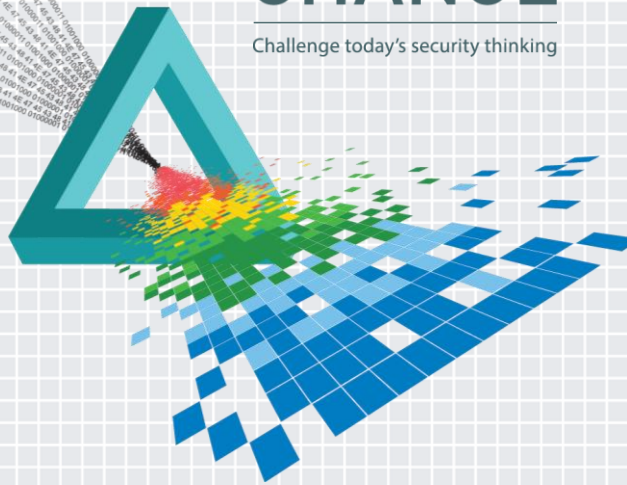
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: CXO-R01

Compliance by Design

Using Innovation to Beat the Compliance Rat-Race

Hayden Delaney
Partner, ICT and Data Protection
HopgoodGanim Lawyers
@HaydenDelaney_1

Bob Griffin
Chief Security Architect
RSA, the Security Division of EMC
@RobtWesGriffin

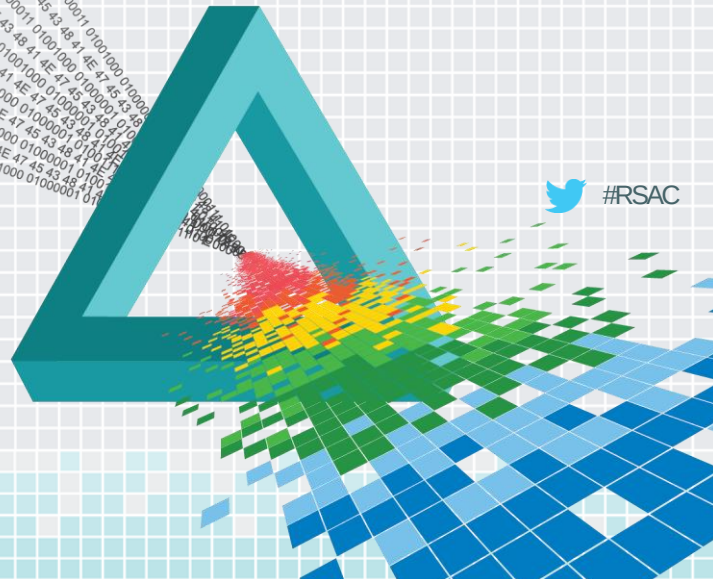
RSAConference2015

San Francisco | April 20-24 | Moscone Center

The Compliance Challenge (Hayden)

A Strategy for Compliance by Design (Bob)

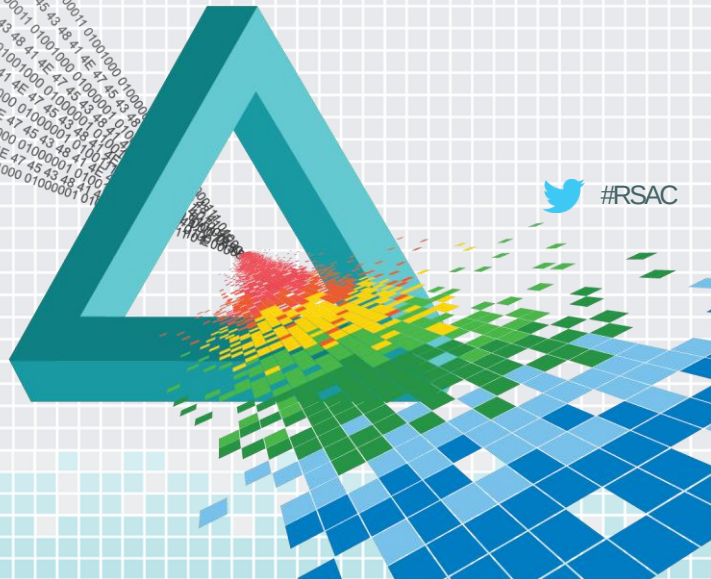
Leveraging Standards in Compliance by Design (Hayden and Bob)



RSAConference2015

San Francisco | April 20-24 | Moscone Center

The Compliance Challenge



#RSAC

Why privacy + security matters

"*At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a valuable asset and people will be tempted to trade and do commerce with that asset.*"

Alex Grove, 2000, Former CEO of Intel Corporation

Data ecosystem

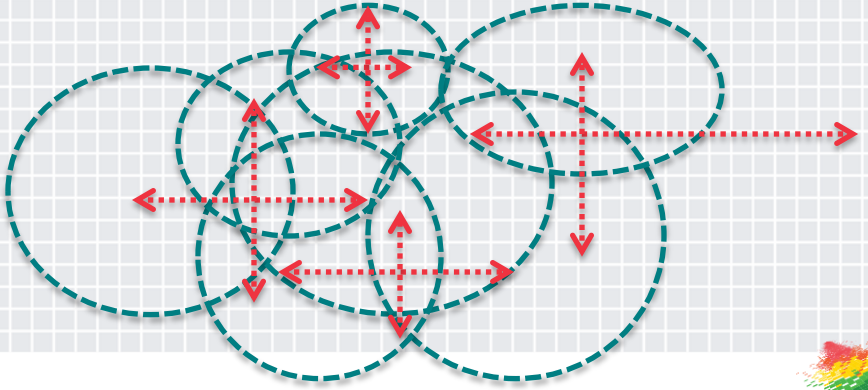
- Data Complexity
  - More data = more noise
- Data Emergence
  - The calculus of privacy & data sovereignty
- Data self-organisation
  - Datasets interact with one-another, modifying the data ecosystem, producing more knowledge – *for example...*

Legal, industry & consumer response framework

- Complex: privacy and data-related law reform at a global level.
- Multi-layered regulatory frame work:
  - Informational privacy + data protection (e.g., Privacy Act (Aus), *Personal Information Protection and Electronic Documents Act* or “PIPEDA” (Canada), EU Data Directive, etc)
  - Data breach notification (e.g., California S.B. 1386 or proposed Aust laws)
  - Anti- spam (e.g., Spam Act 2003 (Aust), CASL (Canada), CAN SPAM (US) etc)
  - Industry regulation & standards (PCI DSS, KMIP, PKCS, etc)

Data is a hard beast to tame

- Data is BIG and it flows seamlessly.
- Data collection, use, disclosure is regulated & creates risk.
- Cloud and the Internet of Things (IoT) make it hard to control.
- We **want** the benefits **but not** the risk and loss of control.
- How do we resolve this?



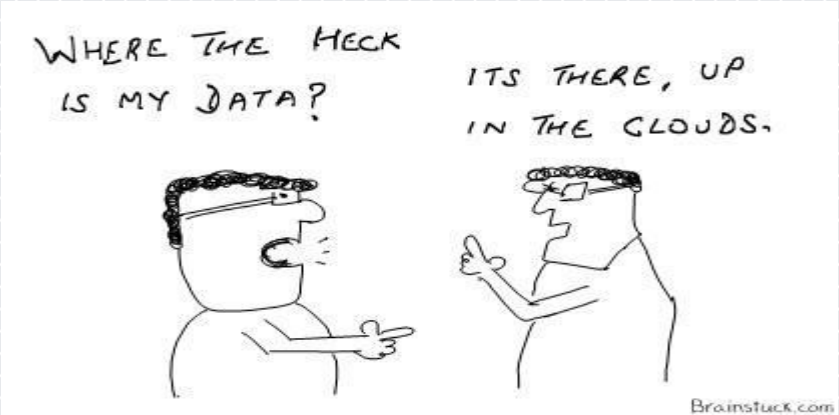
Maybe we're asking the wrong questions?

- The answer ≠ "just encrypt it".
- The issue is not use X algorithm or use ABC vendor.
- The issue not (necessarily) just all about data (or at least encrypted data).
- Instead, we need to turn the debate to *key management*, *visibility* and *interoperability.*

Data sovereignty

- Once data leaves a jurisdiction's borders, other laws apply (and not always the good type) + loss of physical control.

- Data sovereignty is not solely a privacy issue
  - Business sensitive information
  - Confidential information
  - Ownership



Data sovereignty & cross border disclosures in Australia

- Cross border disclosure of personal information (*Privacy Act, APP 8*):

  Before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles

- A focus on ongoing accountability (*Privacy Act,* Section 16C):

  Acts of overseas recipients of personal information (in summary)

  Where:

  a) An Australian entity discloses personal information about an individual to an overseas recipient; and

  b) The overseas recipient breaches the Australian Privacy Principles; then

  that act is taken to have been done by the Australian disclosing entity.

Case study: Apple's solution to data sovereignty & privacy

- Consider the risk environment:
  - Broad government data access laws via *Patriot Act* brought starkly to light by the Snowden leaks
  - Consumer concerns around personal privacy (e.g., Government access (Snowden) and also malicious access (e.g., Celebrity iCloud leaks))
- Business value (*probably* the real reason):
  - Money, money, money
  - Apple seeking to create an environment where financial transactions can be conducted via biometric finger scanner
  - Laws requiring authentication for financial transactions
- The solution - engineering control
  - Not (effectively) holding the data (despite actually holding it via Apple's cloud infrastructure)
  - Encryption keys wrapped in user device & linked to biometric finger print scanner

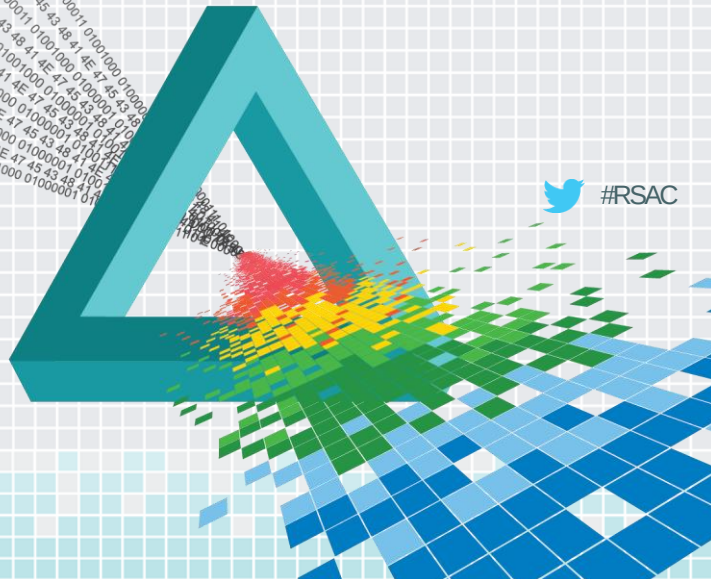
Marketing and big data – the legal challenge

- The drive to communicate with customers is key to business.
- Organisations operating in multiple jurisdictions, with geographically dispersed retail outlets, the compliance problem is massive.
- Compliance requirements vary between:
  - Communication medium (e.g., Email, SMTP messages, SMPP messages, telephone calls)
  - Jurisdiction (CASL for Canada, CAN SPAM and Telephone Consumer Protection Act of USA, Spam Act and Do Not Call Register Act for Aus)
- A compliance strategy is discussed later.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

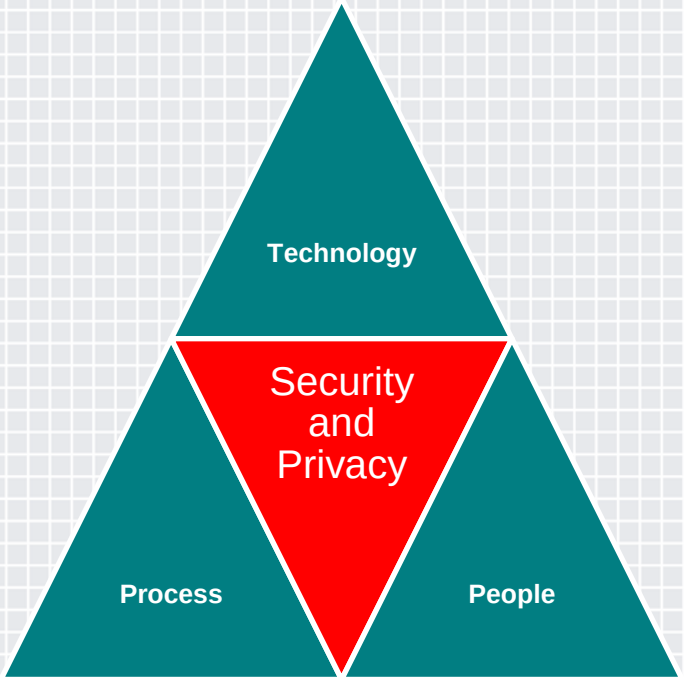
A Strategy for Compliance by Design



#RSAC

Operating in harmony

Business value



Legal and Compliance

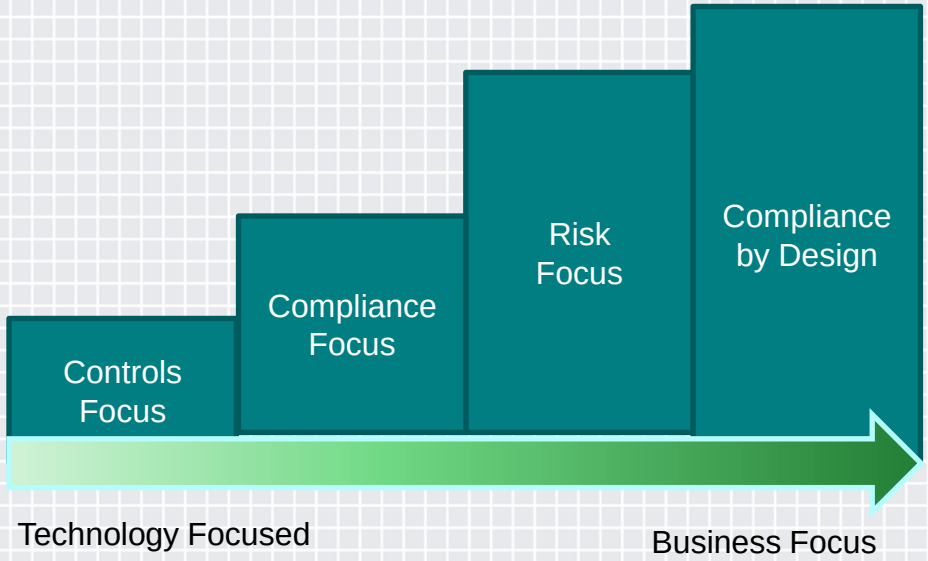
Design

Disruption: an opportunity for transformation

Infrastructure Transformation	Business and Legal Transformation	Threat Landscape Transformation

http://www.emc.com/collateral/industry-overview/h11391-rpt-information-security-shake-up.pdf?pid=sbiclandingpage-sbicspecialreport-122112

A change in strategy



Enabling "Compliance by Design"

Communication Valley Reply (Italy)

- Requirements:
  - Reduce cost of compliance reporting
  - Efficient, cost-effective management of security
  - Reduced cost of service delivery
  - Improved service as competitive advantage
- Solution:
  - Automatically track and report on client risk and compliance
  - Enhance incident triage
  - Improve event analysis

http://www.emc.com/collateral/customer-profiles/h11982-reply-cp.pdf

Risk discipline across the organization

CIO & CISO

Board

LOB Executives

Business Operations Managers

IT ..... **Business**

IT Security Risk	Regulatory & Corporate Compliance	Operational & Enterprise Risk
Business Resiliency	Audit	Third Party & Vendor Risk

Common Foundation

Silos → Managed → Advantaged

Maturity

Identity governance across the organization

Trusted interactions between identities and information

Employees/Partners/Customers

Access Platform

Authentication

Federation/SSO

Identity Intelligence

Governance Platform

Compliance

Identity Lifecycle

Provisioning

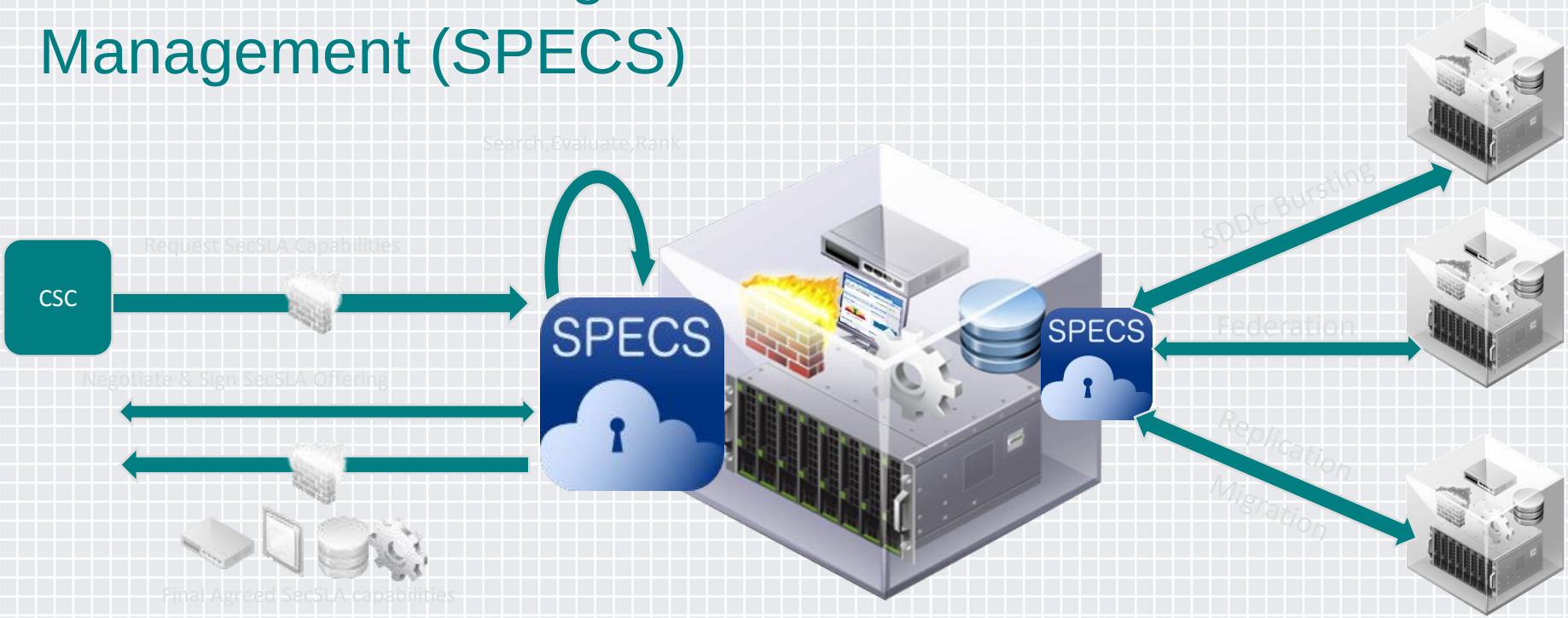
Applications/Data/Resources

Security analytics across the organization

Capture, analyze and act on data from across the enterprise.

What about leveraging standards?

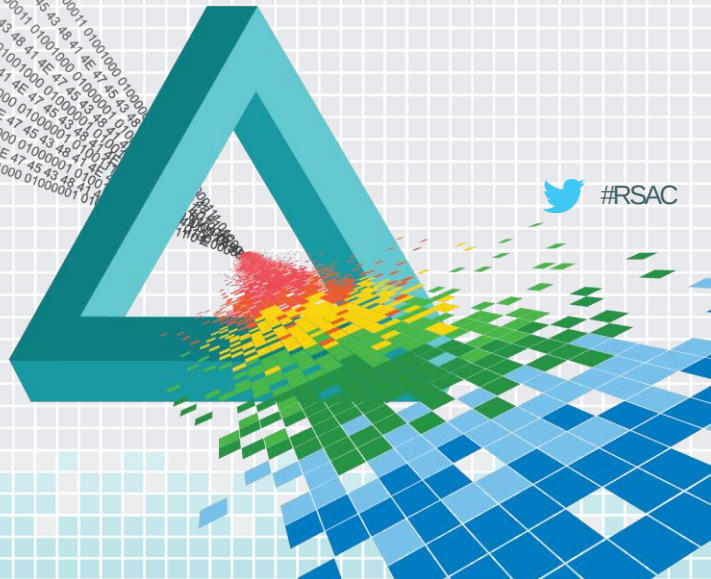
Secure Provisioning of Cloud Services based on SLA Management (SPECS)



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Leveraging Standards in Compliance by Design

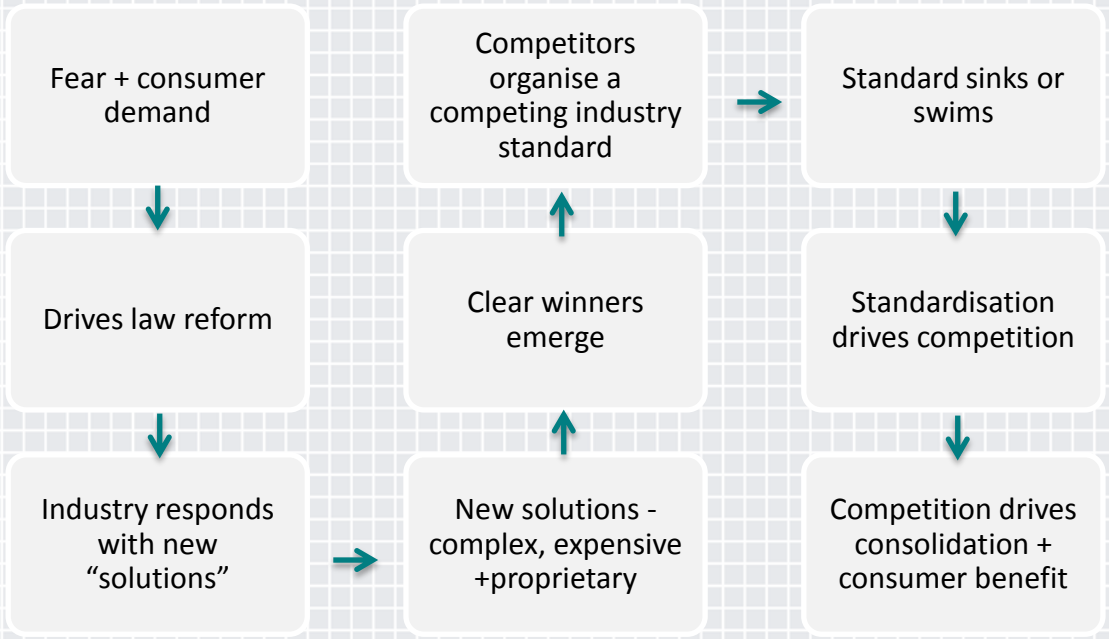


#RSAC

How does one decide?

- **Popularity test** - follow the crowd
- **Fashion test** – pick your favourite vendor and follow them
- **Simplicity test** – weigh the standards
- **Complexity test** – run tools over the standards document
- **Taste test** - read the standards

The natural evolution of standards

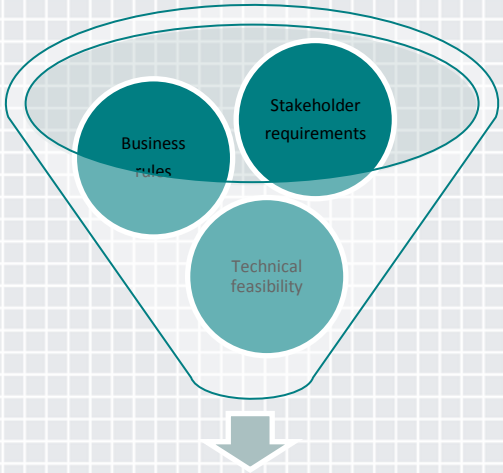


Interoperability in “Compliance by Design”

- Interoperability:
  - Creates competition
  - Helps prevent vendor-lock in
  - Mitigates business continuity risk
- Interoperability standards:
  - Make acquisition and use of ICT products streamlined
  - Transparency – for improved governance and audit
  - Consistent semantics enable analytics

Interoperability reduces complexity

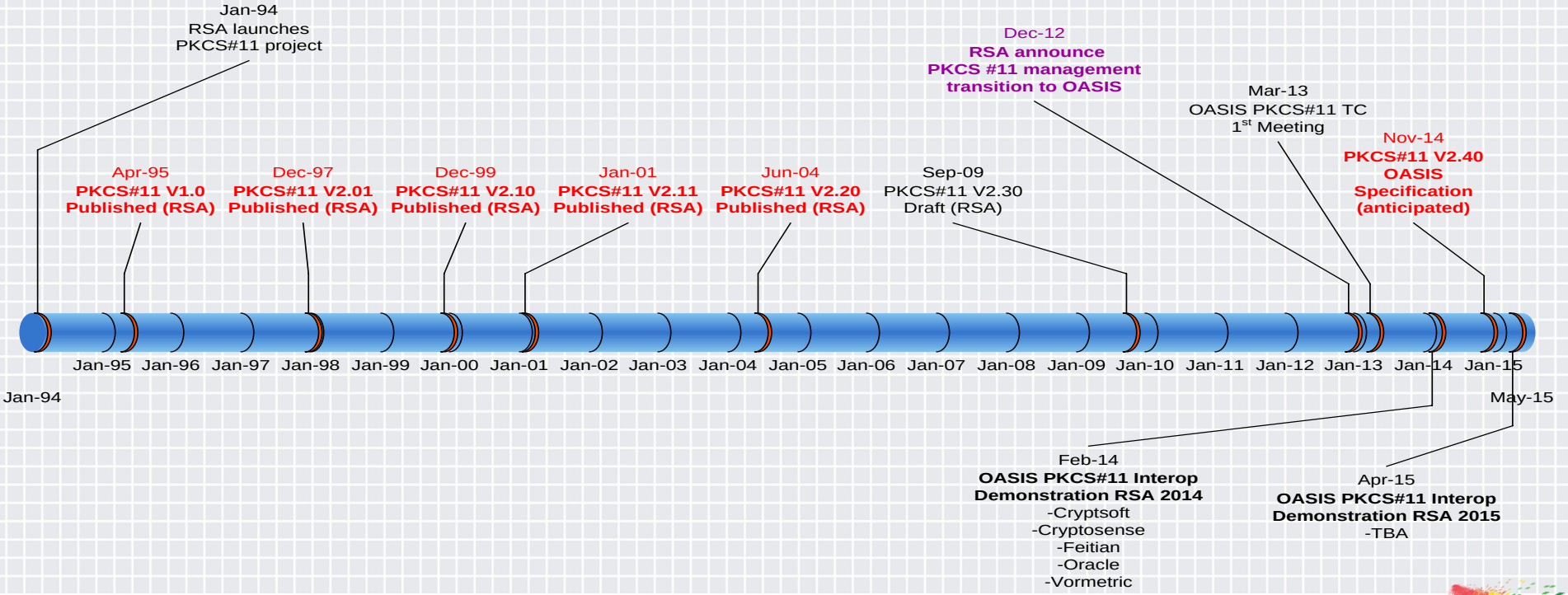
- Interoperability in ICT procurement:
  - Mandatory requirement
  - Measurable targets
- Consider:
  - Interoperability warranties at procurement
  - Interoperability in transition-out
  - Warranties covering standards compliance
  - False standards – beware!



Examples of interoperability standards

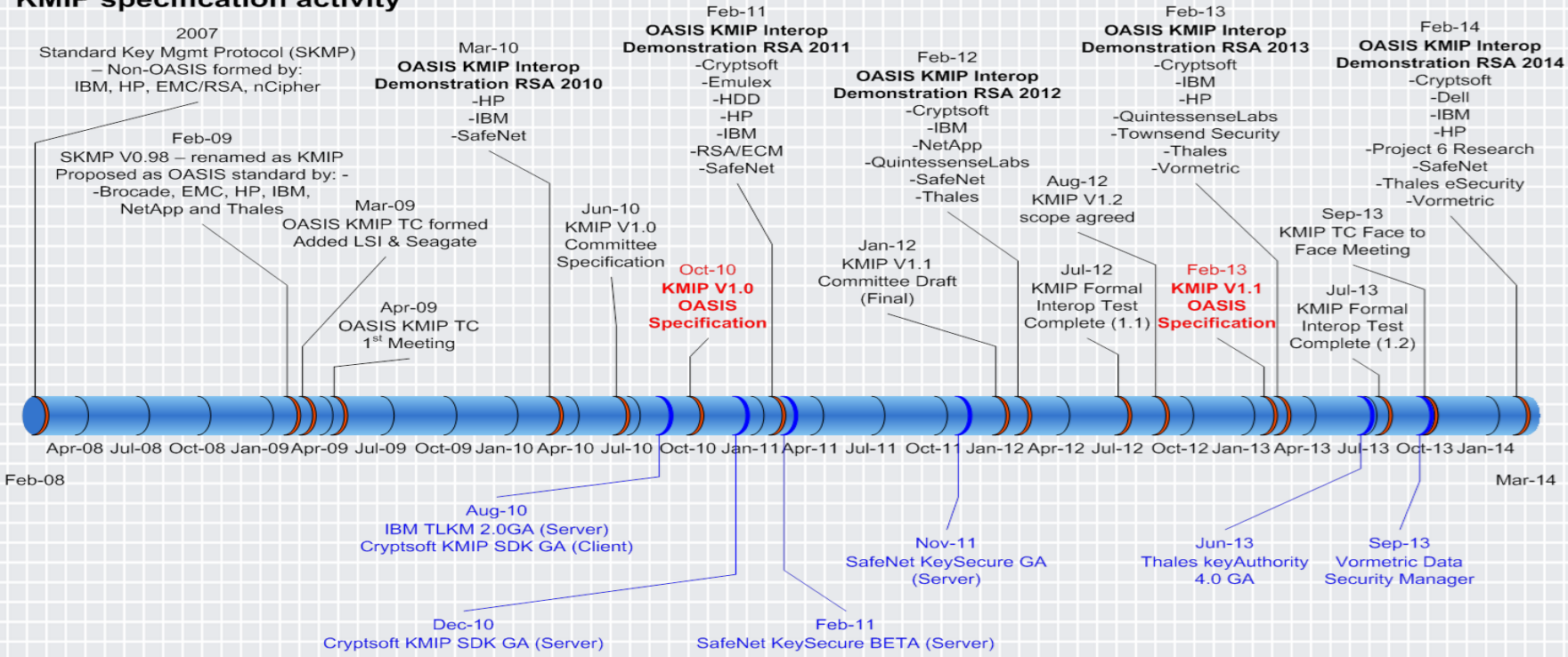
- PKCS#11
- OASIS Key Management Interoperability Protocol (KMIP)

PKCS#11


Jan-94
RSA launches
PKCS#11 project
Apr-95
PKCS#11 V1.0
Published (RSA)
Dec-97
PKCS#11 V2.01
Published (RSA)
Dec-99
PKCS#11 V2.10
Published (RSA)
Jan-01
PKCS#11 V2.11
Published (RSA)
Jun-04
PKCS#11 V2.20
Published (RSA)
Sep-09
PKCS#11 V2.30
Draft (RSA)
Dec-12
RSA announce
PKCS #11 management
transition to OASIS
Mar-13
OASIS PKCS#11 TC
1st Meeting
Nov-14
PKCS#11 V2.40
OASIS
Specification
(anticipated)
Jan-94
Jan-95 Jan-96 Jan-97 Jan-98 Jan-99 Jan-00 Jan-01 Jan-02 Jan-03 Jan-04 Jan-05 Jan-06 Jan-07 Jan-08 Jan-09 Jan-10 Jan-11 Jan-12 Jan-13 Jan-14 Jan-15
May-15
Feb-14
OASIS PKCS#11 Interop
Demonstration RSA 2014
-Cryptsoft
-Cryptosense
-Feitian
-Oracle
-Vormetric
Apr-15
OASIS PKCS#11 Interop
Demonstration RSA 2015
-TBA

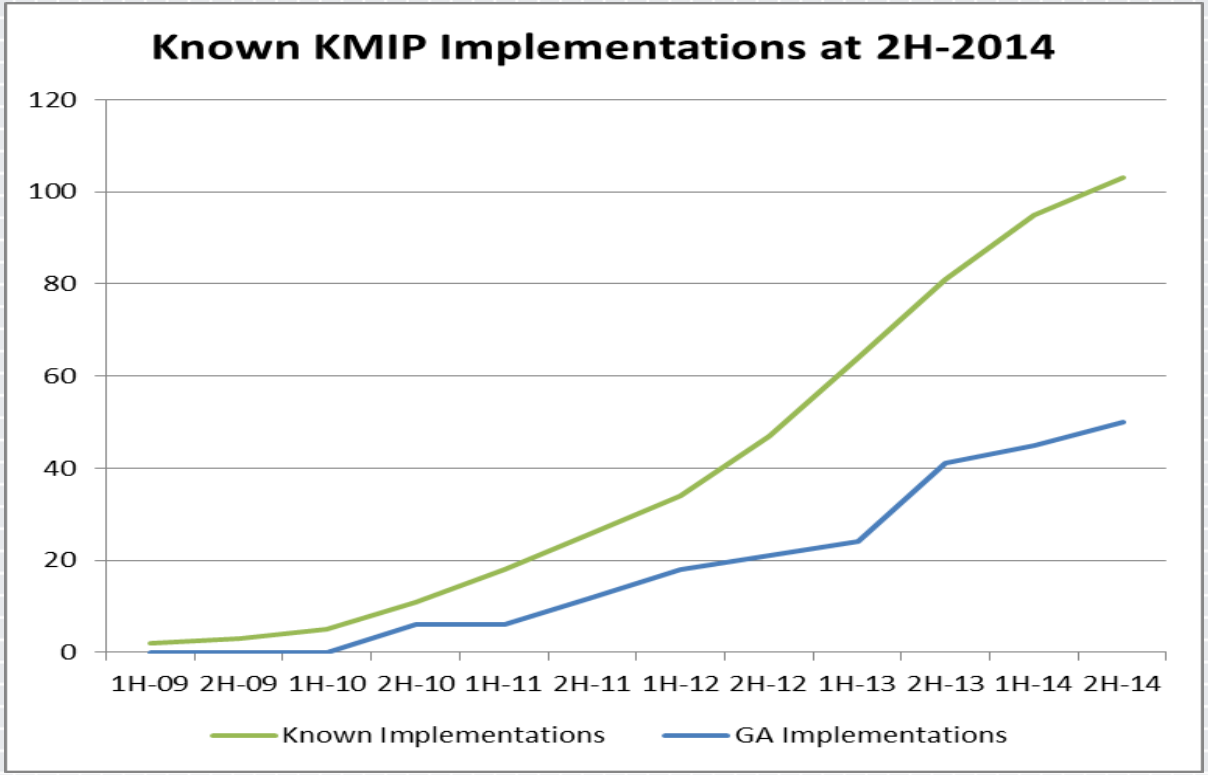
OASIS KMIP

KMIP specification activity



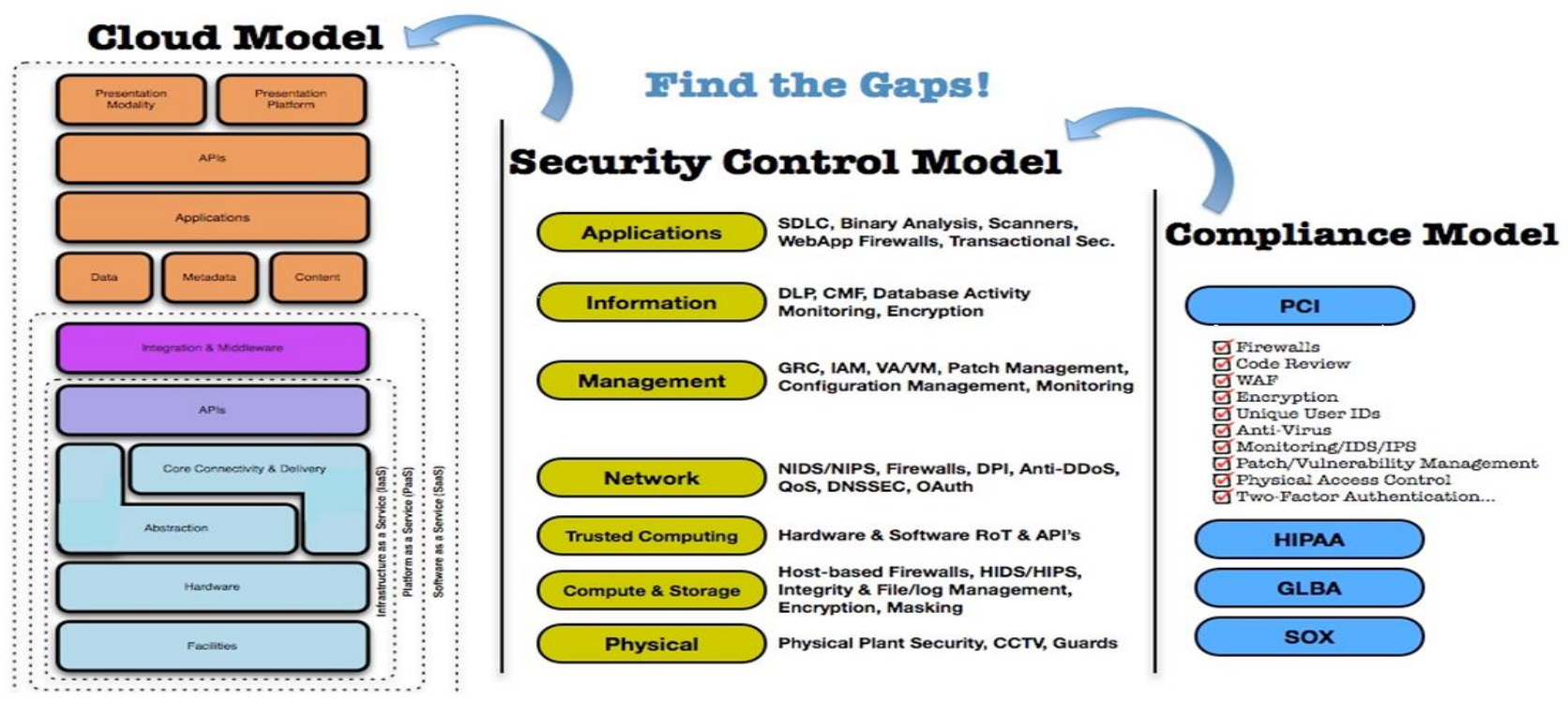
Vendor (server) product activity

Interoperability: KMIP Adoption

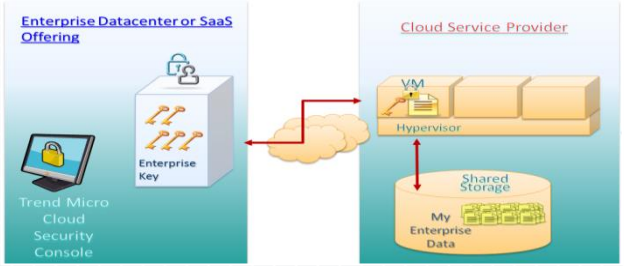


Source: Cryptsoft

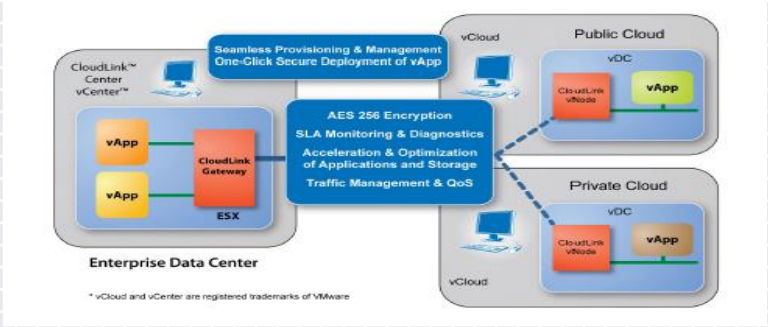
Security architectures



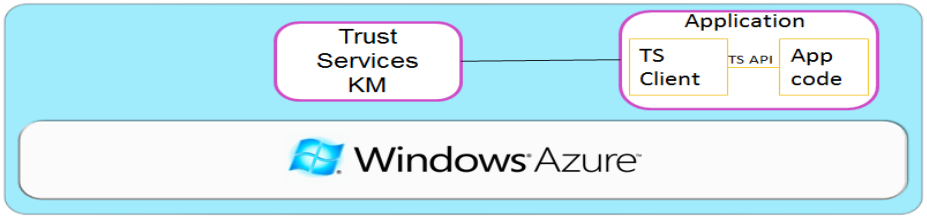
Cloud security architectures - encryption



Model 1
Enterprise
Key Management



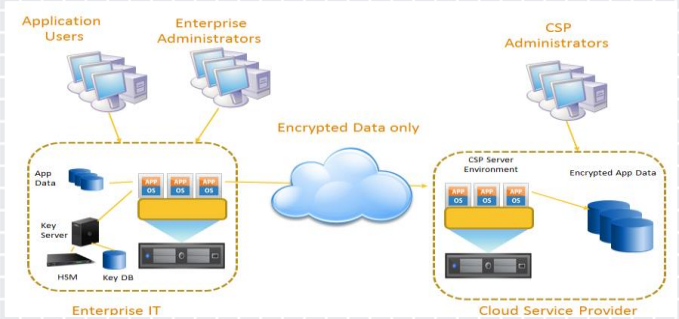
Model 2
Hybrid
Key
Management

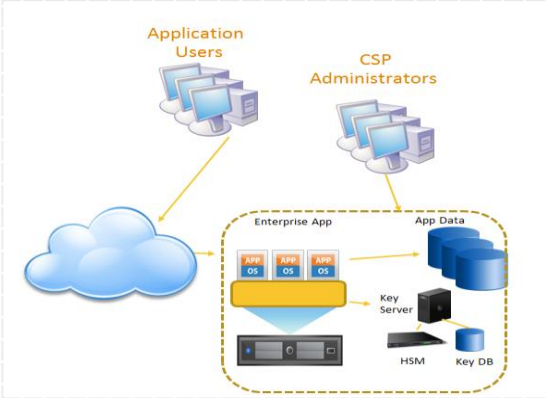


Model 3
CSP Key Management

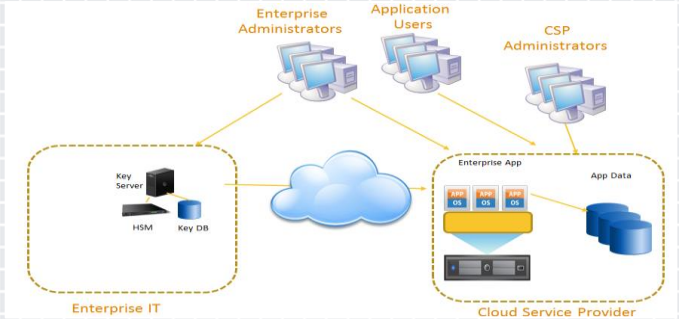
Cloud security architectures – encryption key management

Model 1
Enterprise
Key Management





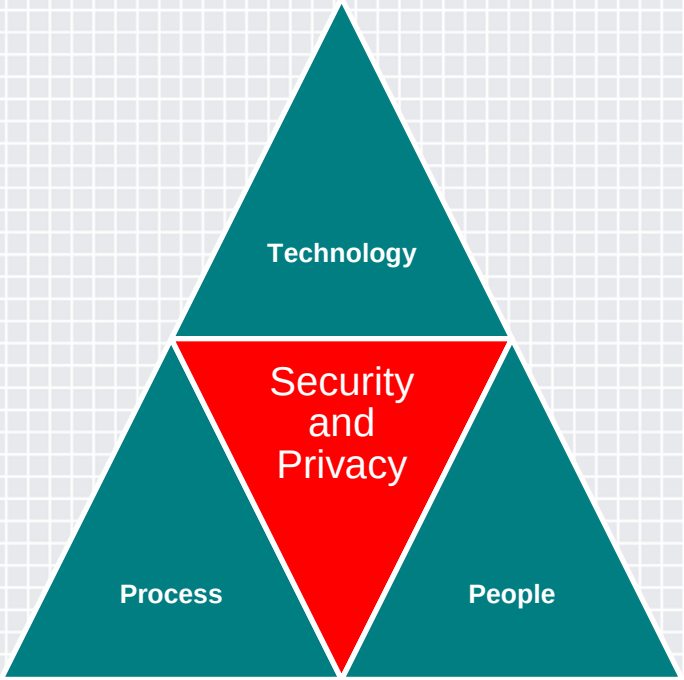
Model 2
Hybrid
Key
Management



Model 3
CSP
Key
Management

Compliance by Design

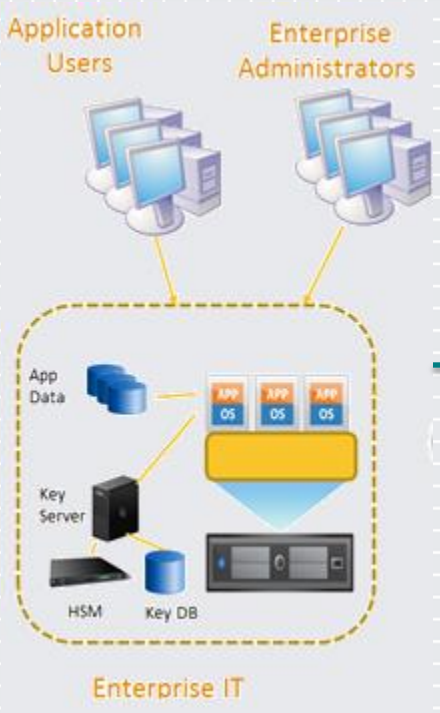
Business value



Legal and Compliance

Design

Resolving a problem via key management: Public cloud data sovereignty



Encrypted data only

CSP California data centre

CSP Ireland data centre

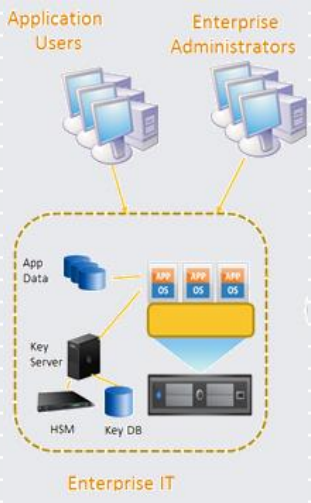
CSP Sydney data centre

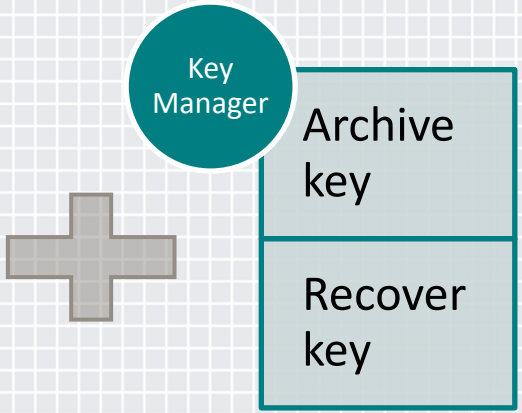
Resolving a problem via key management: Data breach & notification

- Key questions (by reference to **California S.B. 1386**):
  - Does data include "personal information?
  - Does "personal information" relate to a California resident?
  - Was the "personal information" unencrypted?

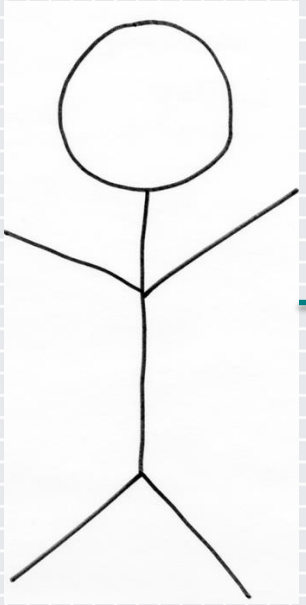
Resolving a problem: beyond use data

- Most jurisdictions with informational privacy laws support the de-identification and minimization of personal information. Consider strengths of KMIP standard

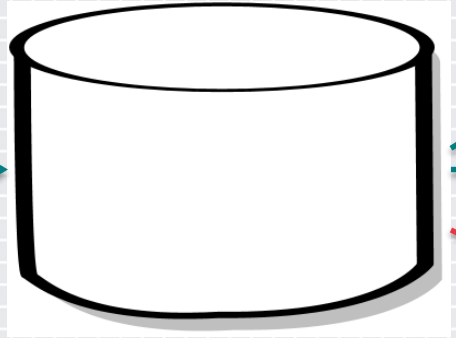




Resolving marketing compliance: consent database



Gives consent + customer-defined preferences



Email

SMPP

Text message

SMTP

Telemarketing

Captures:

- Contact mediums
- Uses & disclosures
- Duration
- Jurisdictions (data sovereignty)

Apply what you have learned today

- Next week you should:
  - Identify opportunities for applying compliance by design
  - Ask your vendor if they support enterprise key management
  - Ask your vendor if they support interoperability in cloud environments
- In the first three months following this presentation you should:
  - Define a project to evaluate compliance by design
- Within six months you should:
  - Drive an implementation to evaluate compliance by design

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You!