions, it was elaborated a proposal of resolution.
- This proposal was approved by the BCB Board of Directors according to the Public Consultation 57, 9/19/2017.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- The regulatory proposal cover two main subjects:
  - The establishment of cibersecurity policy in FIs; and
  - **Minimum requirements for IT outsorcing services (data processing/data storage) and cloud based services.**
- This regulatory proposal is not applied to payment institutions and consortium managers.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- FIs are responsible for the **reliability, integrity, availability, security and confidentiality** of contracted services.
- FIs are responsible for **complying with applicable laws and regulations**.
- FIs must adopt **governance and risk management practices** in proportion to the outsourced services.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- Outsourcing contracts shall contain **minimum requirements**, including:
  - **the location** where the data will be stored, processed and managed; and
  - the **security measures** if such data is transmitted and stored.
- In addition, the contracts' clauses must ensure the **due diligence of the FI** in the third party provider, as well as the **BCB access** to the third party provider installations.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- It is forbidden to outsource the relevant processing, data storage services and cloud based services abroad.
- On this point, **the evaluation of public consultation feedback** will comprise arguments / conditions for revision / adjustment of the proposal previously cited.
- The FIs must mantain, in Brazil, **a copy of the data and information** available for BCB access.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- **Business Continuity Issues:**
  - FIs should set **procedures in the event of disruption of the relevant IT outsourced service / cloud based service**; and
  - FIs should test scenarios covering **the replacement of the third party service provider**.
- Regarding the **cybersecurity policy initiatives**, FIs should register the cybersecurity incidents related to the **outsourced services**.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- **BCB may establish:**
  - **certification requirements** related to IT outsourced services and cloud based services; and
  - **other technical requirements and operational procedures** for compliance with the proposed Resolution.
- Proposal of validity: **180 days** after publication of Resolution.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- **Where we are:**
  - The public consultation closed on November 21th, 2017.
  - More than 76 comments / suggestions were received from the society (public and private sector), including:
    - FIs and their associations;
    - IT third party providers (including cloud services providers);
    - lawyers specialists, IT/security specialists; and
    - academics.

Brazilian Regulatory Approach to IT Outsourcing Services and Cloud Based Services (in a nutshell)

- **Next Steps**
  - All comments and suggestions are being processed in order to improve a revised proposal of regulation.
  - This revised proposal will be examinated by the Board of the BCB.
  - Finally, the final proposal will be sent to the examination of the National Monetary Council.

Concluding Remarks

- The Banco Central do Brasil stimulates all kind of technology innovation, in order to increase the efficiency of the Brazilian Financial System.
- As a financial regulator, the Banco Central do Brasil also observes issues related to stability of the Brazilian Financial System, including IT outsourcing services and cloud based services.

References

- BCB. Banco Central do Brasil. **Organizational structure**. 2017. Accessed: 11/30/2017. Available at:
- http://www.bcb.gov.br/en/#!/n/ORGSTRUCTURE.
- ENISA. European Union Agency For Network And Information Security. **Secure Use of Cloud Computing in the Finance Sector.** 2015. Accessed: 12/02/2017. Available at: https://www.enisa.europa.eu/publications/cloud-in-finance/at_download/fullReport .
- FFIEC. Federal Financial Examination Council. **Outsourced Cloud Computing.** 2012. Accessed: 12/03/2017. Available at: https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

References

- IRELAND. Central Bank of Ireland. **Cross Industry Guidance in Respect of Information Technology and Cybersecurity Risks.** 2016. Accessed: 12/1/2017. Available at: https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2
- MAS. Monetary Authority of Singapore. **Guidelines on Outsourcing.** 2016. Accessed: 12/01/2017. Available at:
- http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf.

References

- MAS. Monetary Authority of Singapore. **Technology Risk Management Guidelines**. 2013. Accessed: 12/02/2017. Available at:
- http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf.

A Brazilian Financial Regulatory Approach to Information Technology Outsourcing Services / Cloud Based Services

Carlos André de Melo Alves

carlos.demelo@bcb.gov.br

Committee on Credit Rating Agencies (Committee 6)

December – 2017 - Rio de Janeiro - Brazil