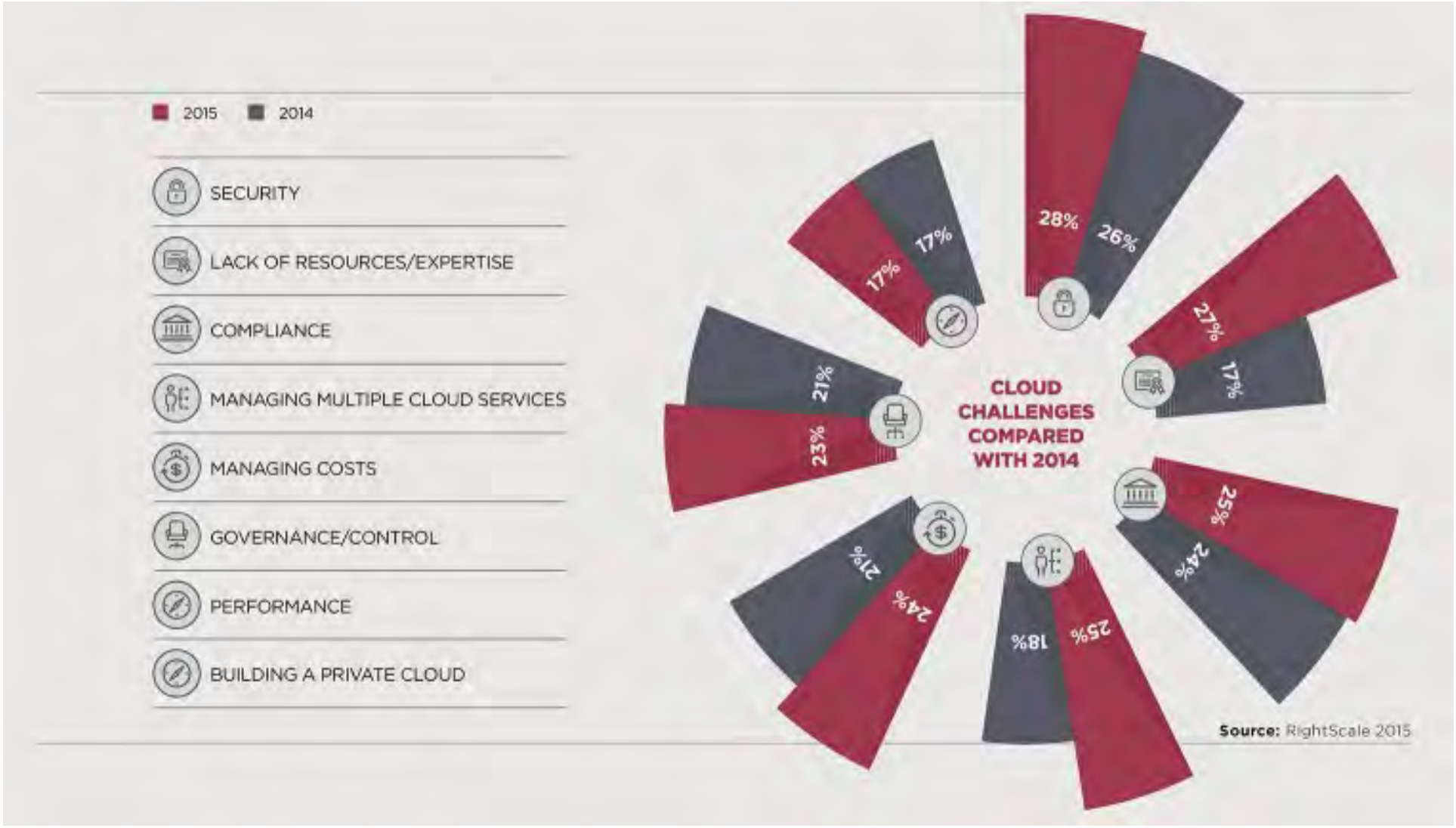
ITU-TRCSL Symposium on Cloud Computing

(28-30 July 2015 Colombo Sri Lanka)

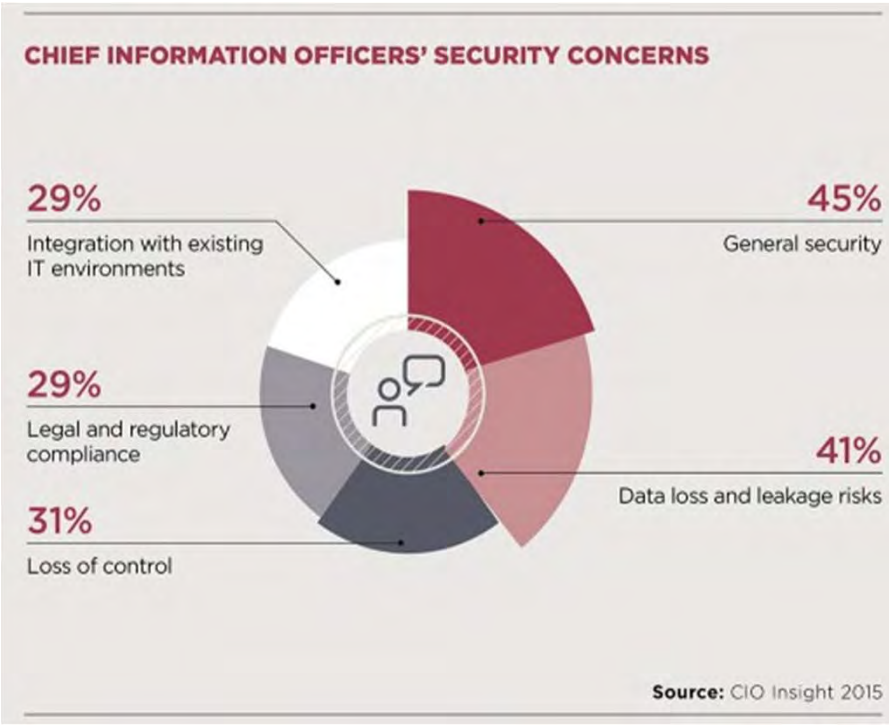
Cloud Security Challenges and Solutions

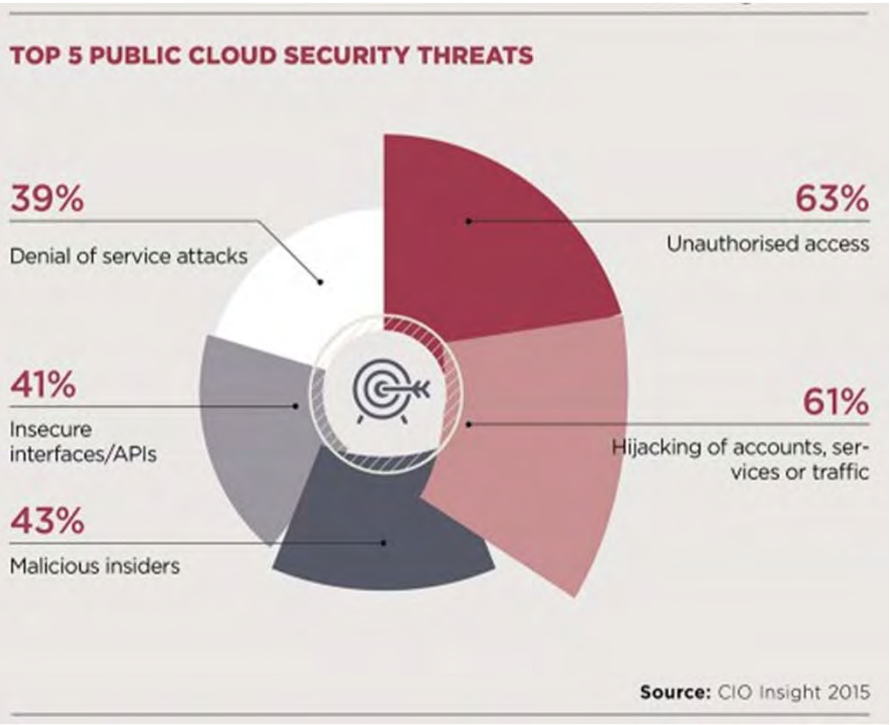
Jayaraj Sayanthan
Lead Engineering Manager – IDC and Cloud
Dialog Axiata PLC

Evolving Cloud Computing Challenges

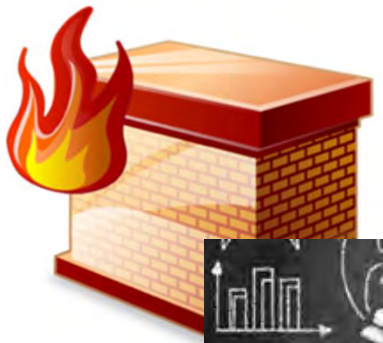


Cloud Security Concerns and Threats

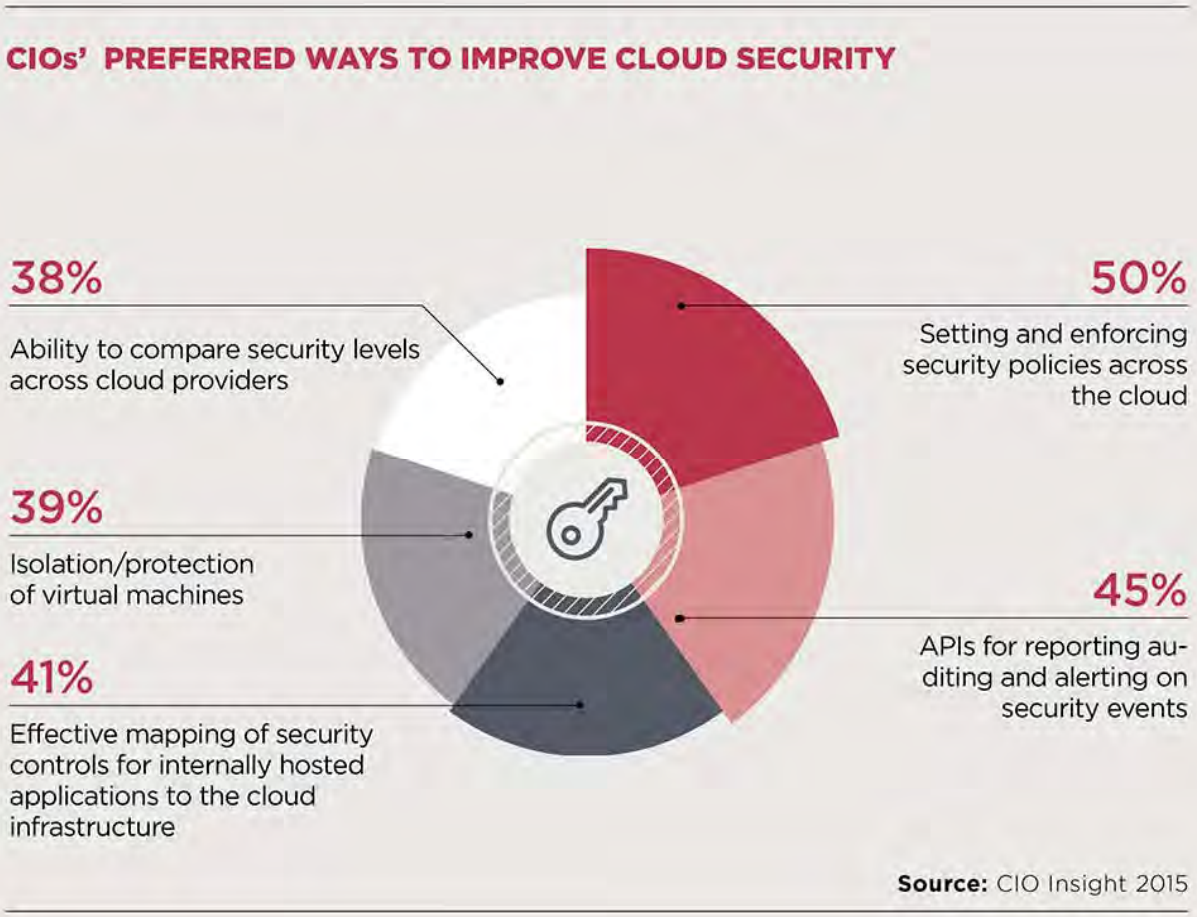




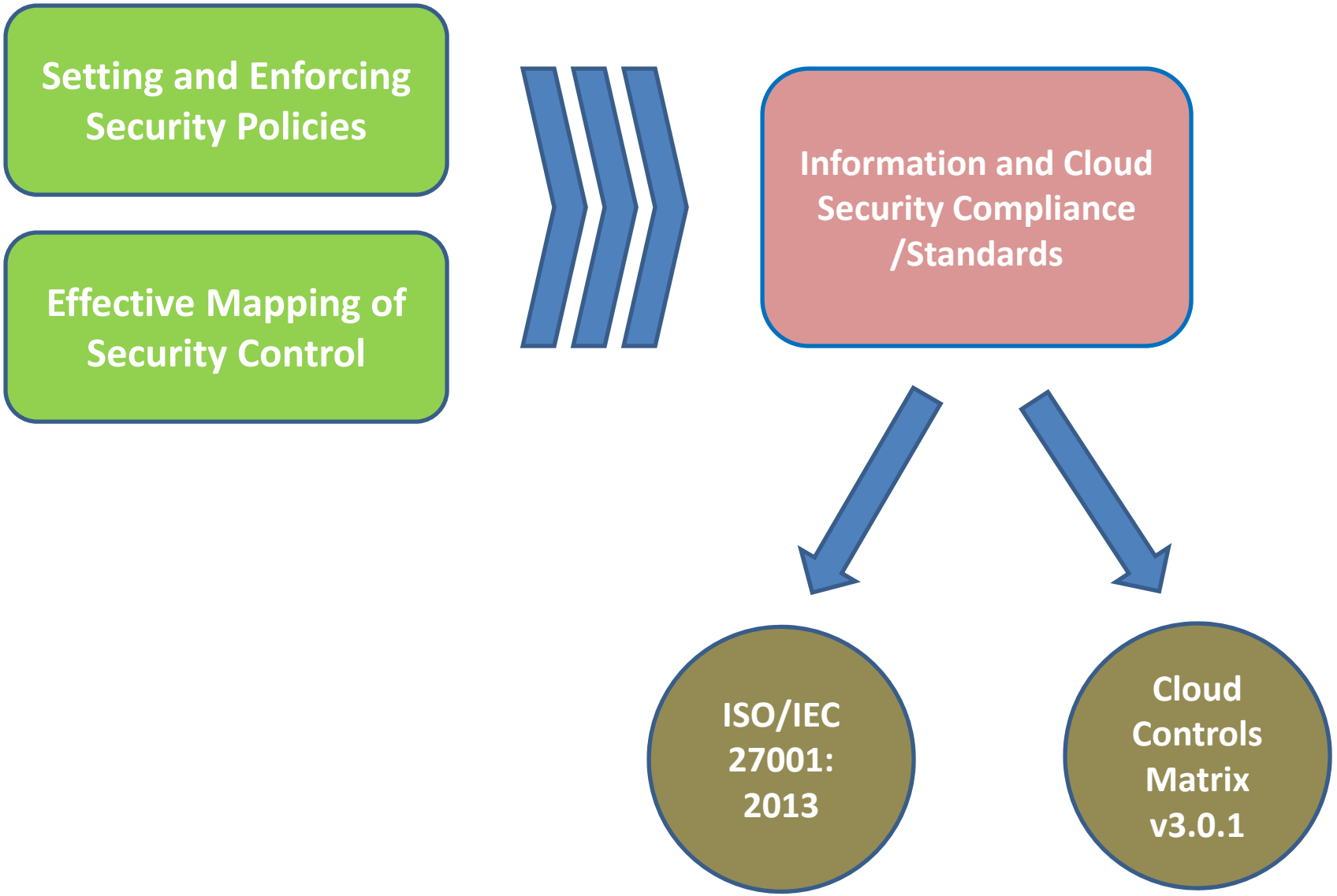
Cloud Security and Defense Plans (lots of devices???)



CIO's Preferred Ways to Improve Cloud Security



What are we missing? and Bridging the gap…!!!



ISO/IEC 27000 – a success story

Original requirement identified by the Department of Trade and Industry (DTI) in late 1980s

- UK companies held back by lack of information security advice and guidance
- Market needed a “code of practice”

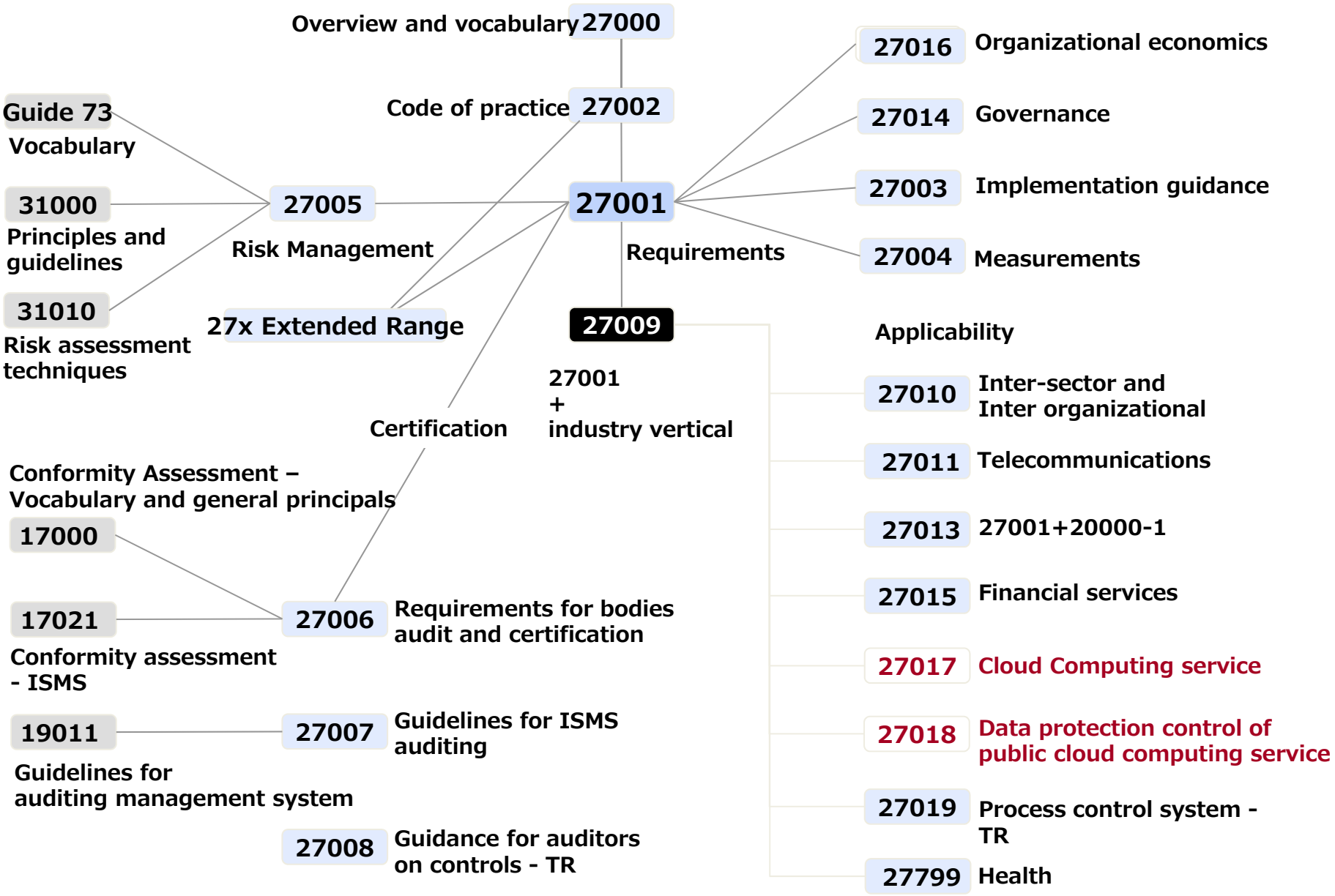
Developed for DTI, published by BSI

Became a British Standard, BS 7799, in 1995 and Certification standard BS 7799-2 followed in 1999

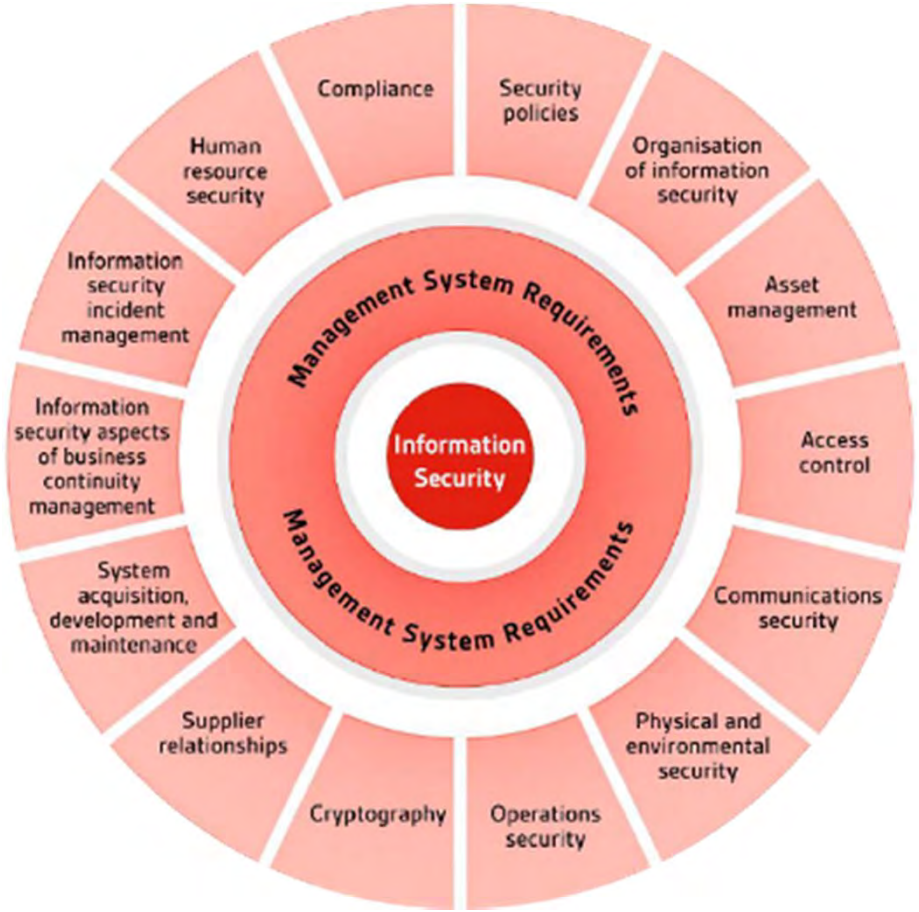
Became International Standards ISO/IEC 27001 and 27002 in 2005

Other information security standards now being developed or harmonized into 270xx series standards

ISO/IEC 27001 family of standards

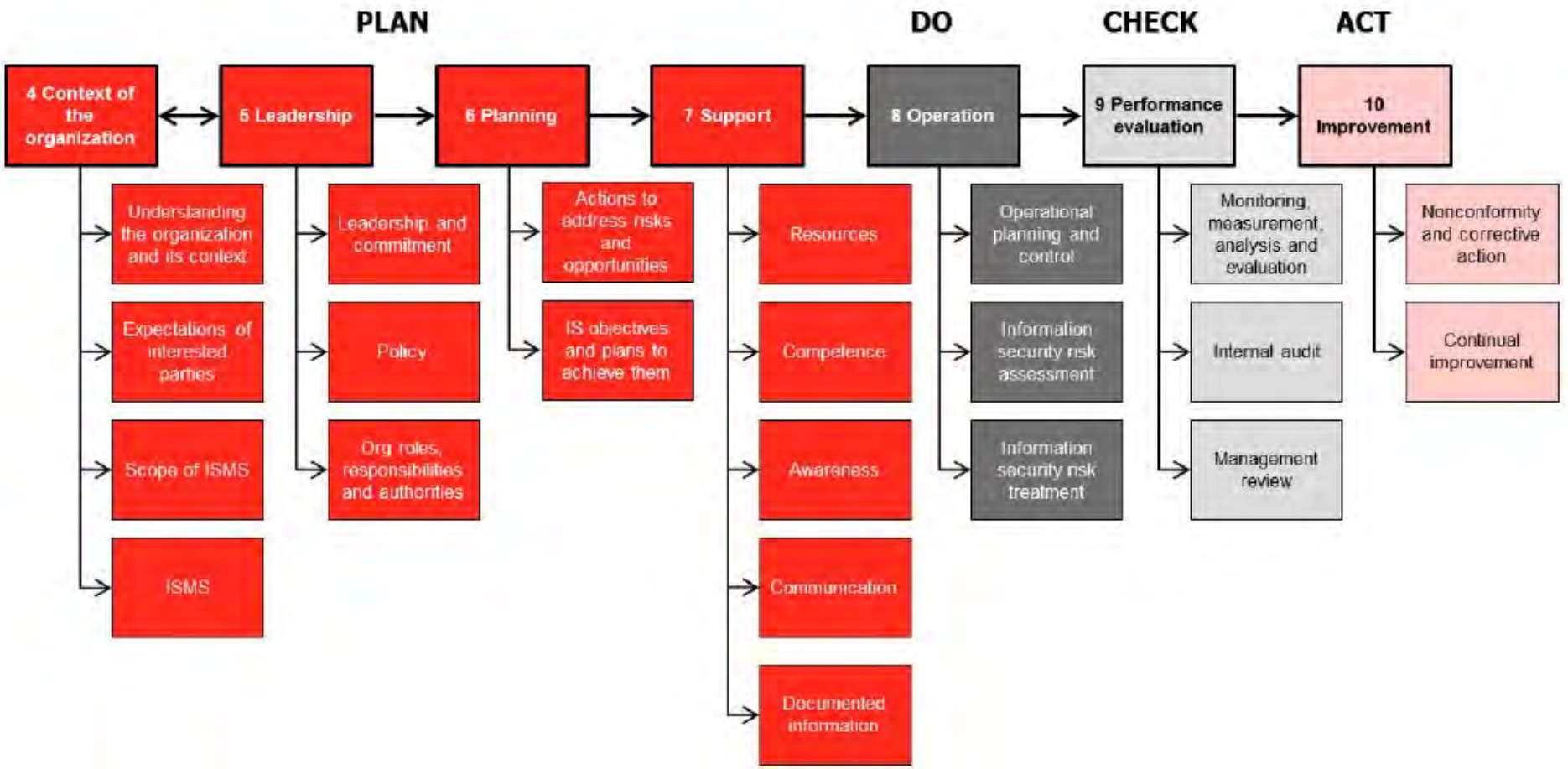


New, Cleaner Organization of Domains in ISO 27001:2013



ISO 27001:2005		ISO 27001:2013	
11	Number of sections in Annexure A	14	Number of sections in Annexure A
133	Number of controls in Annexure A	114	Number of controls in Annexure A

The New ISO/IEC 27001:2013 Structure



Cloud Control Matrix

Cloud Controls Matrix v3.0.1

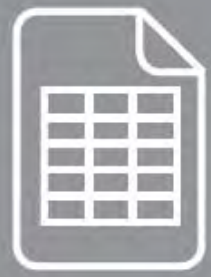
Info Sheet

CCMv3.0.1™

https://cloudsecurityalliance.org/research/ccm/

Welcome to Latest Version of the Cloud Controls Matrix, CCM v3.0.1!

ABOUT THE CSA CLOUD CONTROLS MATRIX



- Provides fundamental security principles to guide cloud vendors and to assist cloud customers in assessing the overall security risk of a cloud provider
- Strengthens information security control environments by delineating control guidance by service provider and consumer, and by differentiating according to cloud model type and environment
- Provides a controls framework in 16 domains that are cross-walked to other industry-accepted security standards, regulations, and controls frameworks to reduce audit complexity
- Seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud

Cloud Control Matrix – Domains and Controls

Sample Control and Applicability

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

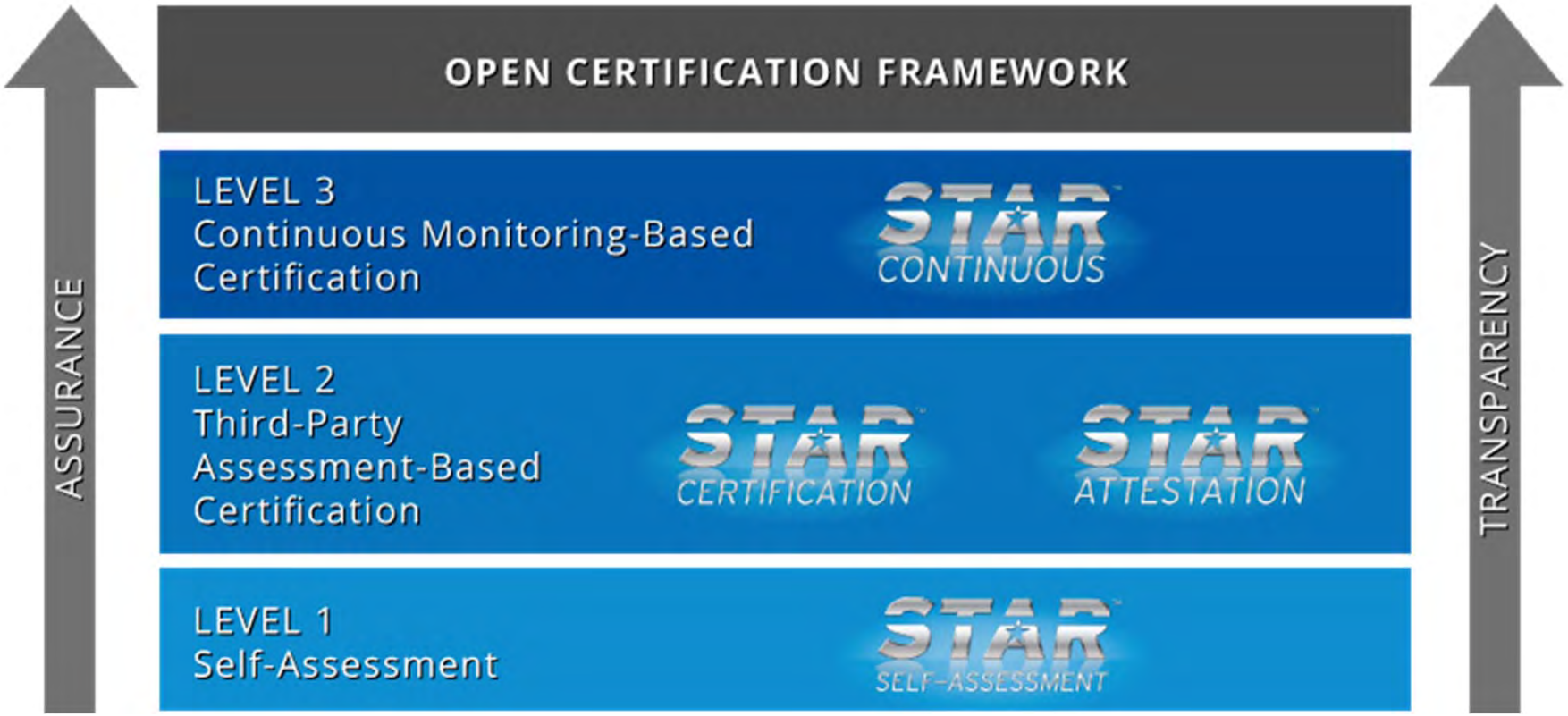
Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability		
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline			X				X	X	X	X
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing	X	X	X	X	X	X		X	X	X
Infrastructure & Virtualization Security Segmentation	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory	X	X	X	X	X	X		X	X	X

Cloud Control Matrix Mapping with Other Standards

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	FERPA	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	ISO/IEC 27001-2013
Infrastructure & Virtualization Security Network Security	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-20 (1) NIST SP 800-53 R3 SC-21 NIST SP 800-53 R3 SC-22 NIST SP 800-53 R3 SC-30		8.2.5		A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline						Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1

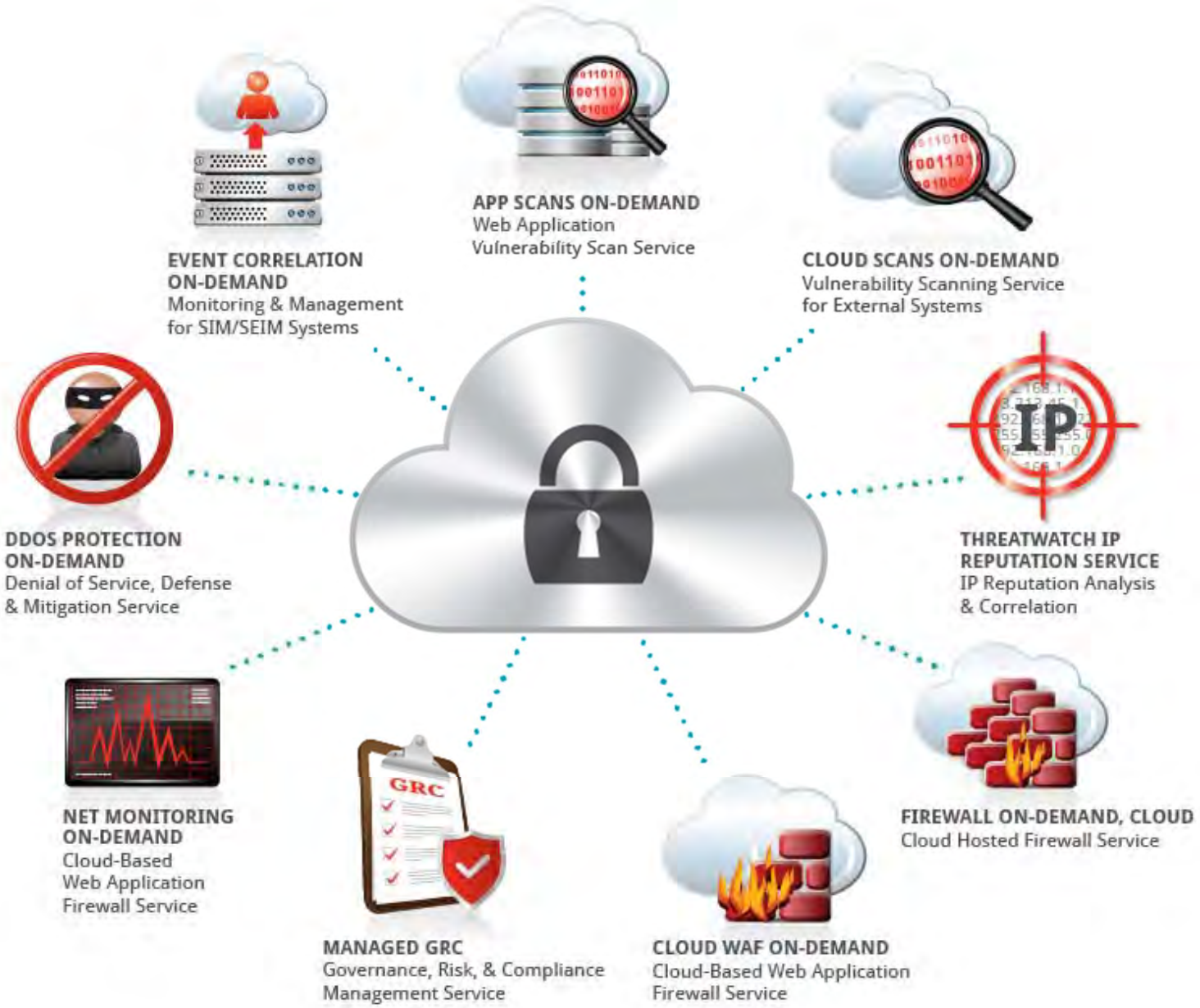
Cloud Security Alliance : The CSA STAR Certification



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

Suitable Security Policies / Controls are mandatory to enforce proper security with security devices and applications

Cloud Security Solutions On Demand



QUESTIONS…?

Thank You Very Much