# Cloud Provider Assurance
## *Trust but Verify*

**Mike Small CEng, FBCS, CITP**

**Senior Analyst**
**KuppingerCole**

***ISACA UK Chapter Member***

Session ID: **GRC-301**

Session Classification: **Intermediate**

RSACONFERENCE
EUROPE 2012

# Agenda

- Can I trust the Cloud?
- Which Cloud Risks concern you?
- Managing the Cloud
- Cloud Auditing and Assurance
- Summary

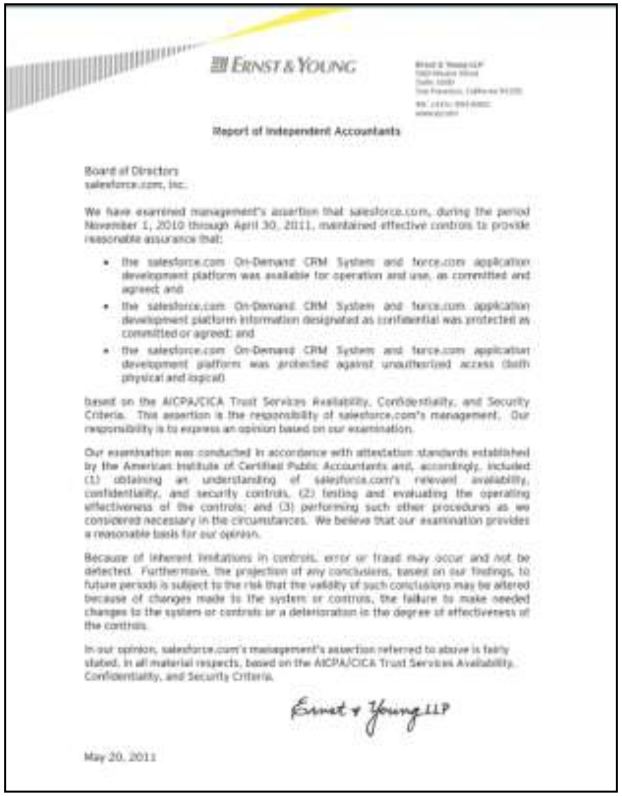
# Can I trust the Cloud?

…strive to deliver products that are “as available, reliable and secure as standard services such as electricity, water services and telephony.” …

**Bill Gates email Jan 12, 2002**

# Does this make the Cloud Trustworthy

- What does this report mean?
- Does it cover what your organization needs?
- How does this provider measure up against best practice?
- How does this provider compare with others?



ERNST & YOUNG

Ernst & Young LLP
[illegible]
[illegible]
San Francisco, California [illegible]
[illegible]
www.ey.com

**Report of Independent Accountants**

Board of Directors
salesforce.com, Inc.

We have examined management's assertion that salesforce.com, during the period November 1, 2010 through April 30, 2011, maintained effective controls to provide reasonable assurance that:

- the salesforce.com On-Demand CRM System and force.com application development platform was available for operation and use, as committed and agreed; and
- the salesforce.com On-Demand CRM System and force.com application development platform information designated as confidential was protected as committed or agreed; and
- the salesforce.com On-Demand CRM System and force.com application development platform was protected against unauthorized access (both physical and logical)

based on the AICPA/CICA Trust Services Availability, Confidentiality, and Security Criteria. This assertion is the responsibility of salesforce.com's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of salesforce.com's relevant availability, confidentiality, and security controls, (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, salesforce.com's management's assertion referred to above is fairly stated, in all material respects, based on the AICPA/CICA Trust Services Availability, Confidentiality, and Security Criteria.

Ernst & Young LLP

May 20, 2011

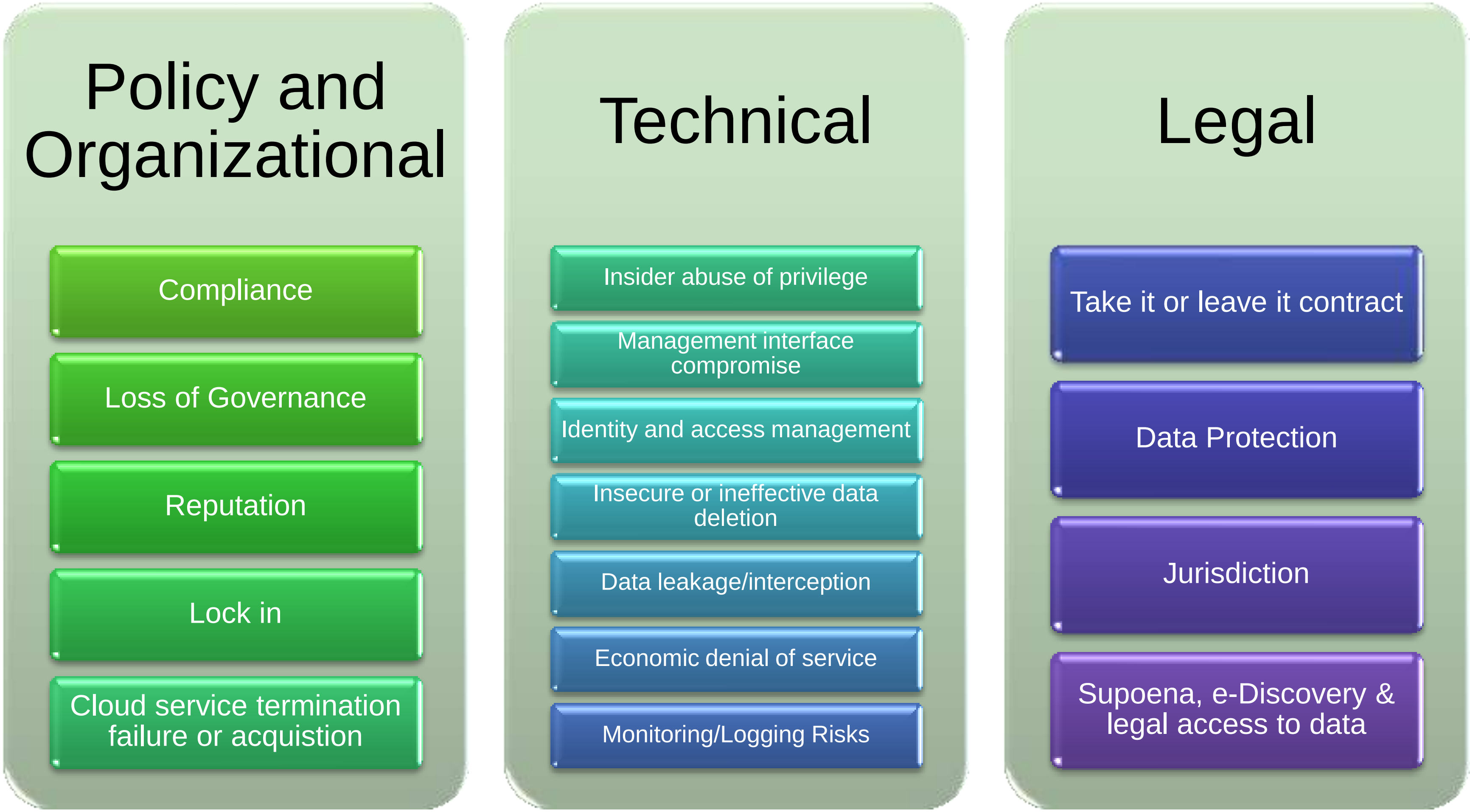
https://trust.salesforce.com/trust/assets/pdf/Misc_SysTrust.pdf

# Which Cloud Risks Concern You?

Cloud security issues (84.4%) and Cloud privacy and compliance issues (84.9%) are the major inhibitors preventing organizations from moving to a private Cloud.

**KuppingerCole Survey**

# Cloud Risks



## Policy and Organizational

- Compliance
- Loss of Governance
- Reputation
- Lock in
- Cloud service termination failure or acquistion

## Technical

- Insider abuse of privilege
- Management interface compromise
- Identity and access management
- Insecure or ineffective data deletion
- Data leakage/interception
- Economic denial of service
- Monitoring/Logging Risks

## Legal

- Take it or leave it contract
- Data Protection
- Jurisdiction
- Supoena, e-Discovery & legal access to data

http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

# Loss of Reputation

| Risk | |
|---|---|
| Probability | Low |
| Impact | High |

## RBS boss blames software upgrade for account problems http://www.bbc.co.uk/news/business-18575932

June 25th, 2012

The boss of RBS has confirmed that a software change was responsible for the widespread computer problems affecting millions of customers' bank accounts.

# Business Continuity

| Probability | Low |
|---|---|
| Impact | High |

## Lightning Strike in Dublin Downs Amazon, Microsoft Clouds

http://www.pcworld.com/businesscenter/article/237476/lightning_strike_in_dublin_downs_amazon_microsoft_clouds.html/
August 8th, 2011

A lightning strike in Dublin on August 8th caused a power failure in data centres belonging to Amazon and Microsoft, causing the companies' cloud services to go offline.

# Secure Data Handling

| | |
|---|---|
| Probability | Medium |
| Impact | Very High |

**NHS Trust fined £325,000 following data breach affecting thousands of patients and staff**

http://www.ico.gov.uk/news/

June 1st, 2012

The data breach occurred when an individual engaged by the Trust's **IT service provider** was tasked to destroy approximately 1000 hard drives. Some of these drives were subsequently sold on an Internet auction site.

# Legal Risk - Contract

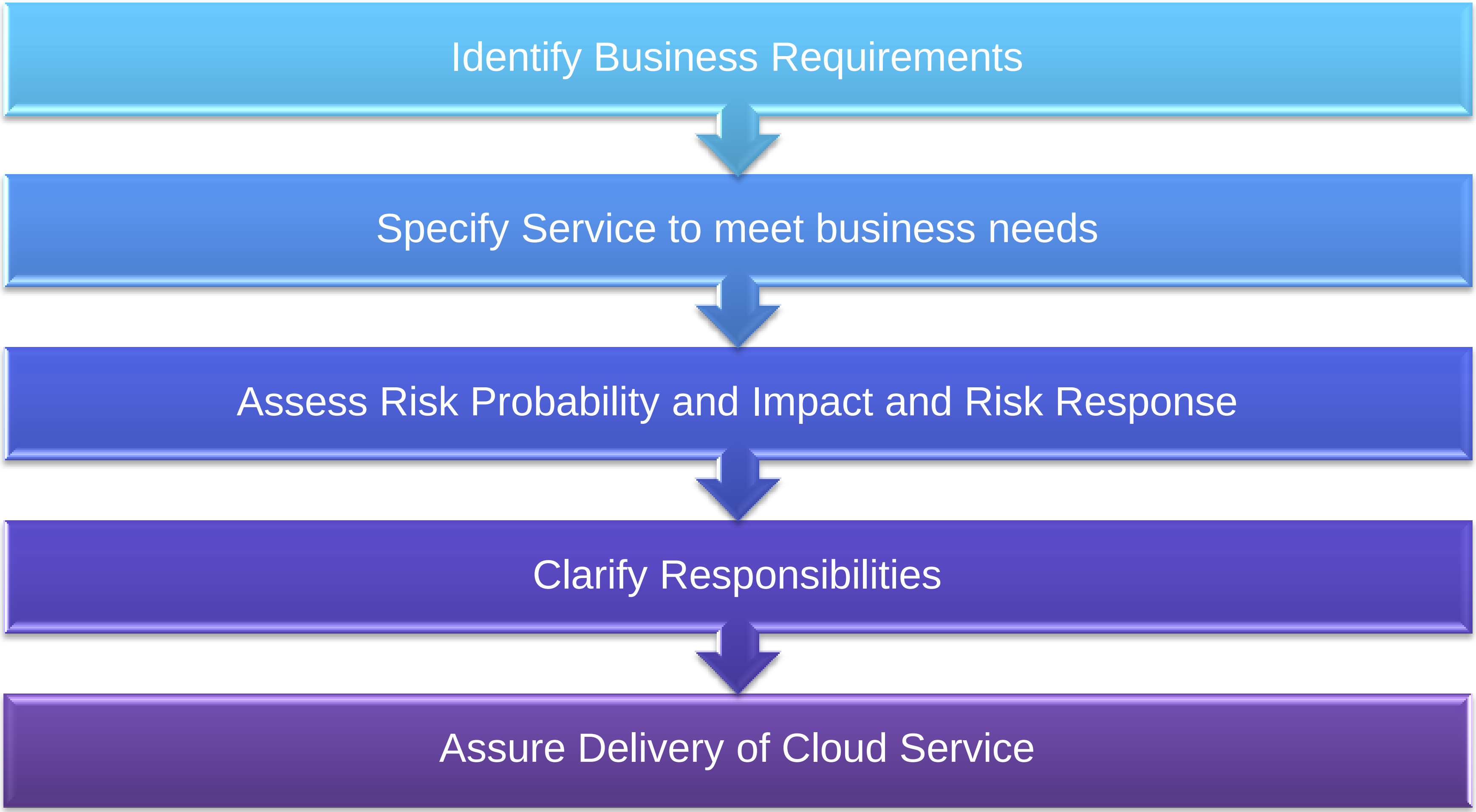
| | |
|---|---|
| Probability | Very High |
| Impact | High |

- Cloud Provider Contracts are
  - Largely “take it or leave it”
  - Less onerous obligations on provider
  - Almost total exclusion of liability
  - Risk of Lock-in

# Managing the Cloud

Adopting the Cloud means moving from direct management to indirect governance.
Taking a good governance approach is the key to safely getting benefits from the Cloud.

# Cloud Governance



Identify Business Requirements

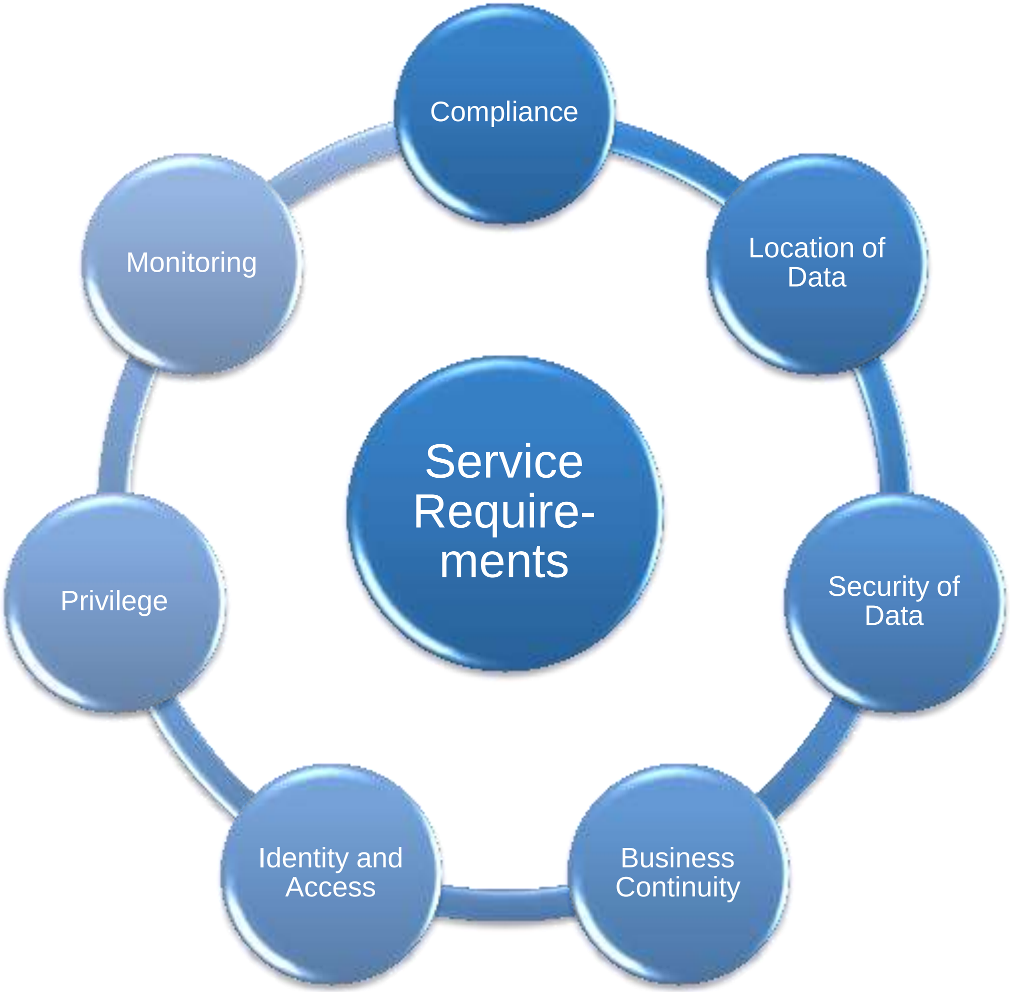
Specify Service to meet business needs

Assess Risk Probability and Impact and Risk Response

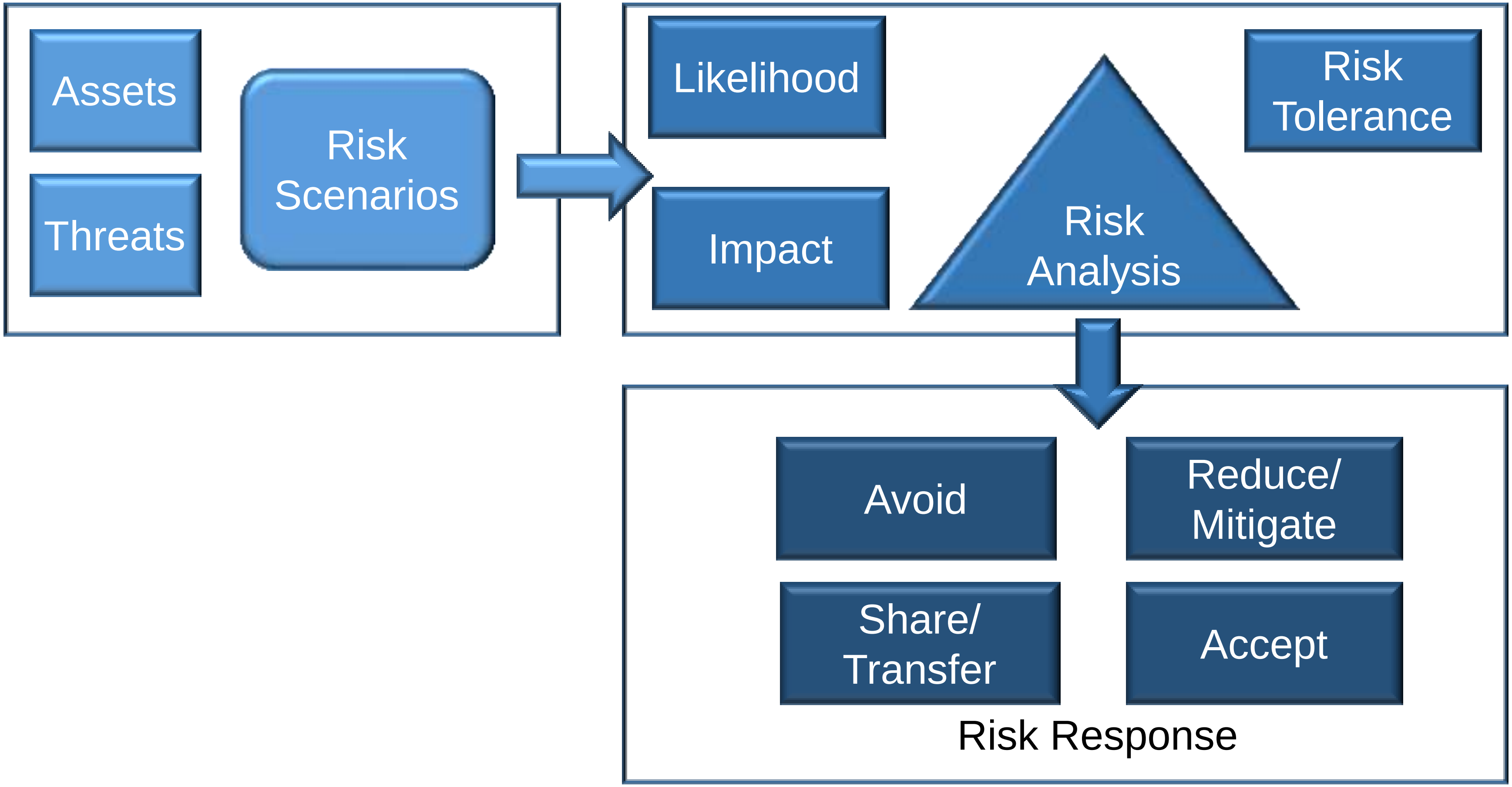
Clarify Responsibilities

Assure Delivery of Cloud Service

# Specify Service Required



# Assess Risk and Choose Response



Assets

Threats

Risk Scenarios

Likelihood

Impact

Risk Analysis

Risk Tolerance

Avoid

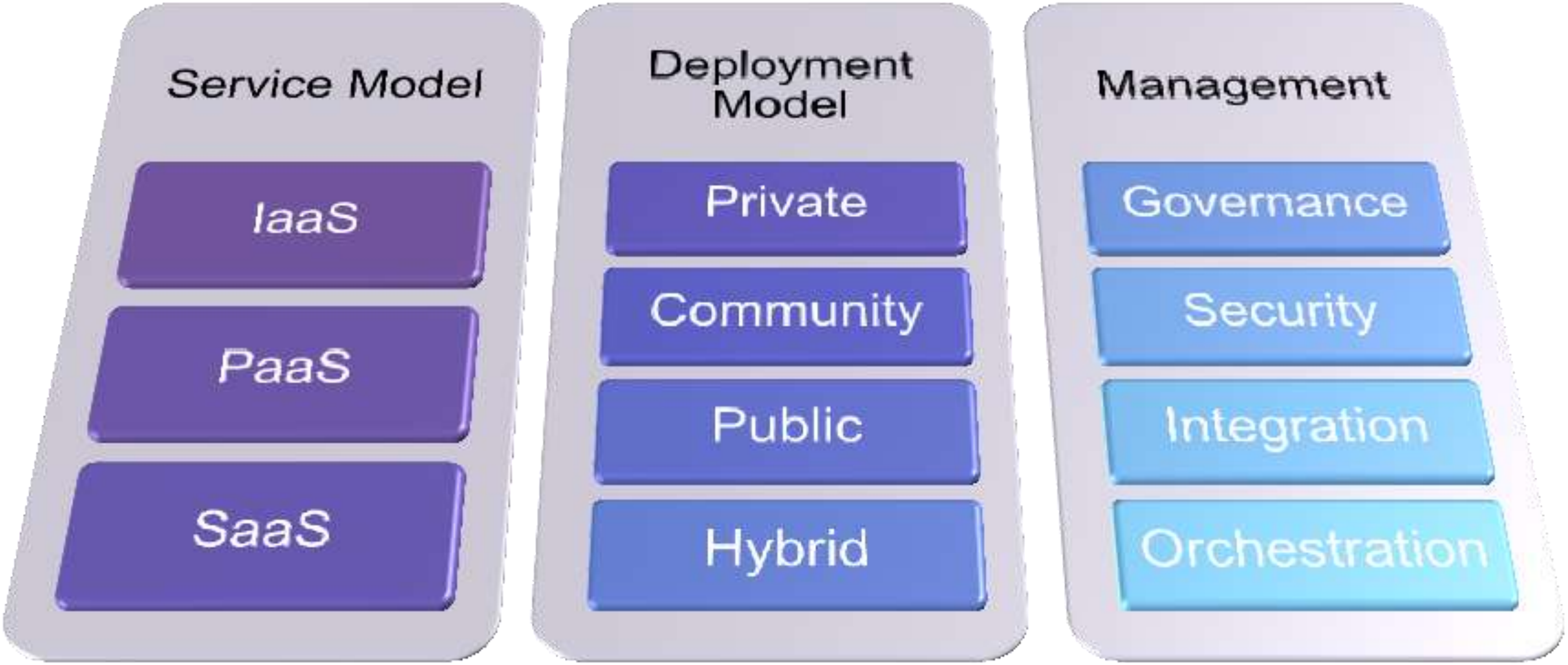
Reduce/ Mitigate

Share/ Transfer

Accept

Risk Response

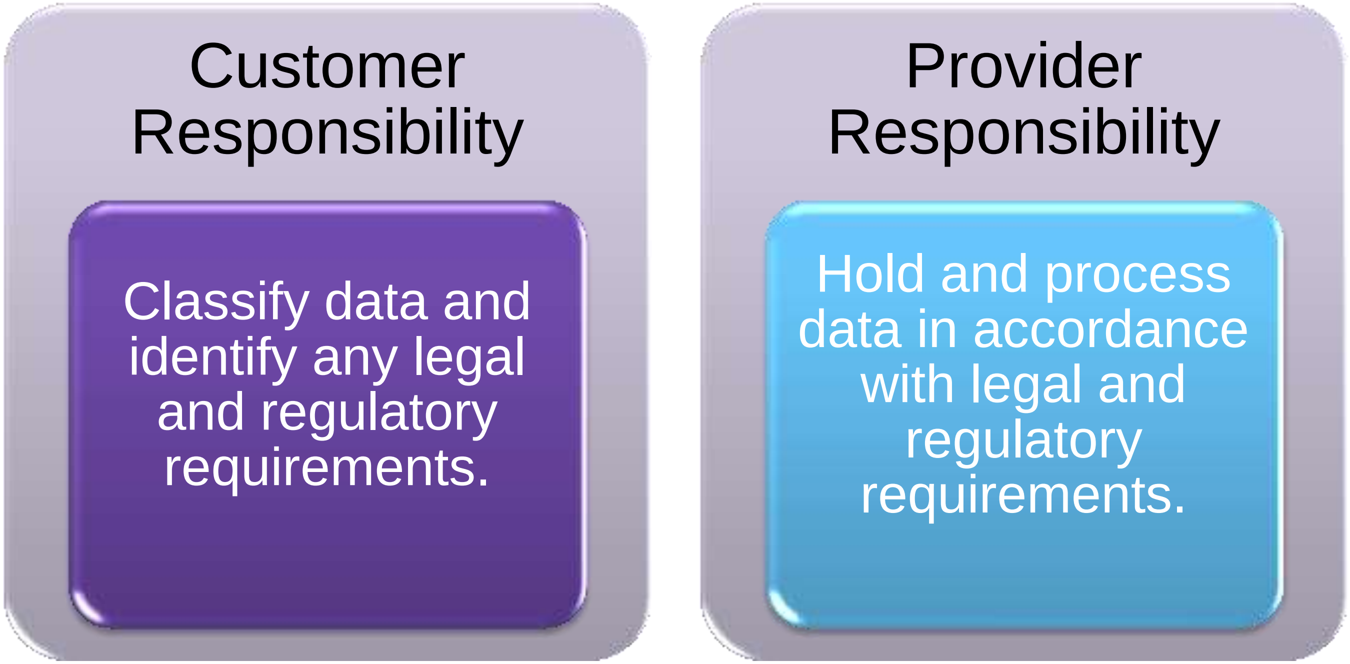
# Choose the Right Cloud



# Define Responsibilities - Compliance

ISO 27001 Control 15.1.4:

- Data protection and privacy should be ensured…



Customer Responsibility

Classify data and identify any legal and regulatory requirements.

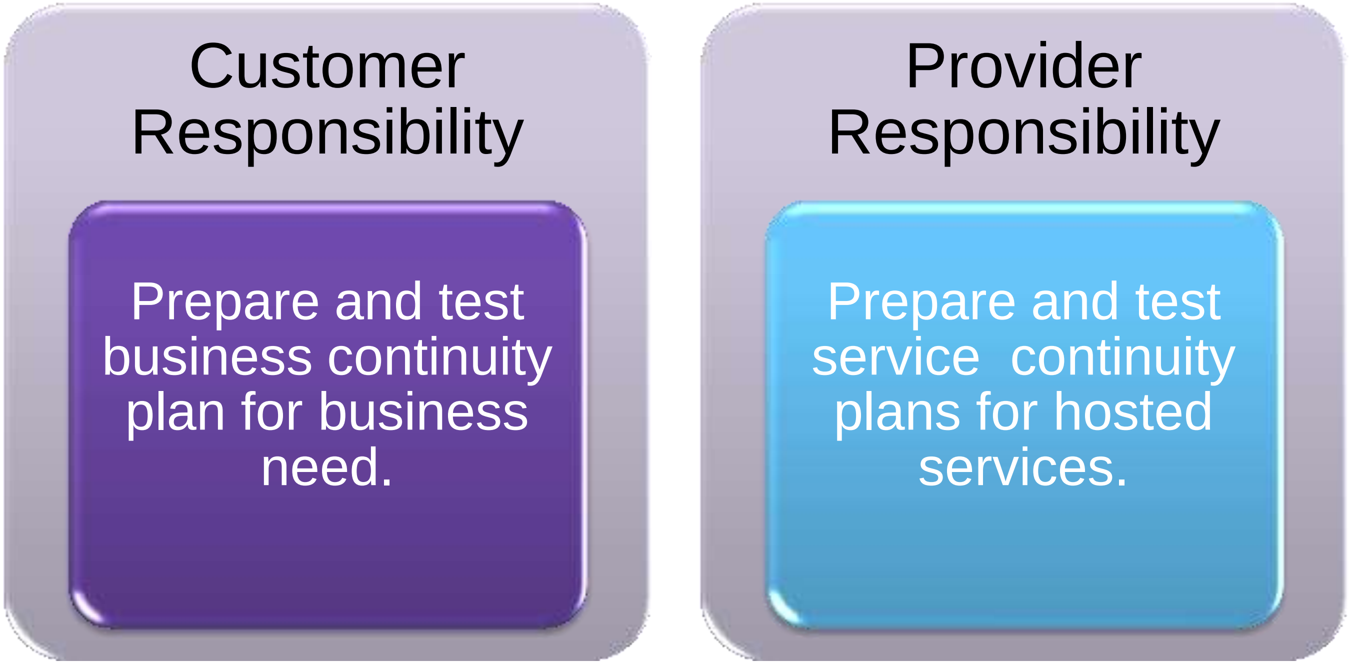
Provider Responsibility

Hold and process data in accordance with legal and regulatory requirements.

# Define Responsibilities - Business Continuity

ISO 27001 Control 14:

- A business continuity management process should be implemented…



Customer Responsibility

Prepare and test business continuity plan for business need.

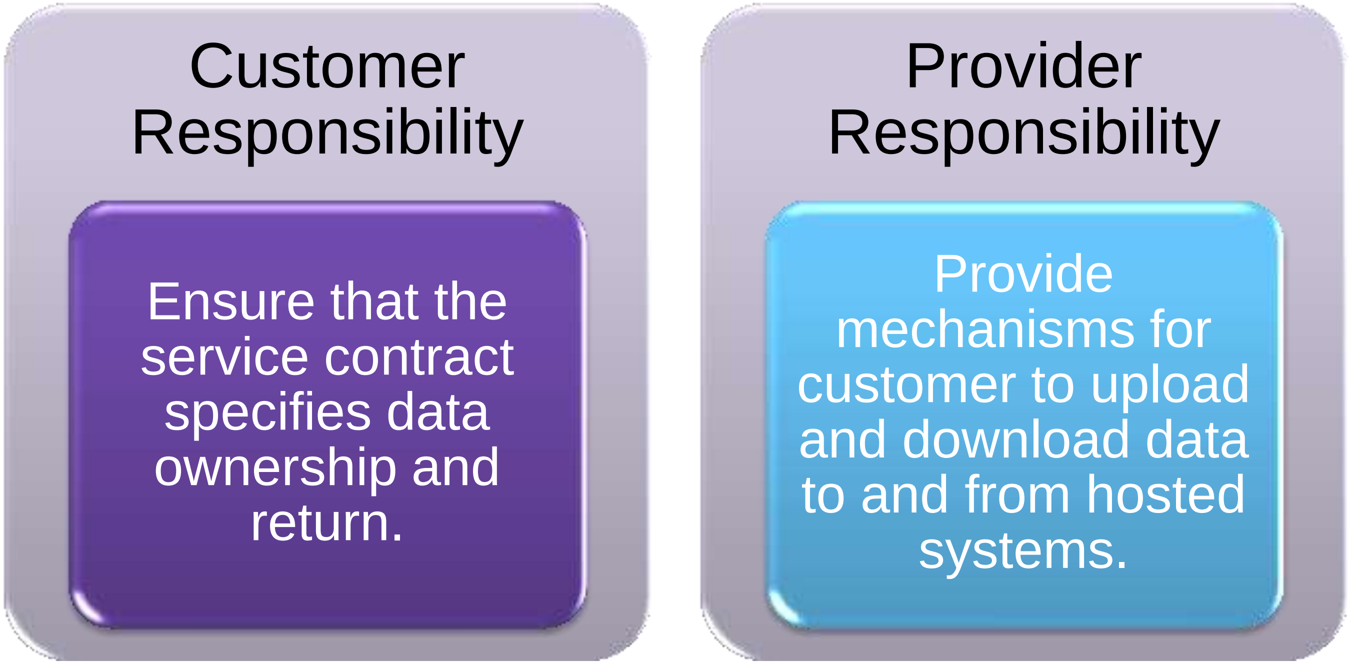
Provider Responsibility

Prepare and test service continuity plans for hosted services.

# Define Responsibilities - Data Return

ISO 27001 Control 8.3.2:

- All employees, contractors and third party users should return all of the organization’s assets in their possession..



Customer Responsibility

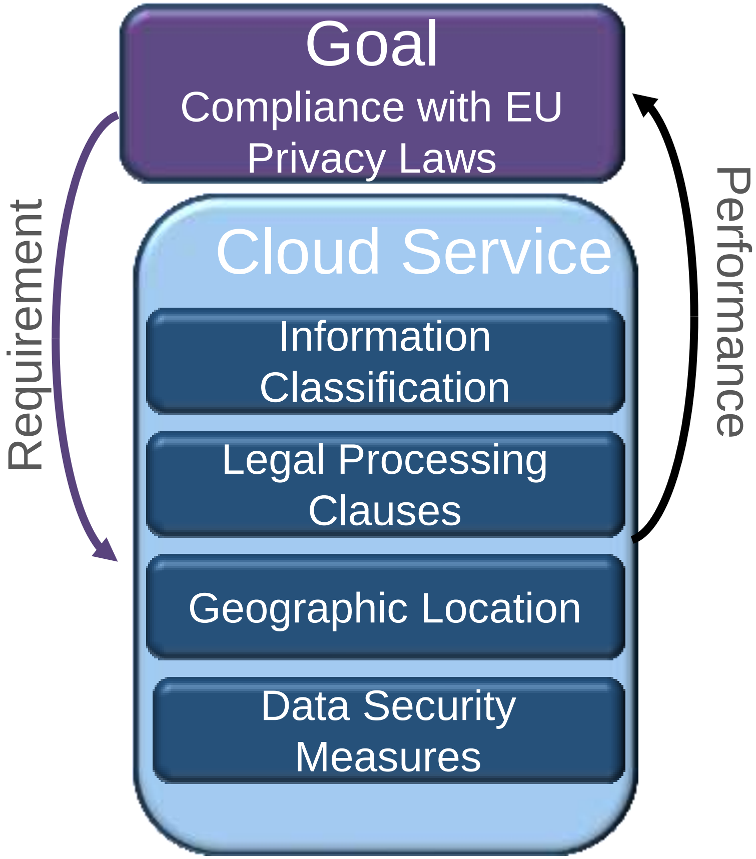
Ensure that the service contract specifies data ownership and return.

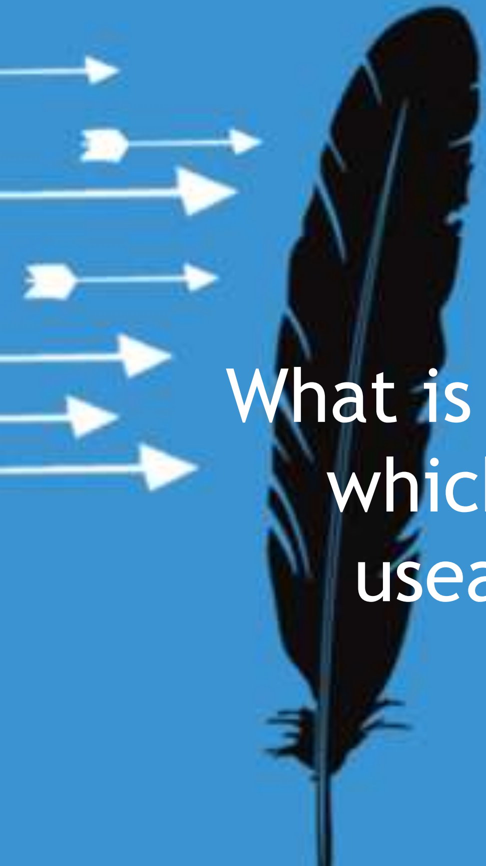
Provider Responsibility

Provide mechanisms for customer to upload and download data to and from hosted systems.

# Monitor against Requirements

- Performance needs to be measured against business needs

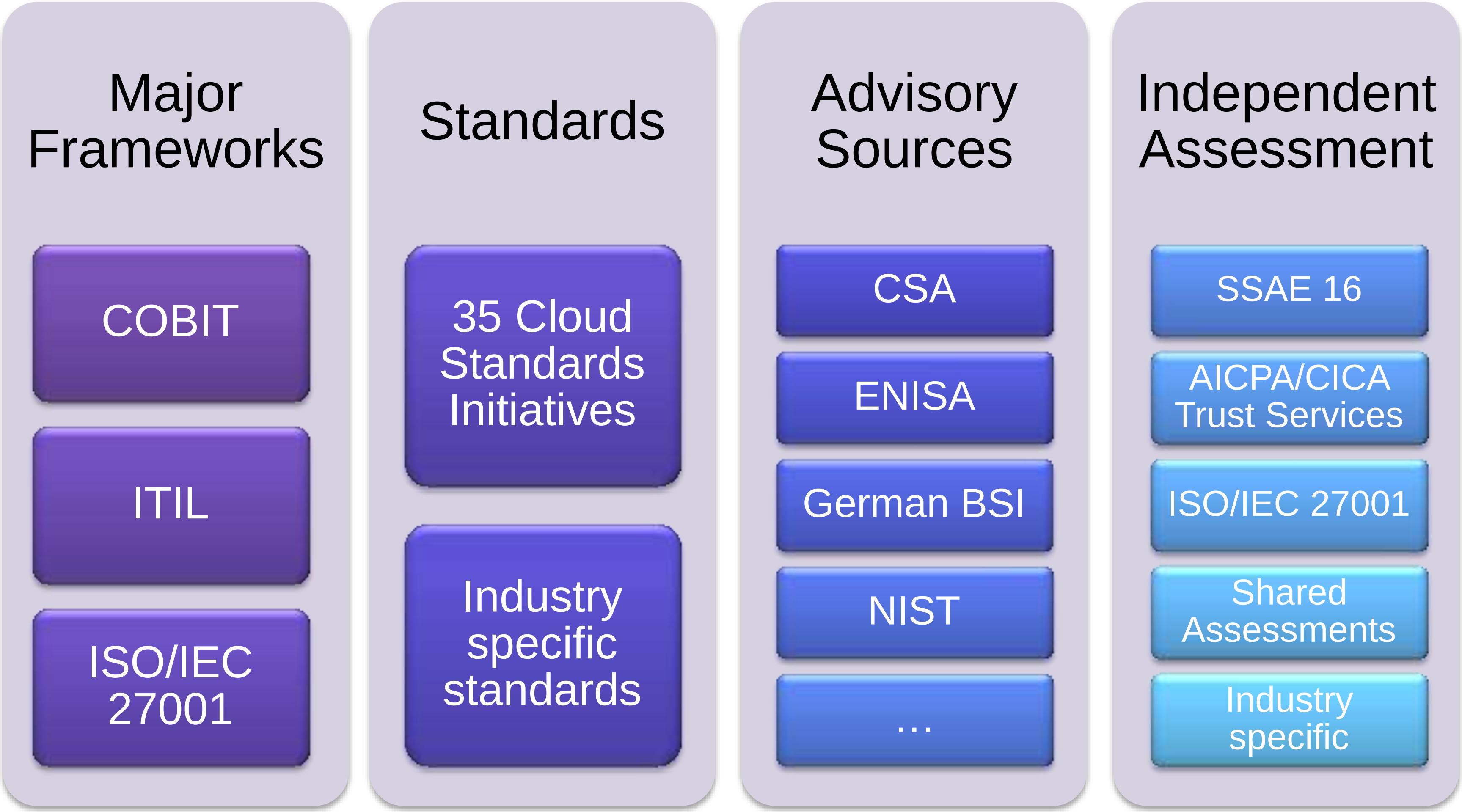




# Cloud Auditing and Assurance

What is needed is a common standard against which to measure Cloud services that is useable by both the customer and the provider.

# Many Sources of Advice = Confusion



**Major Frameworks**

- COBIT
- ITIL
- ISO/IEC 27001

**Standards**

- 35 Cloud Standards Initiatives
- Industry specific standards

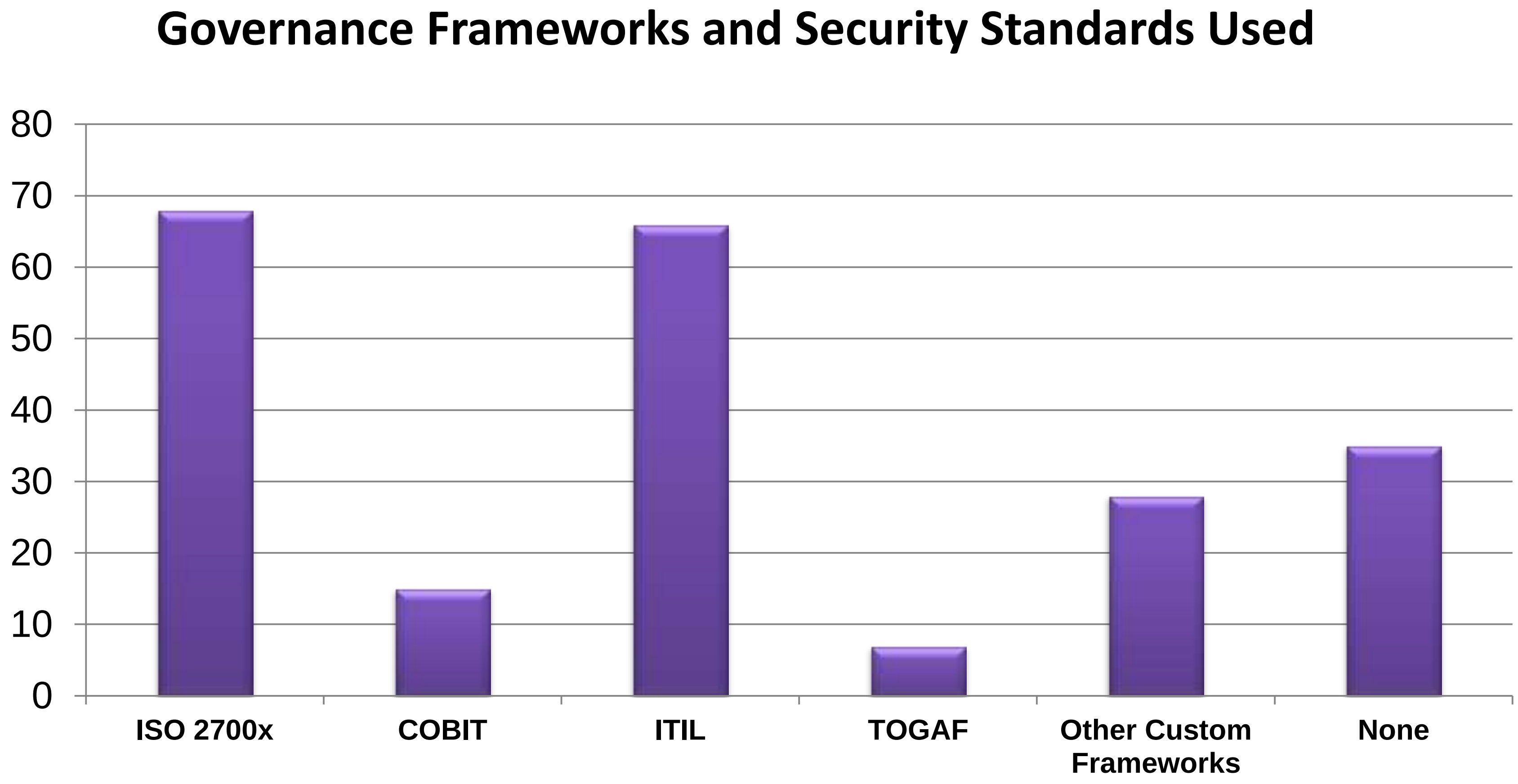
**Advisory Sources**

- CSA
- ENISA
- German BSI
- NIST
- …

**Independent Assessment**

- SSAE 16
- AICPA/CICA Trust Services
- ISO/IEC 27001
- Shared Assessments
- Industry specific

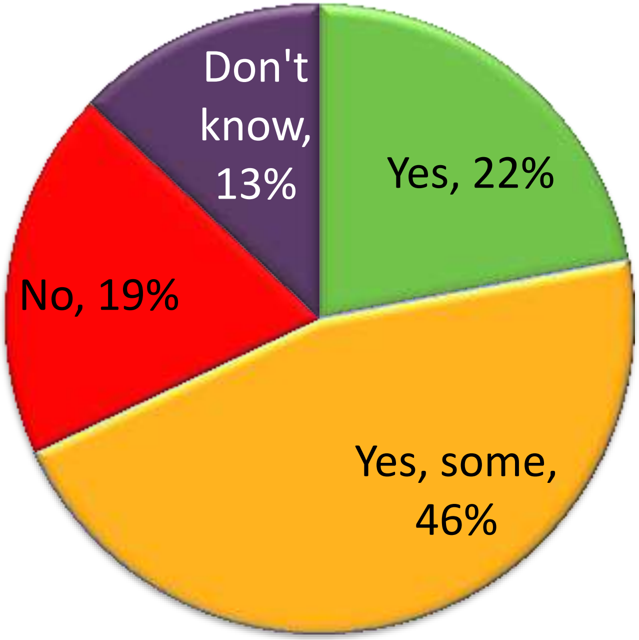
# Governance Frameworks Used



ENISA Survey of SLAs across EU Public Sector, Dec 2011

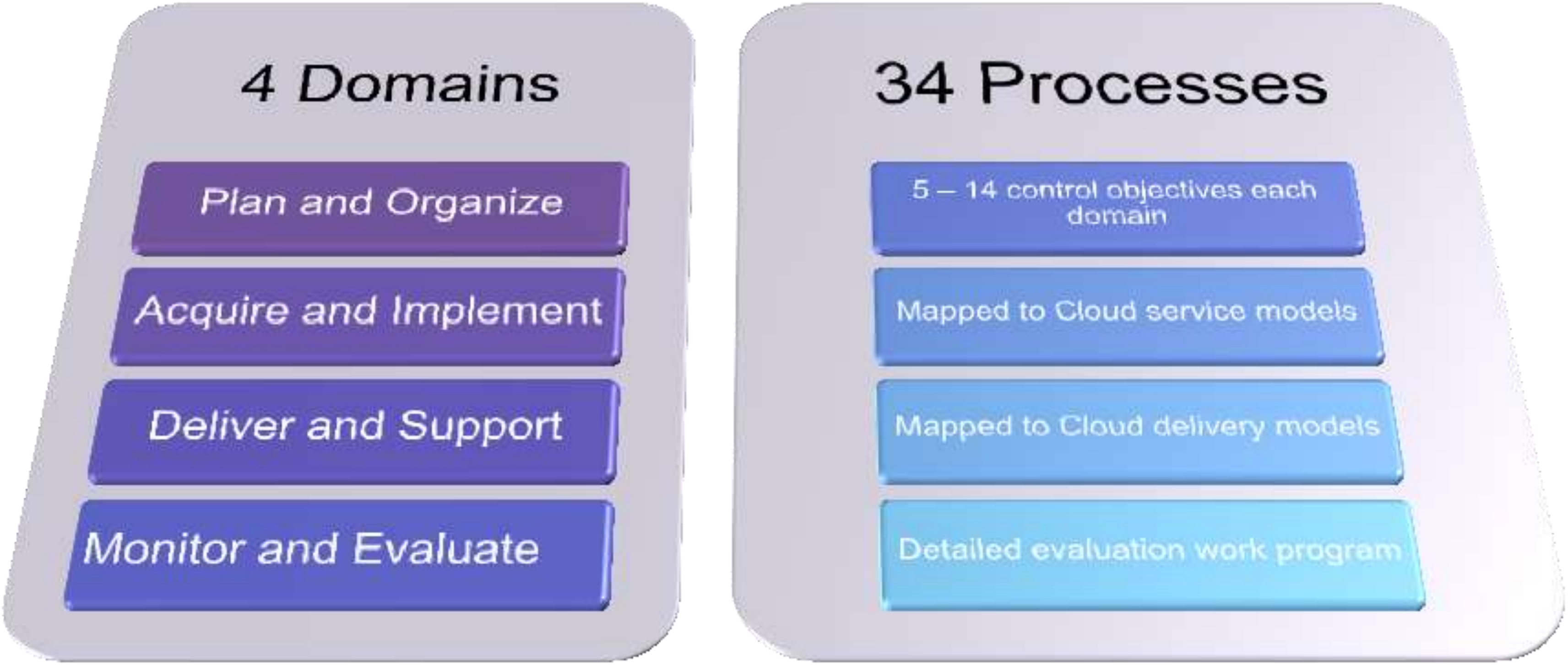
# Provider Standards

**Are your IT service providers obliged to adhere to these standards too?**



ENISA Survey of SLAs across EU Public Sector, Dec 2011

# Framework: COBIT - IT Control Objectives for Cloud Computing



4 Domains

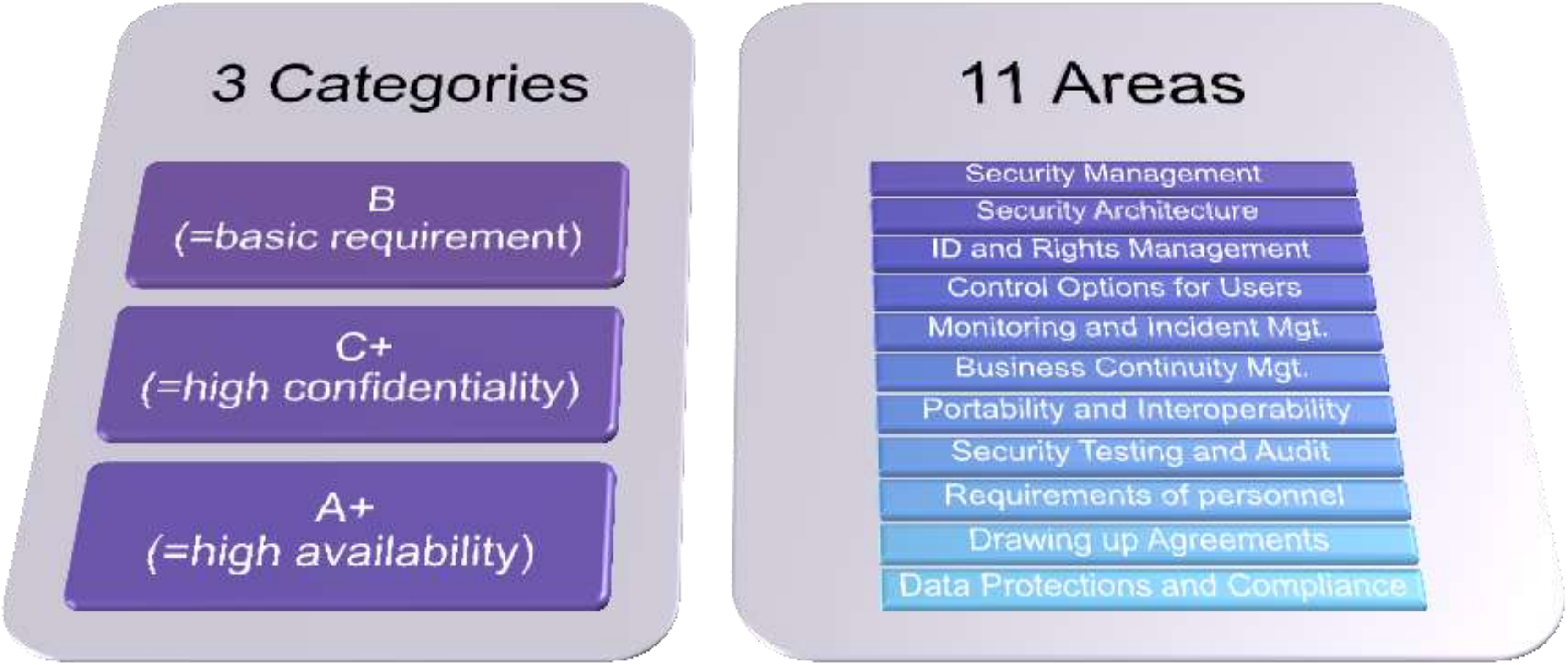
- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

34 Processes

- 5 – 14 control objectives each domain
- Mapped to Cloud service models
- Mapped to Cloud delivery models
- Detailed evaluation work program

ISACA: IT Control Objectives for Cloud Computing

# Advice: German BSI - Security Recommendations for Cloud Providers



3 Categories

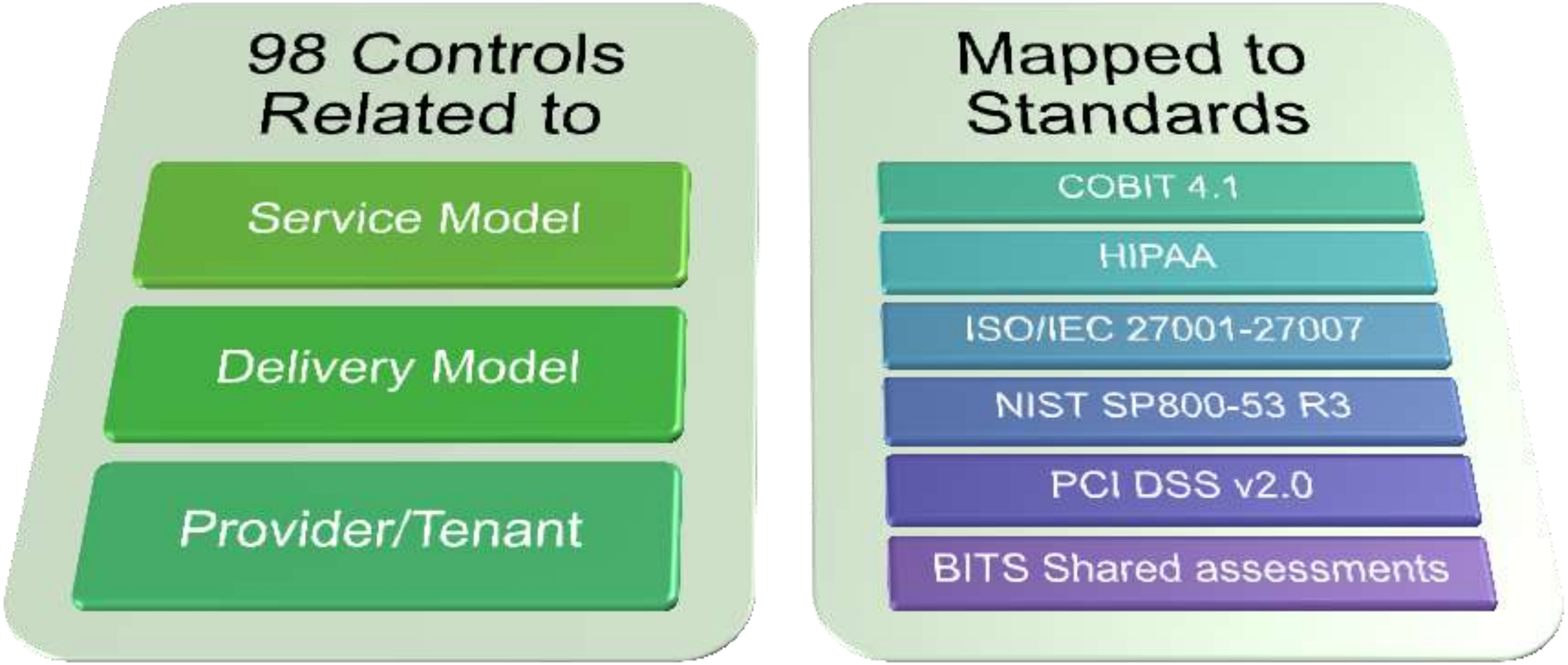
- B (=basic requirement)
- C+ (=high confidentiality)
- A+ (=high availability)

11 Areas

- Security Management
- Security Architecture
- ID and Rights Management
- Control Options for Users
- Monitoring and Incident Mgt.
- Business Continuity Mgt.
- Portability and Interoperability
- Security Testing and Audit
- Requirements of personnel
- Drawing up Agreements
- Data Protections and Compliance

https://www.bsi.bund.de/

# Advice: CSA Cloud Controls Matrix 2v1



98 Controls Related to

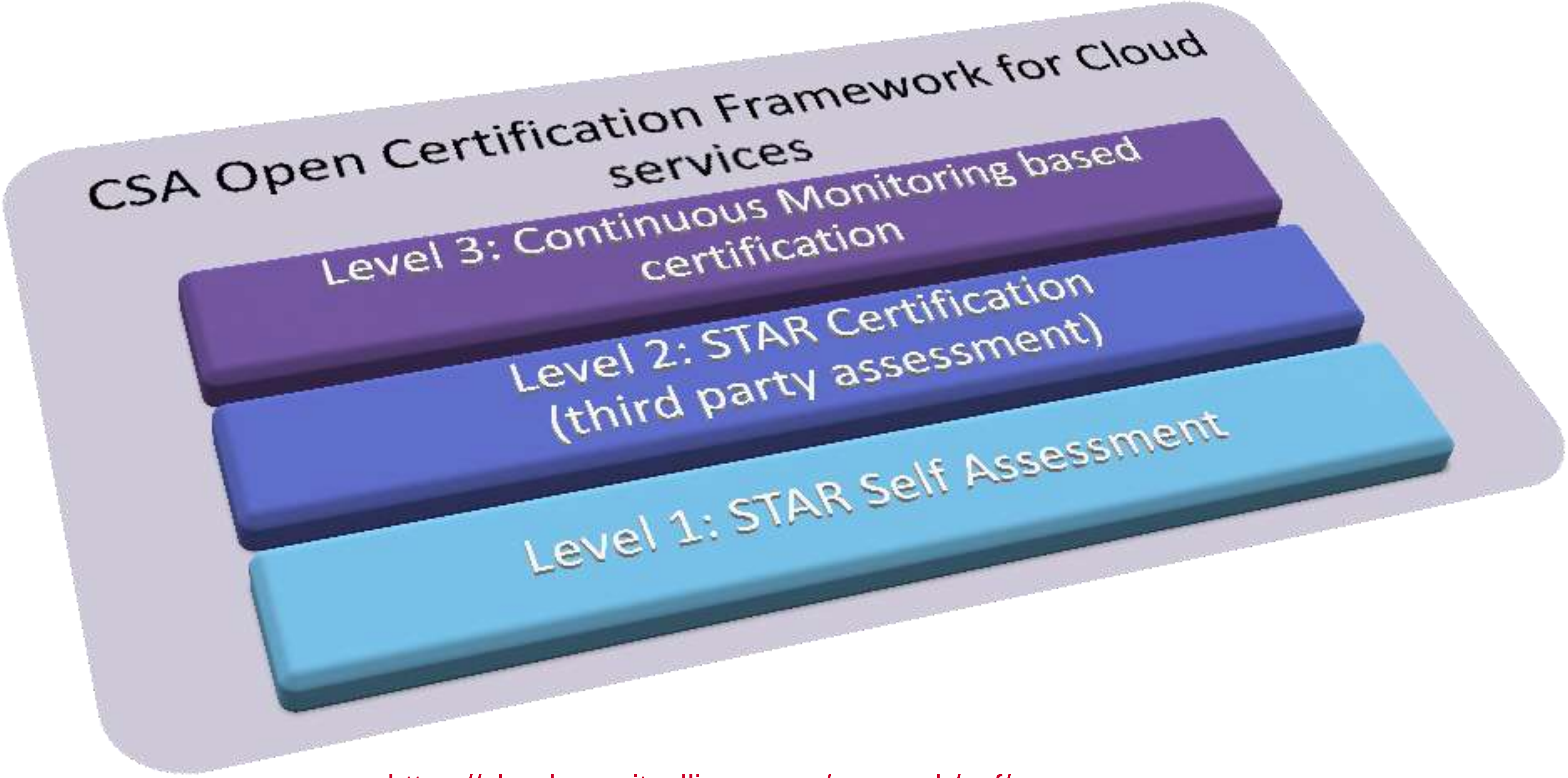
- Service Model
- Delivery Model
- Provider/Tenant

Mapped to Standards

- COBIT 4.1
- HIPAA
- ISO/IEC 27001-27007
- NIST SP800-53 R3
- PCI DSS v2.0
- BITS Shared assessments

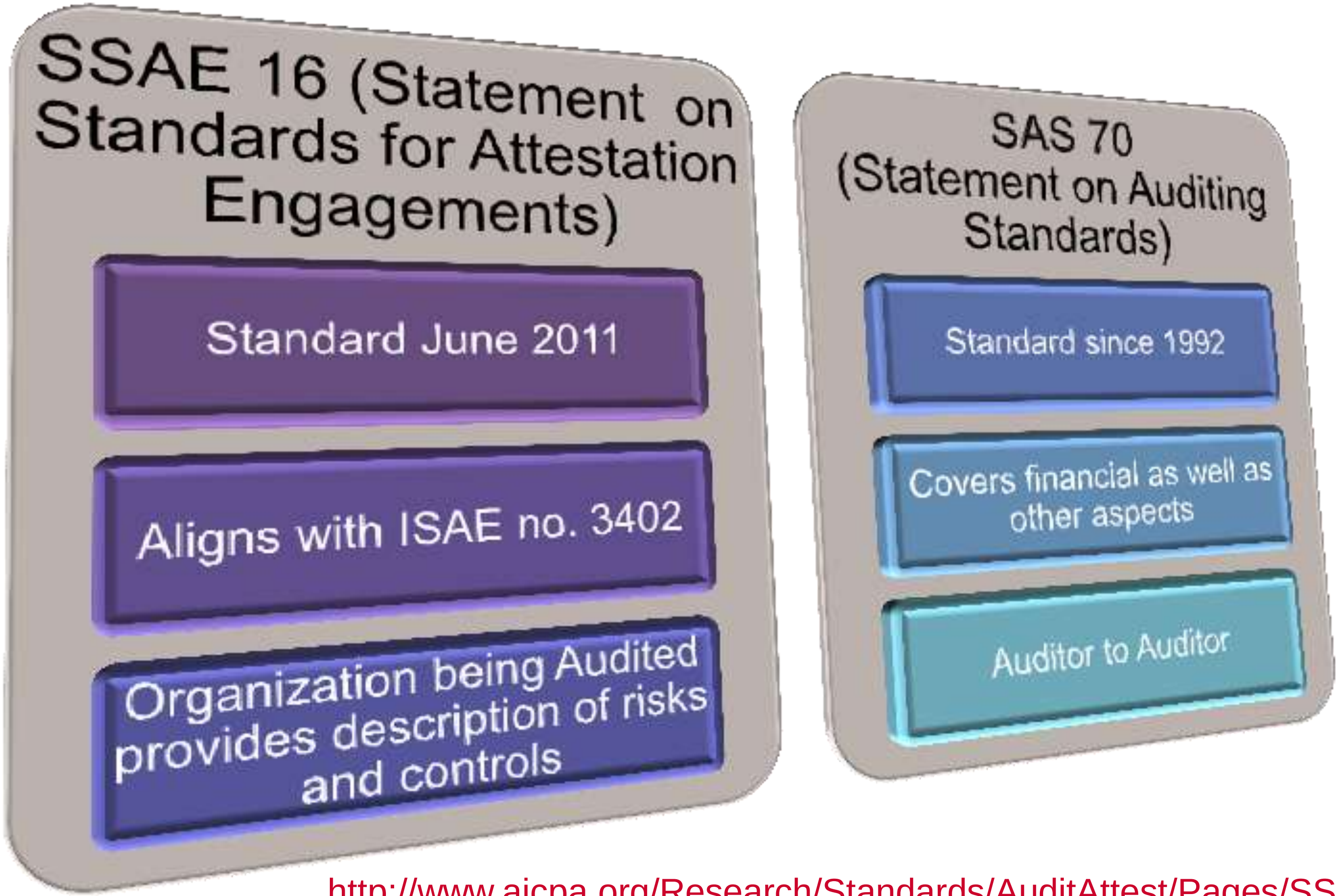
https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/

# CSA Security Trust and Assurance Registry


CSA Open Certification Framework for Cloud services
Level 3: Continuous Monitoring based certification
Level 2: STAR Certification (third party assessment)
Level 1: STAR Self Assessment

https://cloudsecurityalliance.org/research/ocf/

# Independent Assessment



SSAE 16 (Statement on Standards for Attestation Engagements)

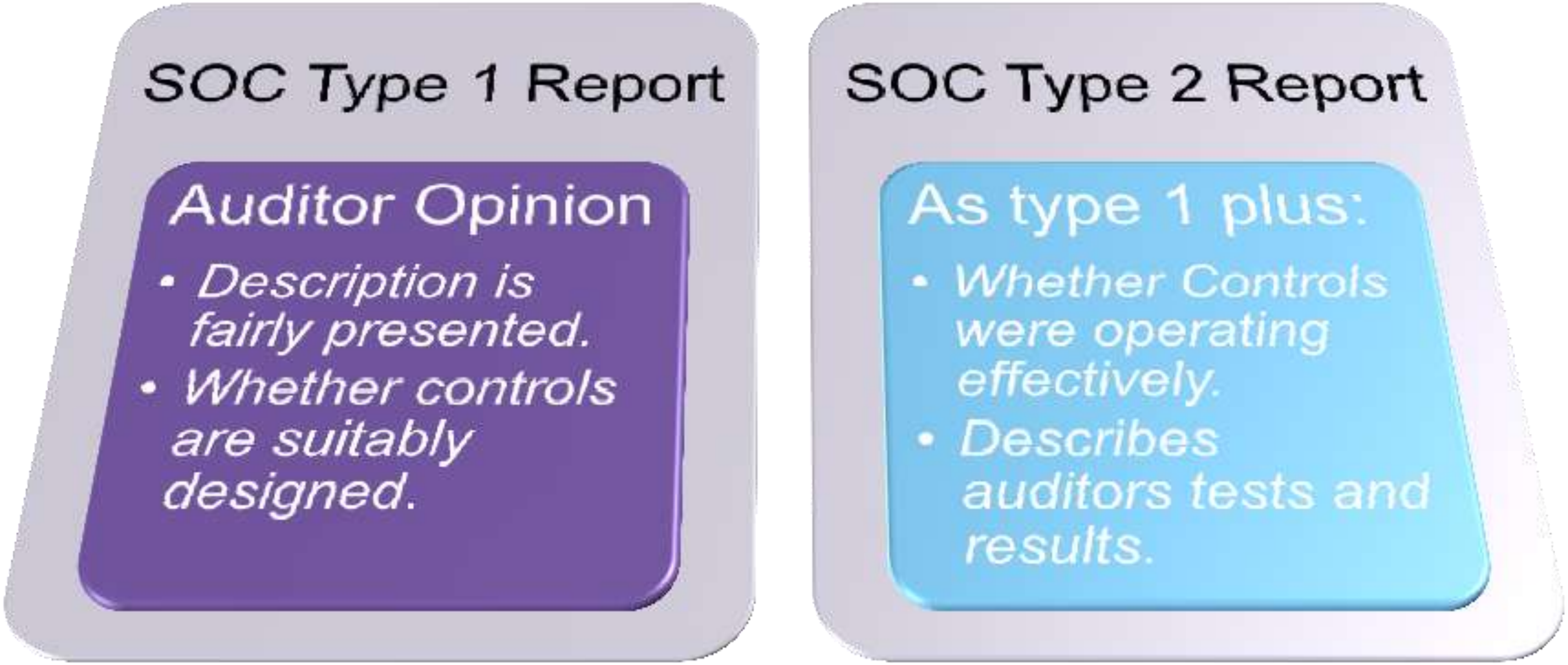
- Standard June 2011
- Aligns with ISAE no. 3402
- Organization being Audited provides description of risks and controls

SAS 70 (Statement on Auditing Standards)

- Standard since 1992
- Covers financial as well as other aspects
- Auditor to Auditor

http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx

# SSAE 16 Reports



SOC Type 1 Report

Auditor Opinion

- *Description is fairly presented.*
- *Whether controls are suitably designed.*

SOC Type 2 Report

As type 1 plus:

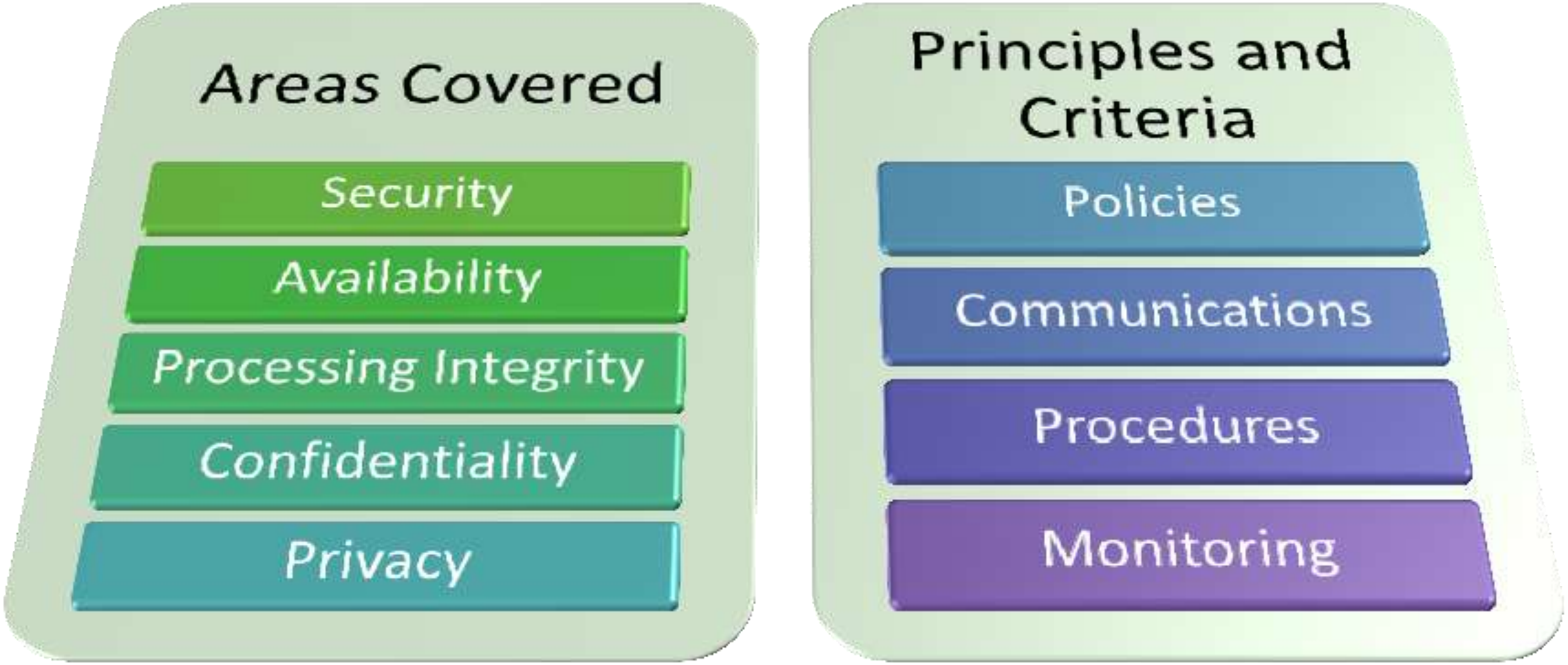
- *Whether Controls were operating effectively.*
- Describes auditors tests and results.

# Example AWS

- SOC 1 Attestation: Control Objectives Attested:
  - Security Organization
  - Amazon Employee Lifecycle
  - Logical Security
  - Secure Data Handling
  - Physical Security
  - Environmental Safeguards
  - Change Management
  - Data Integrity, Availability and Redundancy
  - Incident Handling

http://aws.amazon.com/security/

# AICPA Trust Services



Areas Covered

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

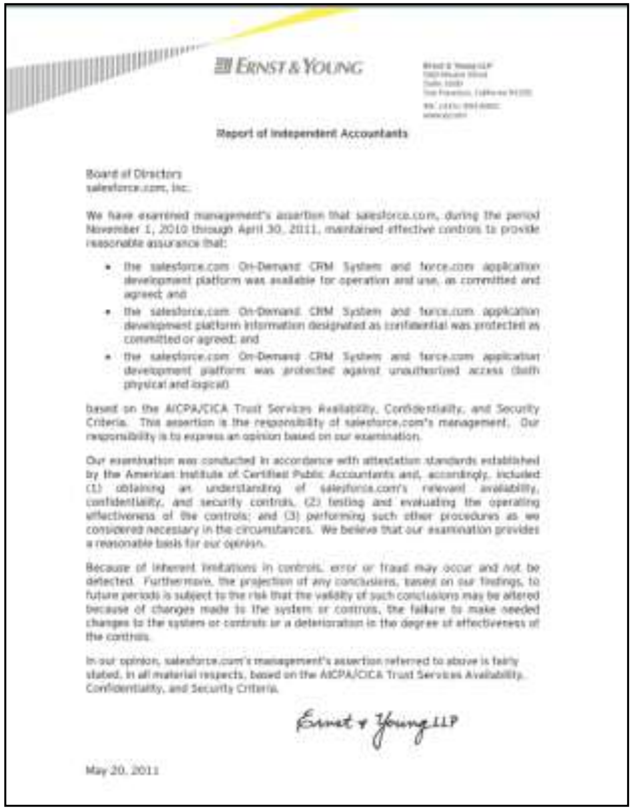
Principles and Criteria

- Policies
- Communications
- Procedures
- Monitoring

http://www.webtrust.org/principles-and-criteria/item27818.pdf

# Example SalesForce.com

- Example based on AICPA Trust Services principles and criteria for:
  - Confidentiality,
  - Availability and
  - Security.



ERNST & YOUNG

Ernst & Young LLP
[illegible]
Suite [illegible]
San Francisco, California [illegible]
Tel: [illegible]
www.ey.com

Report of Independent Accountants

Board of Directors
salesforce.com, inc.

We have examined management's assertion that salesforce.com, during the period November 1, 2010 through April 30, 2011, maintained effective controls to provide reasonable assurance that:

- the salesforce.com On-Demand CRM System and force.com application development platform was available for operation and use, as committed and agreed; and
- the salesforce.com On-Demand CRM System and force.com application development platform information designated as confidential was protected as committed or agreed; and
- the salesforce.com On-Demand CRM System and force.com application development platform was protected against unauthorized access (both physical and logical)

based on the AICPA/CICA Trust Services Availability, Confidentiality, and Security Criteria. This assertion is the responsibility of salesforce.com's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of salesforce.com's relevant availability, confidentiality, and security controls, (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, salesforce.com's management's assertion referred to above is fairly stated, in all material respects, based on the AICPA/CICA Trust Services Availability, Confidentiality, and Security Criteria.

Ernst + Young LLP

May 20, 2011

https://trust.salesforce.com/trust/assets/pdf/Misc_SysTrust.pdf

# ISO/IEC 27001/27002:2005

Information Security Management

Confidentiality, Integrity, Availability

134 Controls

New version expected in 2013

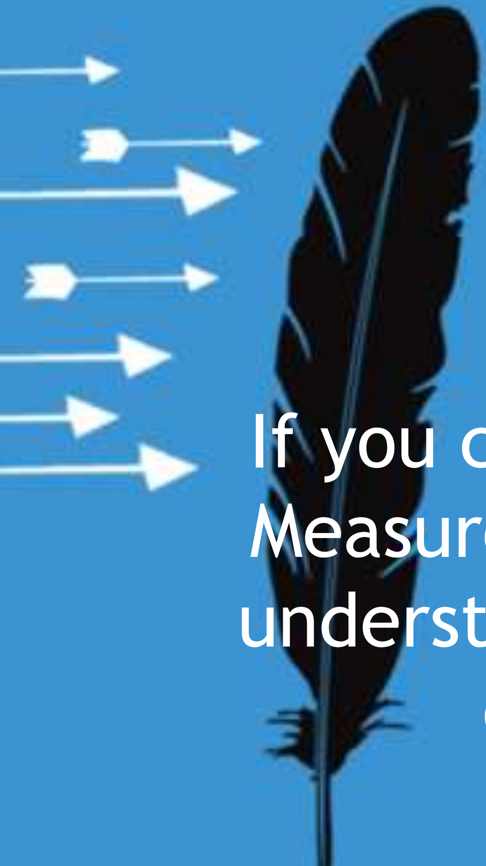
New standard ISO27017 covering Cloud Services in 2013

# Example Microsoft Azure

- **Compliance**
  - **ISO 27001 certification of parts of infrastructure**
  - Safe Harbor signatory
  - Choice data being located within EU
  - New contracts for Office 365 customers in Germany to end uncertainty about the Patriot Act.

http://www.globalfoundationservices.com/security/

# Example Cloud Metrics based on ISO/IEC 27002



If you can’t measure it you can’t manage it. Measurements should be relevant, simple to understand and apply to the Cloud as well as other service delivery models.

# Metrics/SLA Checklist - Data Return

ISO 27001 Control 8.3.2:

- ✓ CCM DG-01 - Data Ownership/Stewardship.
- ✓ Customer owned data clearly identified.
- ✓ Contract specifies ownership of data.
- ✓ Time and cost to return data on termination.
- ✓ Data returned in useable format.

# Metrics/SLA Checklist - Compliance

ISO 27001 Control 15.1.4:

✓ CO-01 to CO-03 Cloud Provider evidence of meeting compliance requirements.

✓ Geographic Location of data and Infrastructure: EU, US Safe Harbor, …

✓ Cloud provider does not use other companies whose infrastructure is located outside that of the provider.

✓ Cloud provider's services are not subcontracted or outsourced.

# Metrics/SLA Checklist - Business Continuity

ISO 27001 Control 14:

- ✓ RS-01 to RS-04 Resiliency Management.
- ✓ Details of availability measurement and metrics.
- ✓ Details of data backup and restore.
- ✓ Details of how technical changes are managed.
- ✓ Business continuity processes exist.
- ✓ Customer activities included in plans.

# Summary

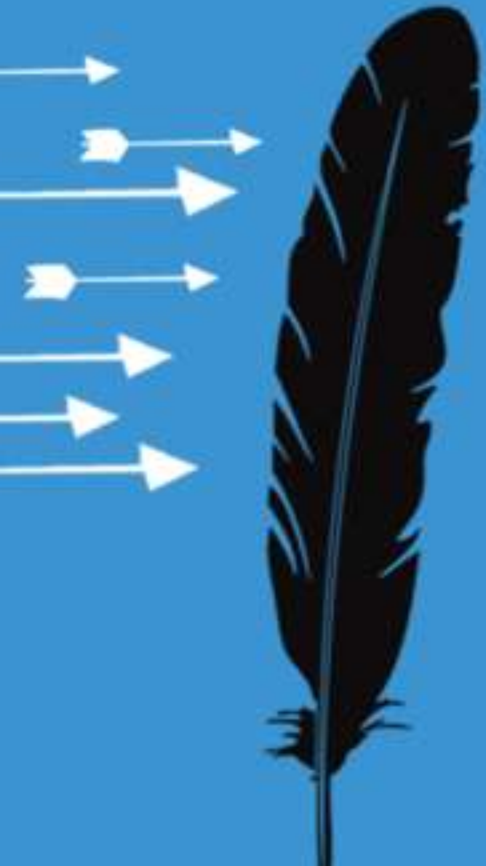
Trust but Verify
An old Russian maxim –
(Доверяй, но проверяй)
– often quoted by President Ronald Regan

# Summary

- Trust in the Cloud depends upon your needs, provider processes and independent assurance.
    - Choose the right Cloud based on business need and risk appetite.
    - Understand the value and sensitivity of data.
    - Specify clearly the service and responsibilities.
    - Specify the controls and monitor them.  Frameworks help.
    - Understand what independent certifications and audit reports mean.
- Trust but Verify

# How to Apply what You Learned Today

- In the first three months following this presentation you should:
  - Identify a cloud service that you are using or plan to use
  - Understand the business requirements for this service
  - List the risks associated with the use of the service
  - Compare these risks with the assurances being offered by the provider. Check what is being monitored and how.
- Within six months you should:
  - Extend the above activities to cover the other cloud services in use or being planned
  - Drive a project to set up a standard process for acquiring cloud services to meet the risk appetite of the organization.



# Questions?

The Future of Information Security - Today.

**KuppingerCole** supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company **KuppingerCole** provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

**Kuppinger Cole Ltd.**

Headquarter
Arnheimer Str. 46
D-40489 Düsseldorf | Germany

Phone +49 (211) 23 70 77 - 0
Fax +49 (211) 23 70 77 - 11

www.kuppingercole.com
clients@kuppingercole.com

Mike Small CEng, FBCS, CITP
Senior Analyst, KuppingerCole
www.kuppingercole.com

Email: Mike.Small@kuppingercole.com

Mobile: +44 7777 697 300

*ISACA UK Chapter Member*

# Information Sources #1

- AICPA
  - Statement  on Standards for Attestation Engagements
  - http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx
- BITS Shared Assessments
  - Evaluating Cloud Risk for the Enterprise
  - http://www.sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf
- BSI (German Federal Office for Information Security)
  - Security Recommendations for Cloud Computing Providers
  - https://www.bsi.bund.de/
- Cloud Security Alliance:
  - Cloud Controls Matrix
  - https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/
  - Open Certification Framework for Cloud service
  - https://cloudsecurityalliance.org/research/ocf/

# Information Sources #2

- ENISA
  - Cloud Computing: Benefits, risks and recommendations for information security.
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
  - Procure Secure: A guide to monitoring of security service levels in cloud contracts.
  - http://www.enisa.europa.eu/activities/application-security/test/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
- International Standards for Assurance Engagements
  - (ISAE) No. 3402
  - http://isae3402.com/

# Information Sources #3

- ISACA:
  - COBIT 5
  - Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives
  - Cloud Computing Management Audit/Assurance Program
  - IT Control Objectives for Cloud Computing
  - http://www.isaca.org/
- ISO 27001
  - Code of practice for information security management
  - http://www.iso.ch
- KuppingerCole
  - Scenario Report: Understanding Cloud Security - 70321
  - http://www.kuppingercole.com/report/mkms_senunderstandingcloudsecurity7032111072012
  - Advisory Report: Cloud Provider Assurance - 70586

# Information Sources #4

- NIST
  - Cloud Computing Synopsis and Recommendations
  - http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075
- NTT
  - Standardization Activities for Cloud Computing
  - https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201106gls.pdf&mode=show_pdf
- Systrust/WebTrust:
  - Principles and Criteria
  - http://www.webtrust.org/principles-and-criteria/item27818.pdf