A Flexible and Comprehensive Approach to a Cloud Compliance Program

Stuart Aston
Microsoft UK

Session ID: SPO-201
Session Classification: General Interest

RSA CONFERENCE EUROPE 2012

Compliance in the cloud

Transparency

Responsibility

Partnership

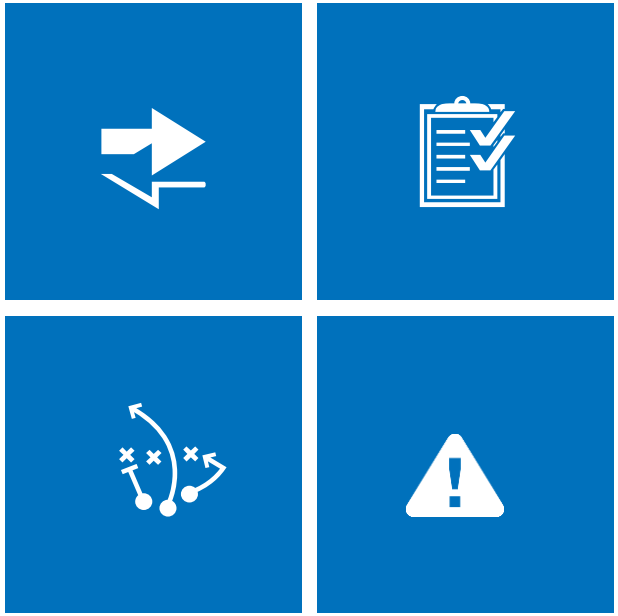
Security

Cloud Compliance Requirements

RSA CONFERENCE EUROPE 2012

Cloud Security Challenges

- Growing interdependence
- Complex, global regulatory requirements and industry standards
- Evolving technologies, changing business models, dynamic hosting environment
- Fear of increasing sophistication of attacks



Frequently requested compliance domains

ISO 27001	SAS 70 / SSAE 16	EU Model Clauses
Personal Information EU Safe Harbour	Industry Specific (PCI / HIPAA-HITECH)	Government Specific (G-Cloud, NIST 800)

Commitment to Transparency Through STAR

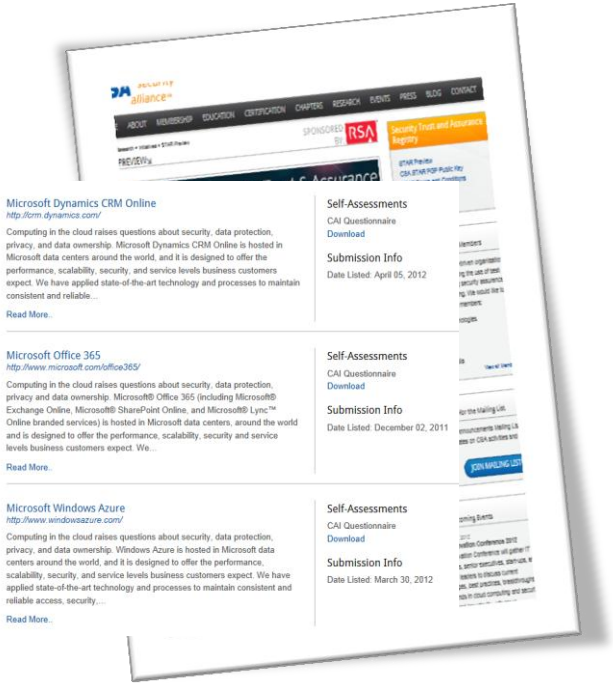
Standard from the Cloud Security Alliance (CSA)

The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Office 365 Security Response in the Context of the CSA Cloud Control Matrix
Controls CO-01 through CO-03

Control ID in CCM	Description (CCM Version 01.1- Final)	Microsoft Response
CO-01 Compliance - Audit Planning	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	Our goals are to operate our services as securely as possible, and to give you accurate assurances about our security. We have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Each year, we undergo third-party audits by internationally recognized auditors to validate that we have independent attestation of compliance with our policies and procedures for security, privacy, continuity and compliance. Audit reports are available under NDA upon request. Monitor and review the Information Security Management System (ISMS) is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.3, for more information review of the publically available ISO standards we are certified against is suggested.
CO-02 Compliance - Independent Audits	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	For more information see CO-01 or the Trust Center for our current certifications and third party attestations.
CO-03 Compliance - Third Party Audits	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	Microsoft Online Services contractually requires third parties to maintain equivalency with Microsoft Online Services Information Security Policy. In addition, Microsoft Online Services requires that third parties undergo an annual third party audit or arrange to be included in Microsoft Online Services annual third party audit. Addressing security in third party agreements and third party service delivery management is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2 and 10.2, for more information a review of the publically available ISO standards we are certified against is suggested.

Microsoft



Microsoft's Standard Responses on STAR!

Specific details about Office 365, Windows Azure and Dynamics CRM Security and Privacy is mapped to the CCM and the ISO certifications

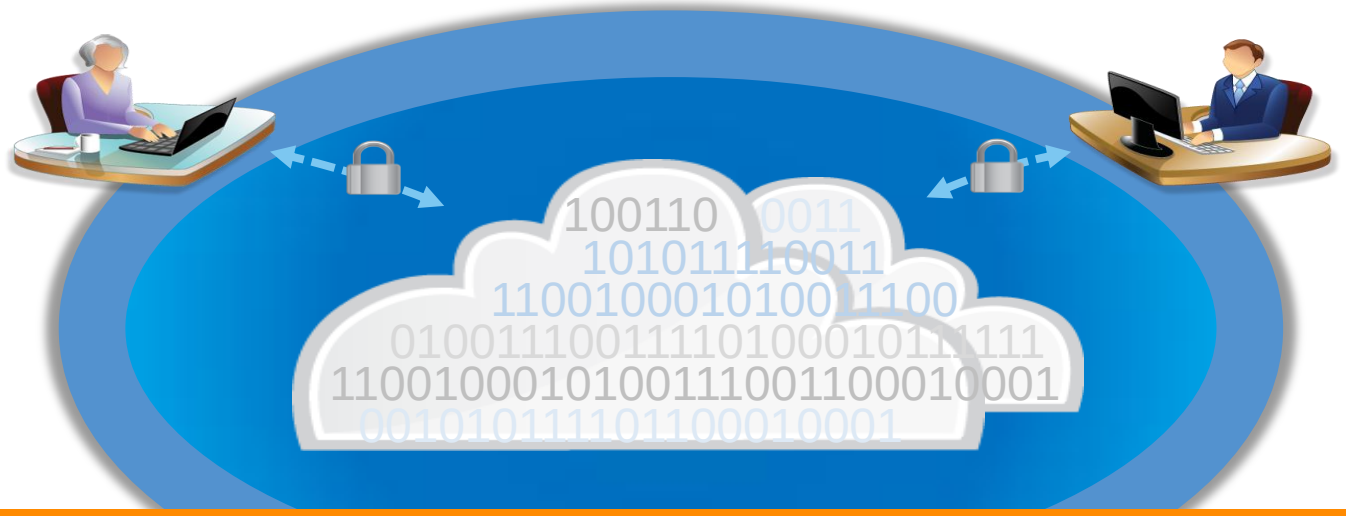
Example: Cloud Security Alliance

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
DG-01 Data Governance - Ownership / Stewardship	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	Microsoft Online Services has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Online Services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. "Allocation of information security responsibilities and ownership of assets" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.1.3 and 7.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.
DG-02 Data Governance - Classification	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.	Microsoft Online Services standards provide guidance for classifying assets of several applicable security classification categories, and then implements a standard set of Security and privacy attributes. "Information classification" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Harmonising Cloud Compliance

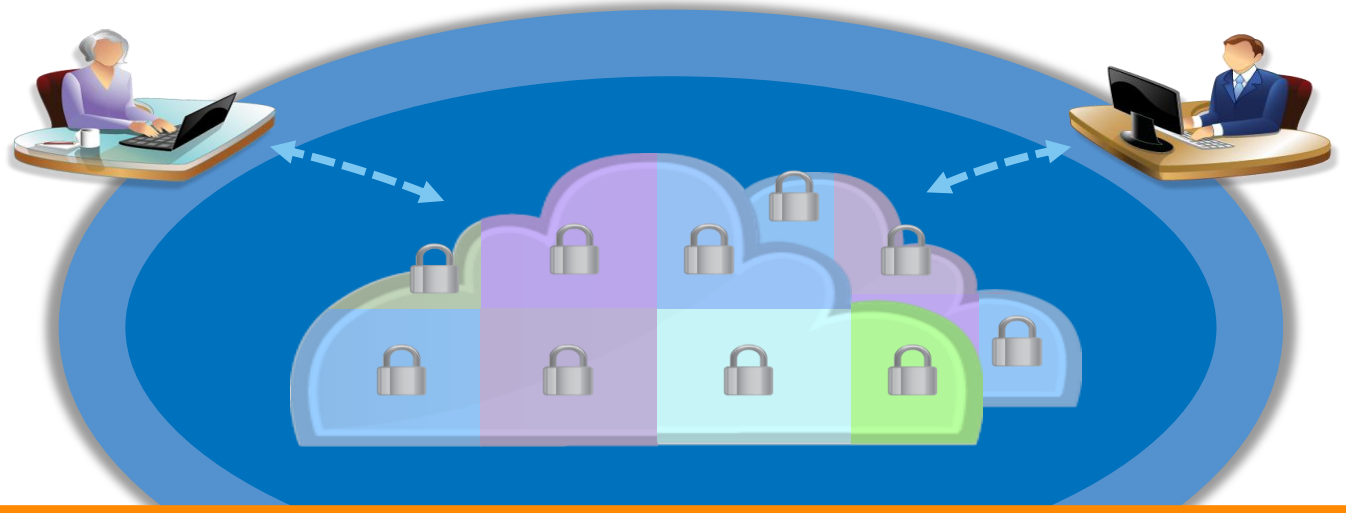
RSA CONFERENCE EUROPE 2012

Data Protection is Critical to Cloud Computing



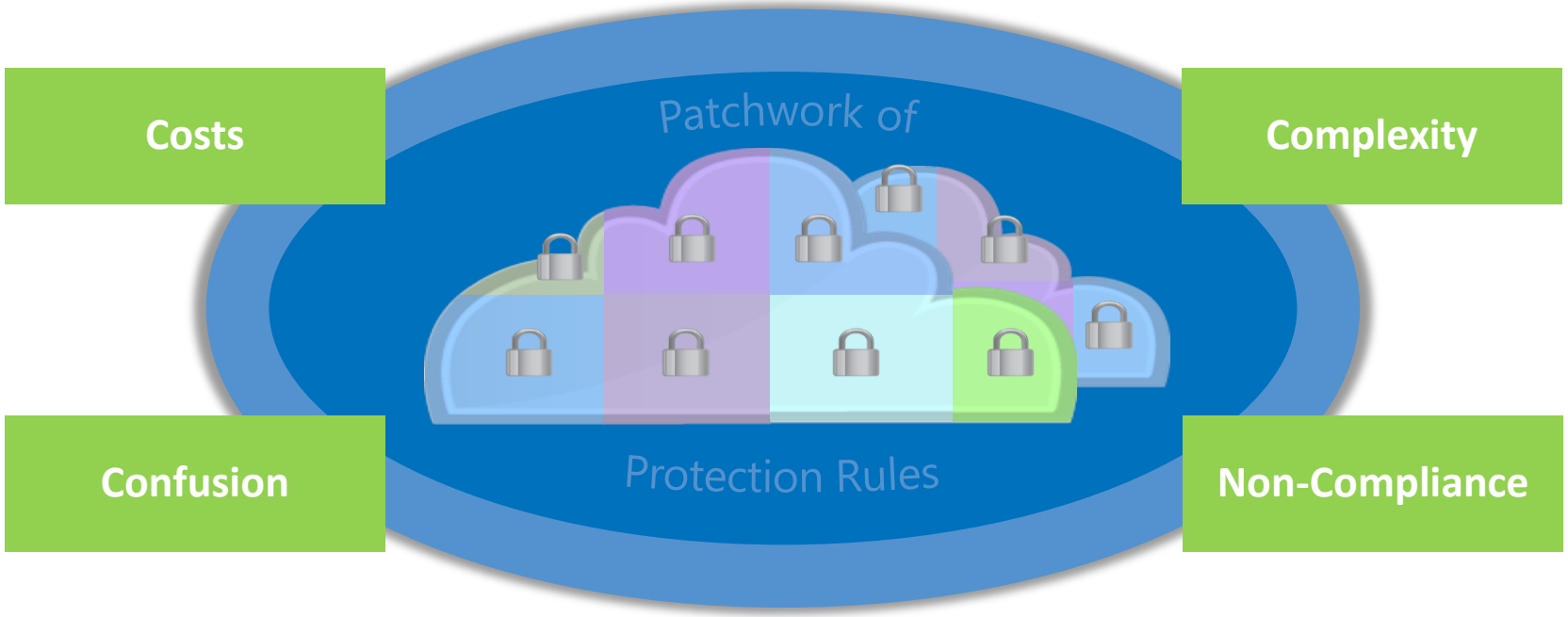
Data protection rules are crucial to ensuring the privacy and security of the data that customers entrust to cloud service providers.

The Compliance Challenge



Variability in Rules For:	Physical access Technical access Use	Distribution Input Purpose	Availability Administration Training

Fragmented Rules Create Obstacles, Stifle Growth



Growing Consensus for Consistency

What's needed is a Harmonised set of rules across jurisdictions that protect the privacy and enable the free, secure flow of data in the cloud.

Support Among Policymakers and Industry

"It is therefore clear that we need to provide further harmonisation and approximation of data protection rules at the EU level."

Viviane Reding,
Vice-President of the European Commission

"For cloud computing services to develop to their full potential, harmonised rules implemented consistently across the EU are essential."

BSA
Business Software Alliance

"There is a need to harmonise regulations on data protection, between the States forming the Latin American community."

RED IBEROAMERICANA DE PROTECCION DE DATOS

Many Stakeholders in Solution

A Way Forward with ISO

- World's largest developer and publisher of standards
- Broad representation with member bodies from162 countries
- Non-governmental organization that bridges the public and private sectors
- Open, transparent, inclusive process for standard development

Extend Existing International Information Security Management System Standard

ISO 27001

- International standard for Information **Security** Management Systems published in 2005
- Nearly **7,500 organizations** worldwide have been certified compliant with ISO 27001 (May, 2012)

"ISO 27001+DP"

- Augment ISO 27001 with **data protection** controls
- Serve as a foundation for **Harmonised** data protection rules across jurisdictions
- Extend 3rd-party **accreditation** to include new provisions

Benefits of Harmonization Are Widespread

Data Protection Agencies

- Improved privacy environment
- Increased compliance
- Lower regulatory cost burden

Cloud Customers

- Greater certainty of data privacy
- Lower prices
- Reduced liability due to non-compliance

Cloud Providers

- Reduced risk of non-compliance
- Lower delivery costs
- Lower barriers to entry and growth

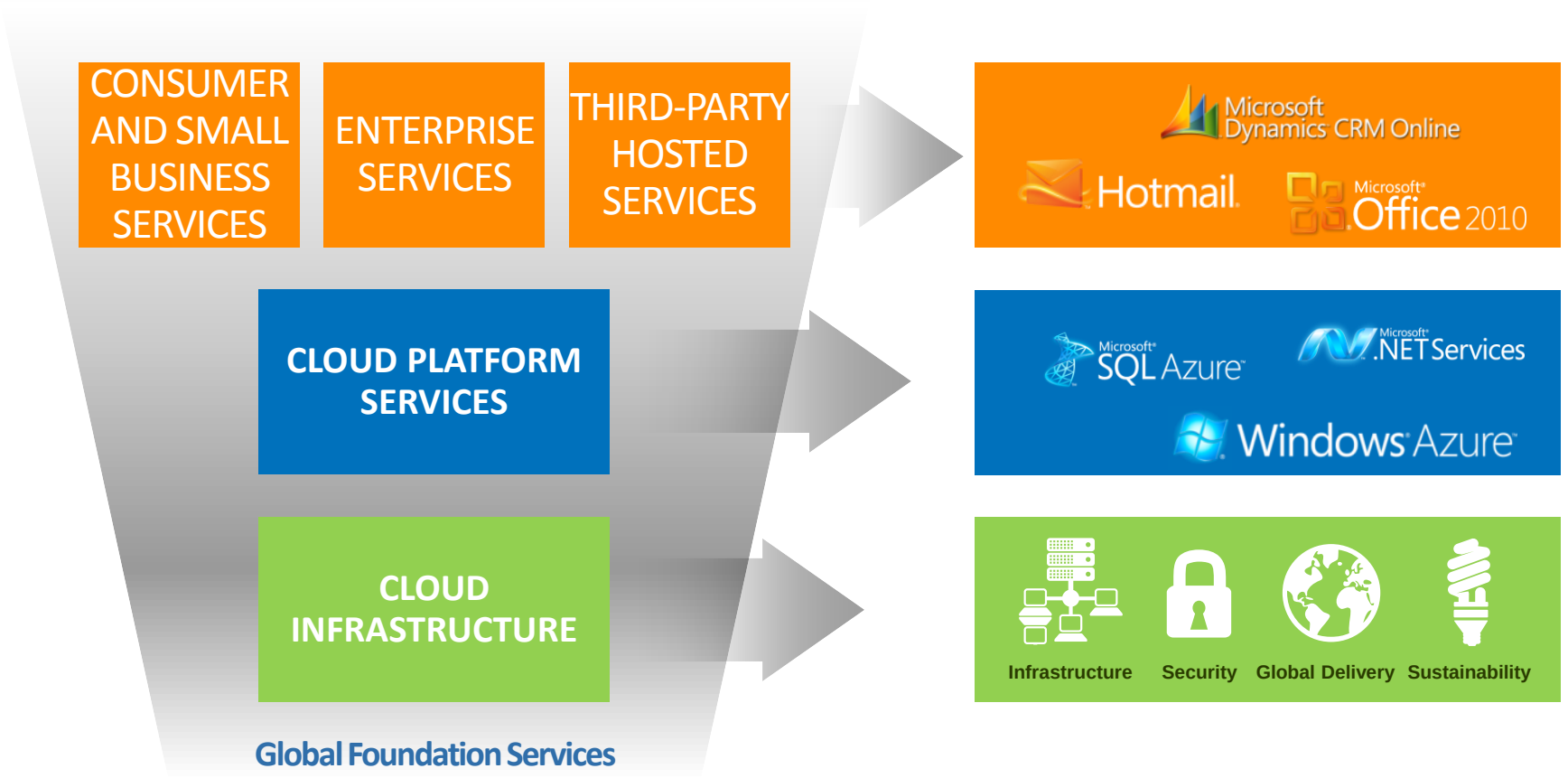
Auditors & Certifiers

- Expanded, global market opportunity
- Greater consistency

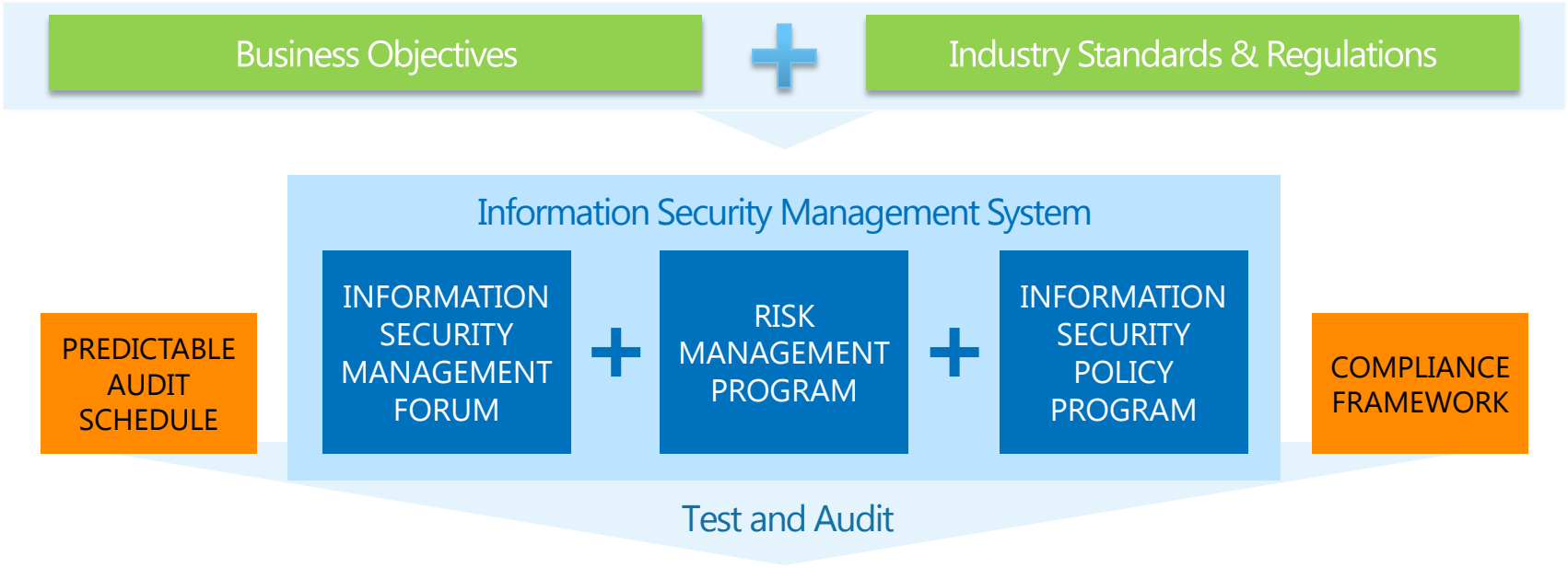
Compliance in Microsoft's Cloud Infrastructure

RSA CONFERENCE EUROPE 2012

Microsoft's Cloud Environment



Information Security Management System



Certificates and Attestations

- ISO / IEC 27001:2005 certification
- SAS 70 Type I and II attestations
- Sarbanes Oxley
- PCI DSS certification
- FISMA certification and accreditation
- And more …

Comprehensive Compliance Framework

INDUSTRY STANDARDS AND REGULATIONS

- Payment card industry data security standard
- Health insurance portability and accountability act
- Media ratings council
- Sarbanes-Oxley, etc.

CONTROLS FRAMEWORK

- Identify and integrate
  - Regulatory requirements
  - Customer requirements
- Assess and remediate
  - Eliminate or mitigate gaps in control design

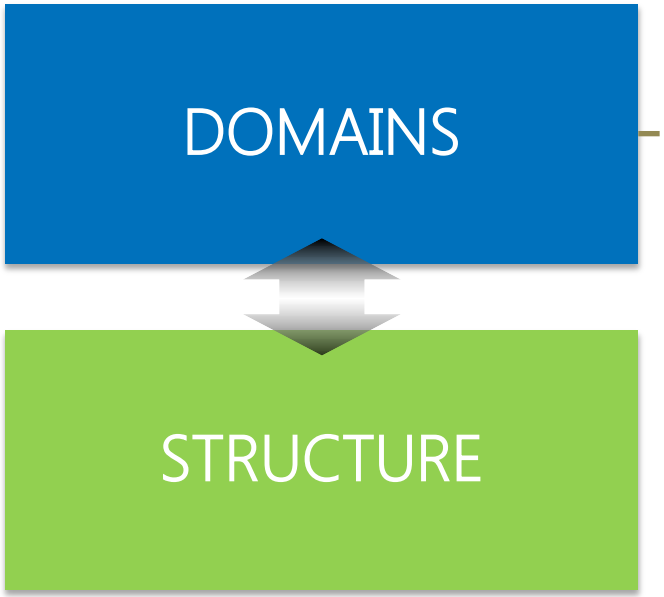
PREDICTABLE AUDIT SCHEDULE

- Test effectiveness and assess risk
- Attain certifications and attestations
- Improve and optimize
  - Examine root cause of non-compliance
  - Track until fully remediated

CERTIFICATION AND ATTESTATIONS

- ISO/IEC 27001:2005 certification
- Statement of Auditing Standard (SAS) 70 type I and type II attestations

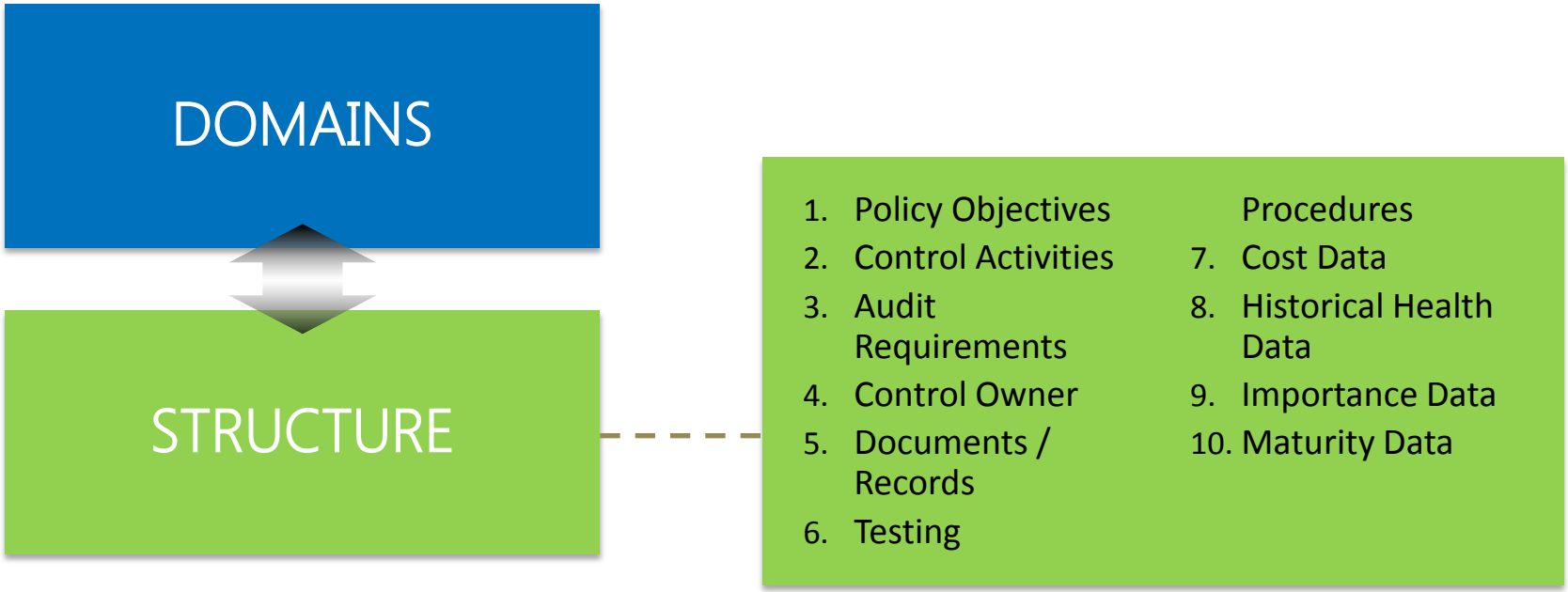
Control Framework
Domains



1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development, and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Control Framework

Structure



Rationalised Requirements

CONTROL OBJECTIVE

Security awareness training for all employees, contractors, and third-party users must be provided:

- When granted access to resources
- When organizational policies and procedures change

Trainees will be expected to understand these policies and procedures as they relate to relevant job function and protection of sensitive information

Applying this control objective meets multiple compliance obligations

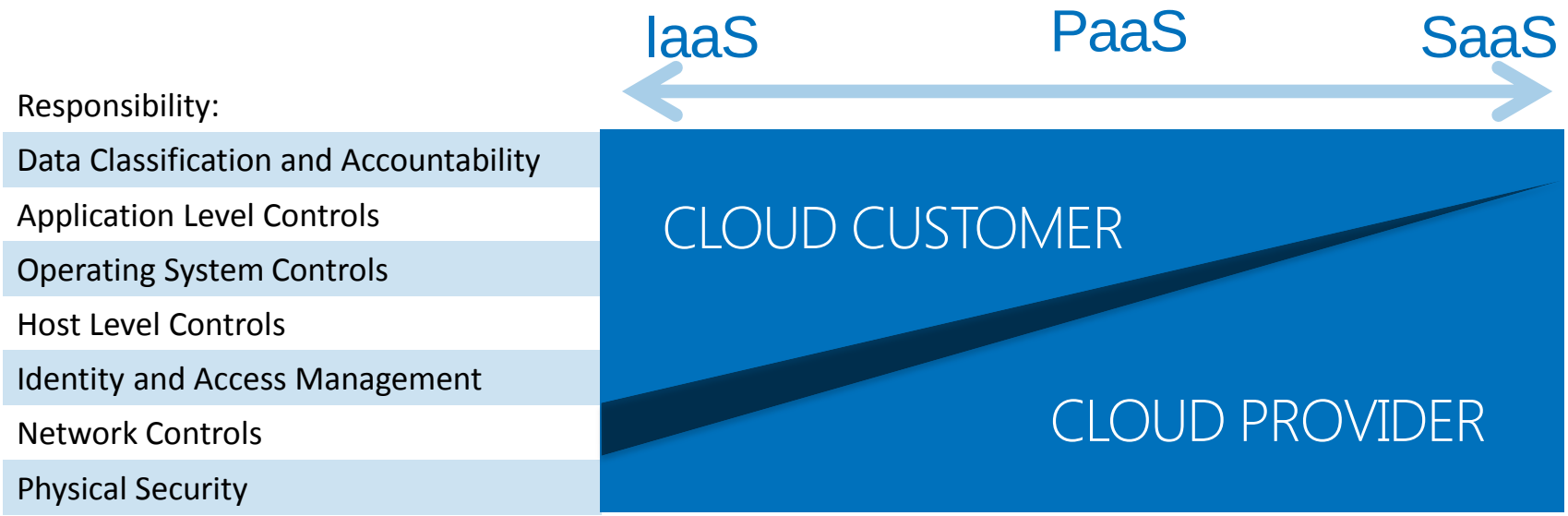
ISO/IEC 27001:2005 A.5.2.2	SOX COBIT DS7
HIPAA 164.530.b.1	PCI-DSS version 1.2 12.6.1

Microsoft's Compliance Capabilities

ISO / IEC 27001:2005 Certification	✓
SAS 70 Type I and II attestations (transitioning to SSAE 16/ISAE 3402 SOC 1, 2 and 3)	✓
HIPAA/HITECH	✓
Various State, Federal, and International Privacy Laws (95/46/EC—aka EU Data Protection Directive; California SB1386; etc.)	✓
PCI Data Security Standard Certification	✓
FISMA Certification & Accreditation	✓
G-Cloud IL2 Accreditation with Office 365	

Helping You Meet Your Compliance Needs

- You are ultimately responsible for ensuring you meet your compliance obligations
- Microsoft will share its certifications and audit reports to help you design your compliance program



Applying Compliance as a Customer

Considerations for choice in a Cloud Services Provider

Consult guidance from organizations such as the Cloud Security Alliance

Require that the provider has attained **third-party certifications and audits**, e.g. ISO/IEC 27001:2005

Know the value of your data and processes and the **security and compliance obligations** you need to meet

Consider the ability of vendors to accommodate **changing security and compliance requirements**

Ensure a clear understanding of security and **compliance roles** and **responsibilities** for delivered services

Ensure data and services can be brought **back in house** if necessary

Require transparency in security policies and operations

Microsoft's Cloud Trust Resources

Global Foundation Services Web Site

www.globalfoundationservices.com

Trust Centres

http://www.microsoft.com/en-us/office365/trust-center.aspx
http://www.windowsazure.com/en-us/support/trust-center/

Global Foundation Services Blog

http://blogs.technet.com/msdatacenters

Cloud Security Alliance STAR

https://cloudsecurityalliance.org/star/


Microsoft