Cloud Supply Chain Risk Management & Assurance Standards

Becky Swain ***CISSP, CIPP/IT, CIPP/US, CISA***

Founding Member, CSA

Board Member, CSA Silicon Valley Chapter

Project Co-Editor, ISO/IEC 27036-1, CSA Liaison Officer to SC27

Security SIG Lead, Cloud Network of Women (CloudNOW)

About Us

- Global, not-for-profit, 501(c)6 organization
- Over 29,000 individual members, 120 corporate members, 60 chapters
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
- Balance compliance with risk management
- Reference models: build using existing standards
- Identity: a key foundation of a functioning cloud economy
- Champion interoperability
- Enable innovation
- Advocacy of prudent public policy

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

Tools CSA Provides Today

- Assessment
- User Certifications
- Best Practices
- Provider Assessments
- Procurement
- Standards Creations

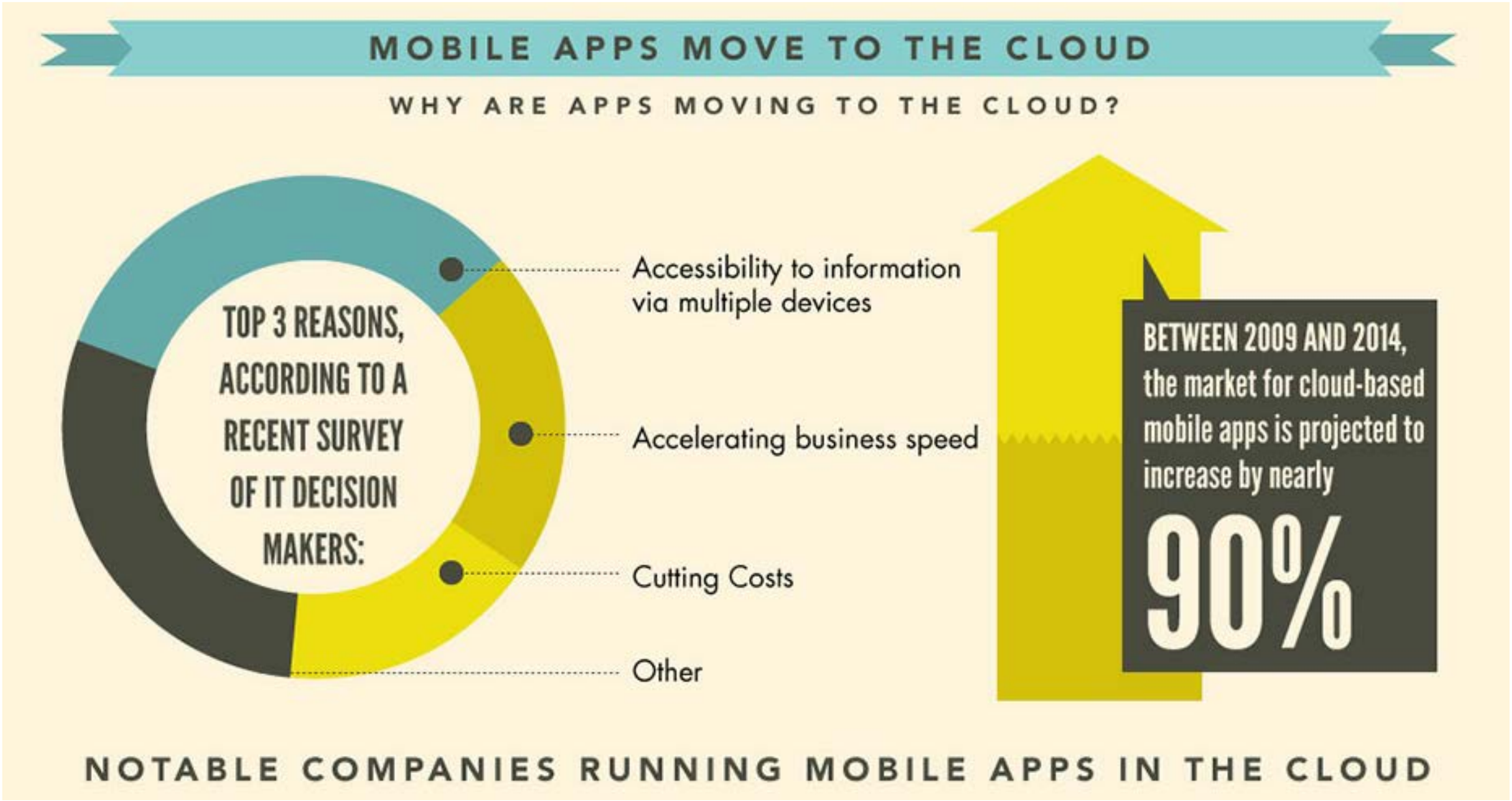
The Profound Paradigm Shift…

- The ***Empowerment*** of the Individual
  - **BYOD & Consumerism of IT**
  - **Productive & Social Collaboration**
  - **Outsource Non-Core**

Market Pressures to Enable Innovation…

- The ***Demands*** of the Business (BUs and SMBs)
  - **Improved Competition with Rapid Time to Market**
  - **Agility & Elasticity (IT as a Utility)**
  - **Big Data**

The Trifecta…Mega Mobility !!

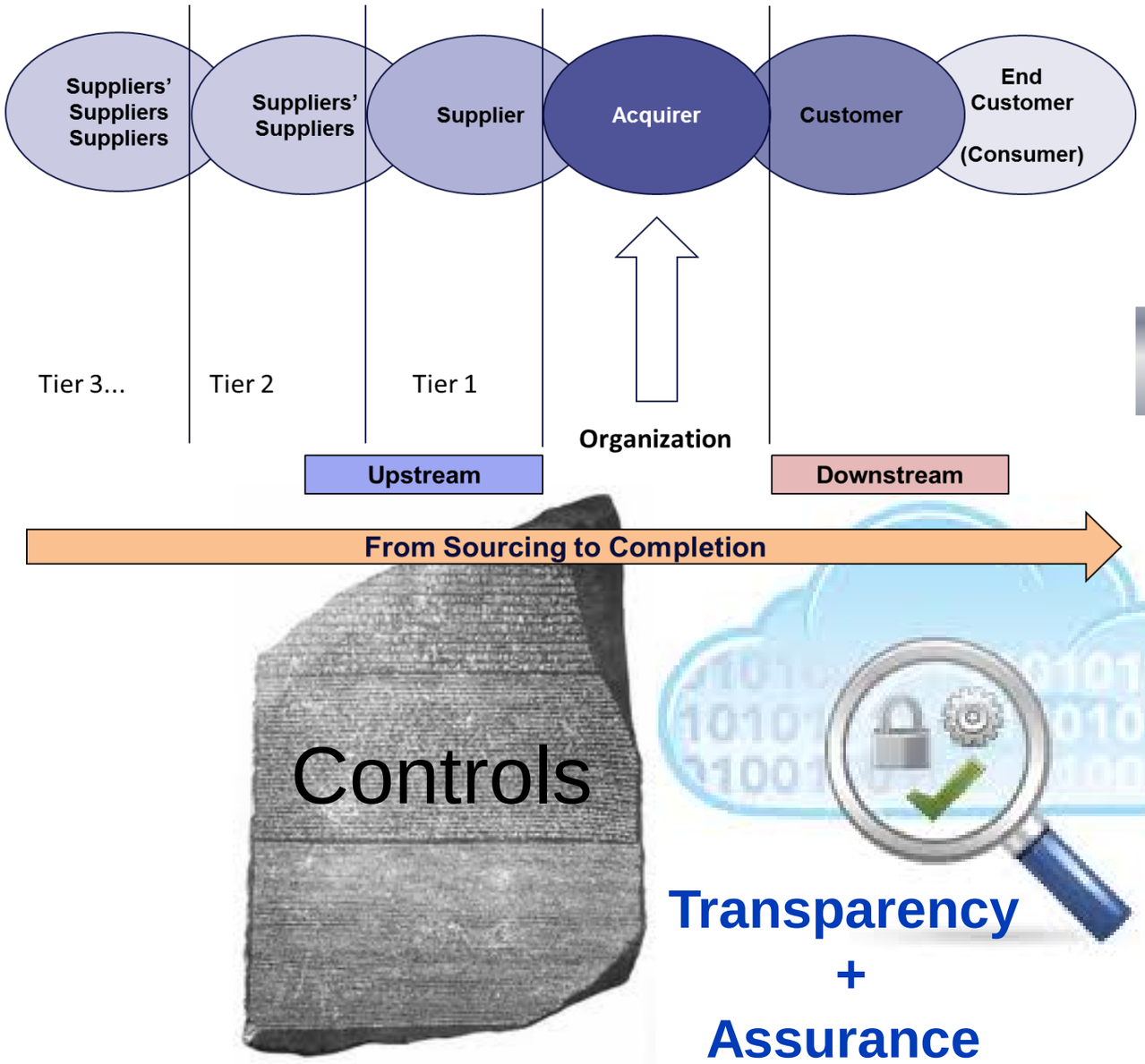


Source: http://www.engineyard.com/blog/2012/platform-as-a-service/

You Cannot Outsource Accountability…

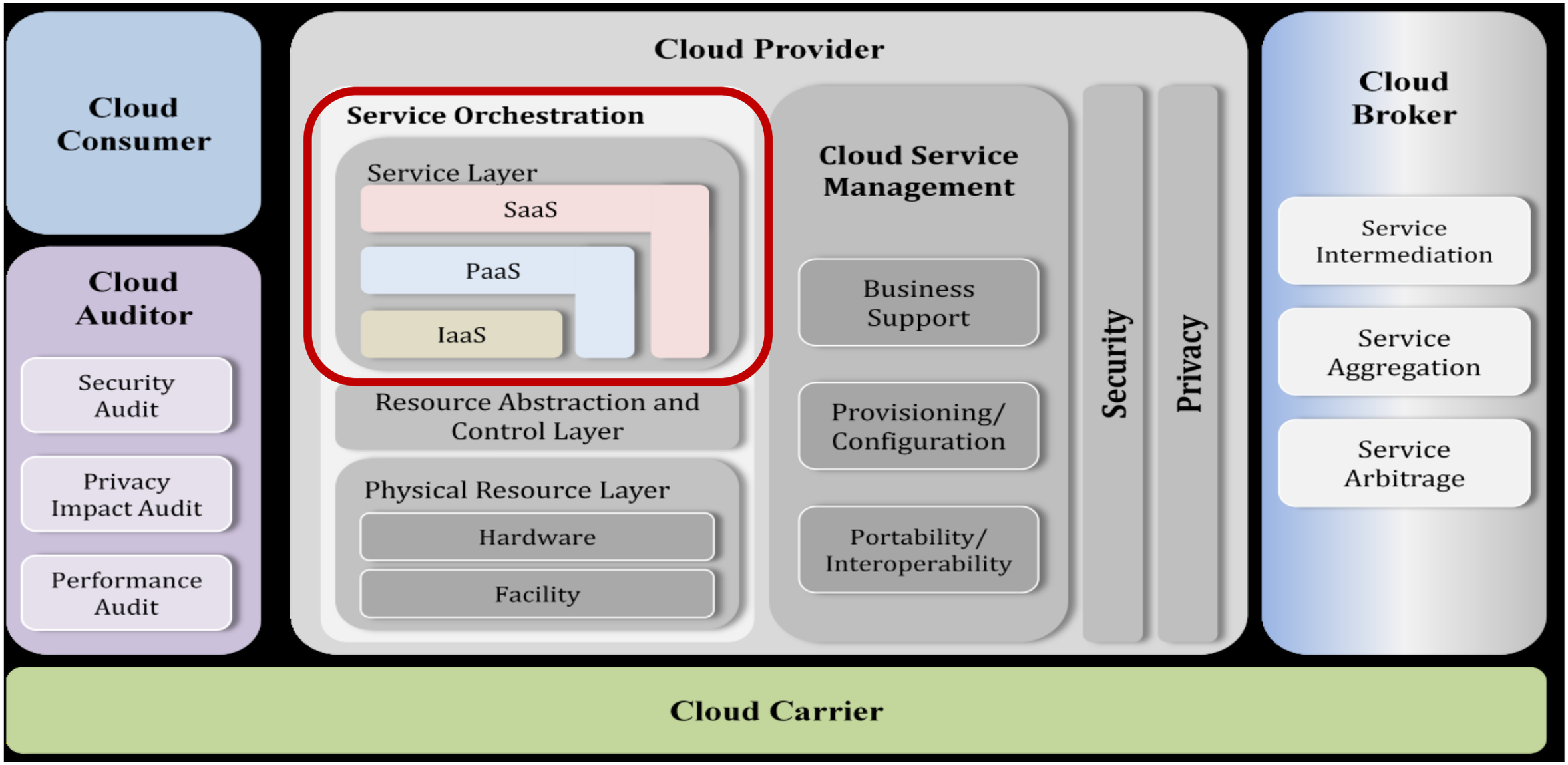
- With Cloud likely comes a ***Supply Chain***
  - Externalization of Sensitive Corporate (or Customer) Data
  - Network Deperimeterization
  - Unclear Control Ownership & Accountability
  - Regulatory Compliance

In *Clouds* We Trust…Or do we?



Who Controls ***What*** in the Cloud Ecosystem?

NIST Cloud Computing Reference Architecture (SP 500-292)



Who Controls ***What*** in the Cloud Ecosystem?

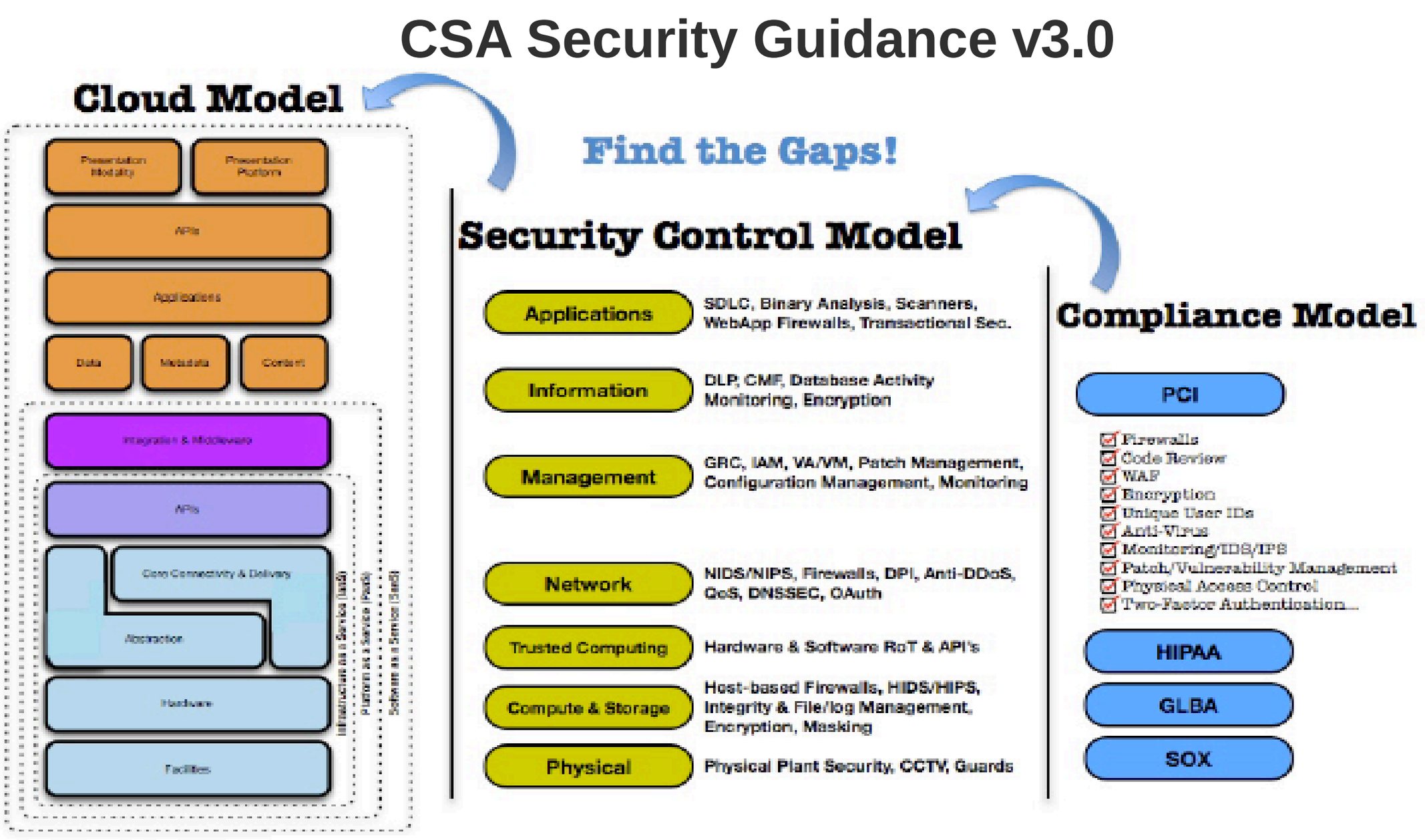


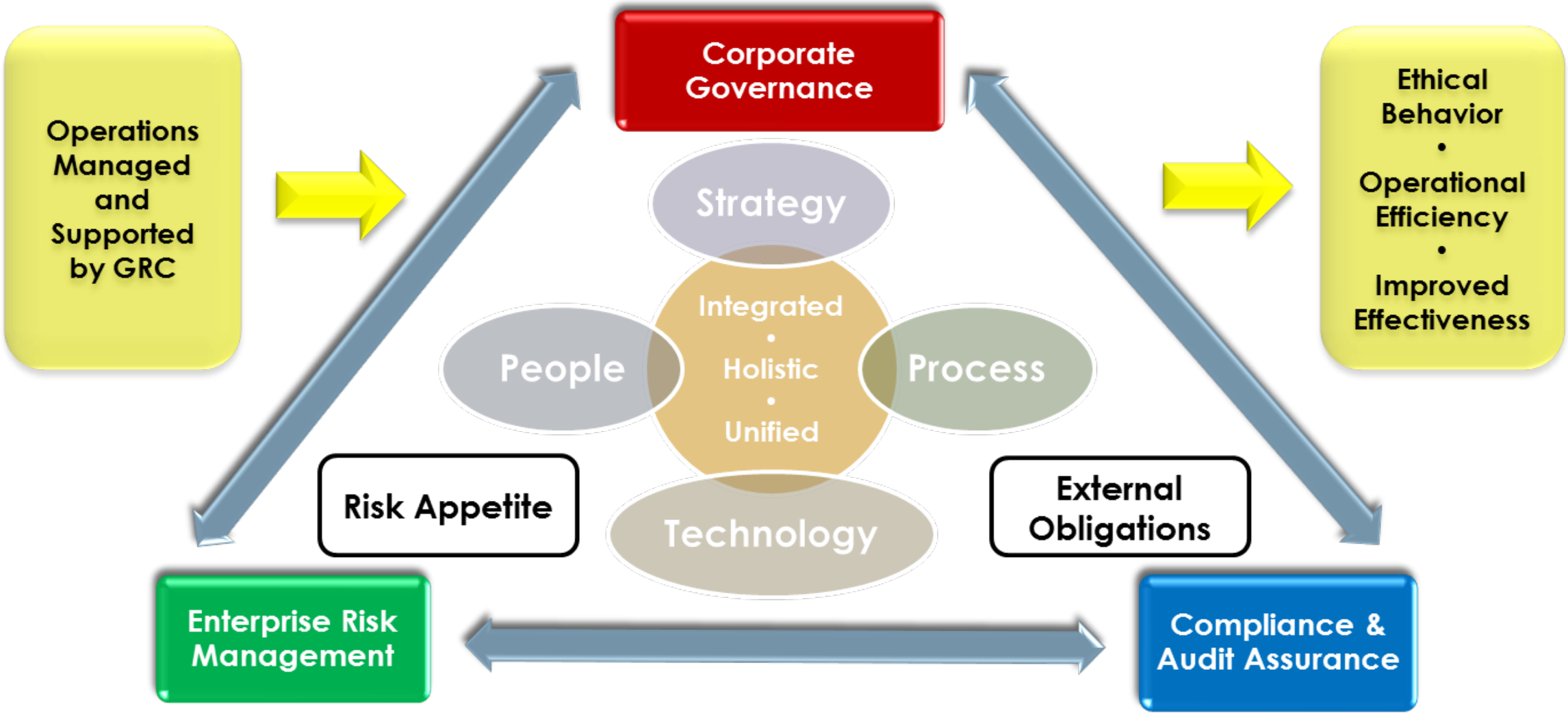
Figure 5—Mapping the Cloud Model to the Security Control & Compliance

Silver Lining → O_O for Standards

CSA GRC Stack

- A suite of four integrated and reinforcing CSA initiatives (the “stack packages”)
  - The Stack Packs
    - Cloud Controls Matrix (CCM)
    - Consensus Assessments Initiative (CAI)
    - CloudAudit
    - Cloud Trust Protocol (CTP)
- Designed to support cloud consumers and cloud providers
- Prepared to capture value from the cloud as well as support compliance and control within the cloud

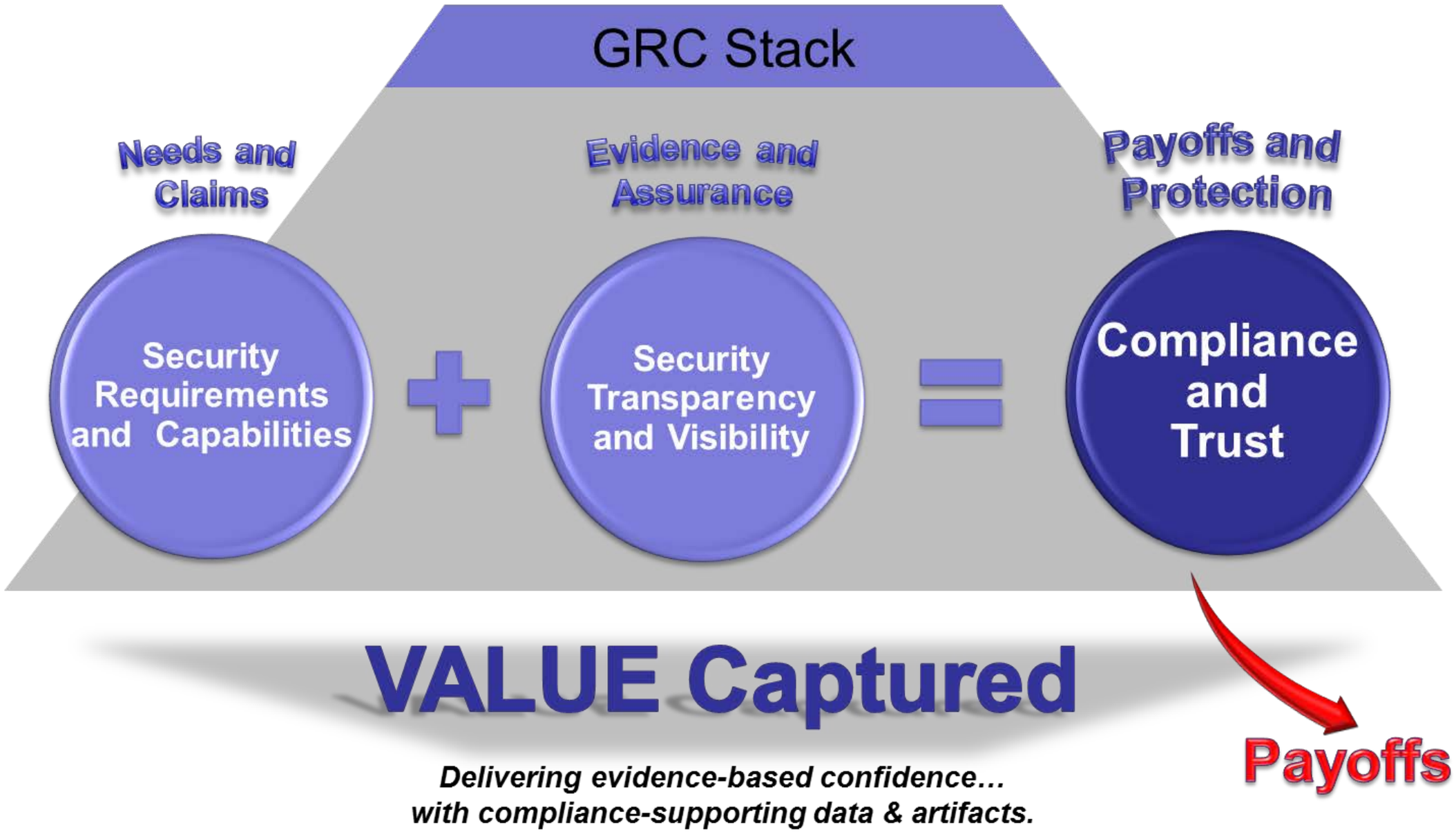
What is GRC?



CSA GRC Stack (cont.)

Delivering	← Stack Pack →	Description
Continuous monitoring … with a purpose	CTP™	• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers
Claims, offers, and the basis for auditing service delivery	Cloud Audit™	• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
Pre-audit checklists and questionnaires to inventory controls	CAI™	• Industry-accepted ways to document what security controls exist
The recommended foundations for controls	CCM™	• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider

CSA GRC Stack (cont.)



CSA CCM → Control Ownership Clarity

SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Controls represent the common language of information security and regulatory compliance between supplier and customer.

CSA GRC Stack (cont.)

What control requirements should I have as a cloud consumer or cloud provider?

CCM Cloud Controls Matrix

How do I ask about the control requirements that are satisfied (consumer) or express my claim of control response (provider)?

CAI Consensus Assessments Initiative

Static claims & assurances

How do I announce and automate my claims of audit support for all of the various compliance mandates and control obligations?

Cloud Audit

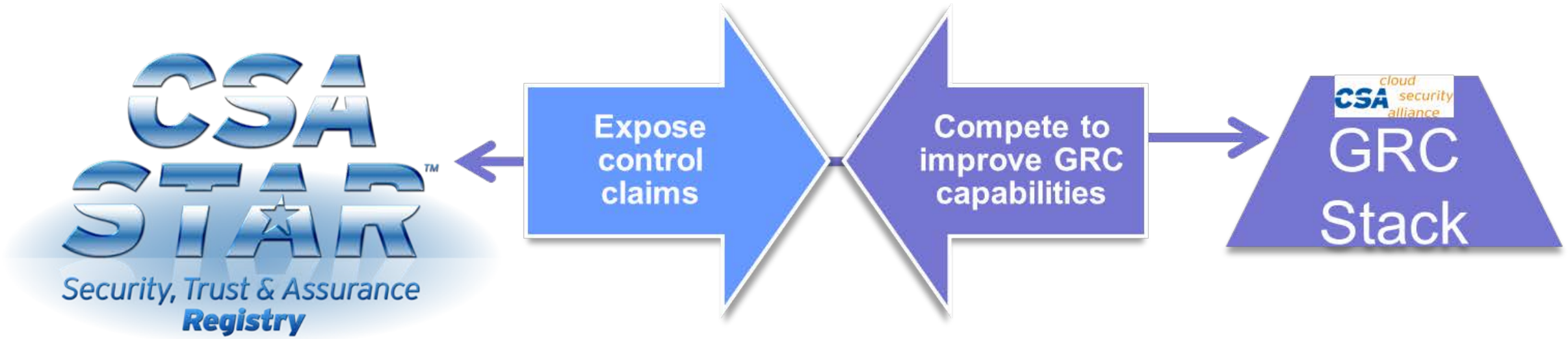
Dynamic (continuous) monitoring and transparency

How do I know that the controls I need are working for me now (consumer)? How do I provide actual security and transparency of service to all of my cloud users (provider)?

CTP Cloud Trust Protocol

- Individually useful
- Collectively powerful
- Productive way to reclaim end-to-end information risk management capability

CSA STAR
(Security Trust & Assurance Registry)



- Encourage transparency of security practices within cloud providers
- Documents the security controls provided by various cloud computing offerings
- Free and open to all cloud providers
- Option to use data/report based on CCM or the CAIQ

CCM™ Cloud Controls Matrix

CAI™ Consensus Assessments Initiative

NIST

- ***National Institute of Standards and Technology (NIST)*** – Promotes the effective and secure use of the technology within the U.S. Federal Government, and, therefore, leading a number of efforts to develop cloud standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.
  - Standards Acceleration to Jumpstart the adoption of Cloud Computing (SAJACC)
  - Strategy to build a US Government (USG) Cloud Computing Technology Roadmap.

NIST

- Publications
  - **SP 800-144** Guidelines on Security and Privacy in Public Cloud Computing
  - **SP 800-145** A NIST Definition of Cloud Computing
  - **SP 800-146** Cloud Computing Synopsis and Recommendations
  - **SP 800-53 Rev 4** DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Initial Public Draft)
  - **SP 800-37 Rev 1** Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - **NIST IR 7622** Notional Supply Chain Risk Management Practices for Federal Information Systems

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Definition of Cloud

The NIST definition of cloud computing (SP 800-145)

- 5 essential characteristics
- 3 service models
- 4 deployment models

Already widely adopted by Cloud Computing industry, including ISO/IEC JTC 1/SC38 and **recognized in CSA Guidance**.

FedRAMP

- The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
  - Chapter 1 – Security Requirements (SP 800-53 R3 ++)
  - Chapter 2 – Continuous Monitoring
  - Chapter 3 – Assessment & Authorization (SP 800-37 R1)

FedRAMP℠

ISO/IEC JTC 1

- ***ISO/IEC JTC 1 is Joint Technical Committee 1*** of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) with a mandate to develop, maintain, promote and facilitate IT standards required by global markets meeting business and user requirements concerning:
  - the design and development of IT systems and tools
  - the performance and quality of IT products and systems
  - the security of IT systems and information
  - the portability of application programs
  - the interoperability of IT products and systems
  - the unified tools and environments
  - the harmonized IT vocabulary, and
  - the user-friendly and ergonomically-designed user interfaces
- Work is conducted by subcommittees (SC) dealing with a particular field and SCs may be comprised of several working groups (WGs).

ISO/IEC JTC 1 Development Phases

- International Standards are developed by ISO technical committees (TC) and subcommittees (SC) by a six-step process

Stage	Title	Timeframe	Process	Deliverables
1	Proposal	3 months	New Work Item Proposal (NP or NWIP)	
2	Preparatory	6 months	New project registered in TC/SC work program; Working draft (WD) study initiated; Building Expert Consensus	Working Draft (WD) – First Committee Draft (CD) or ISO/PAS (Publicity Available Publication)
3	Committee	12 months	Committee draft (CD) registered; CD study/ballot initiated; Consensus Building within TC/SC from Committee Draft (CD)	Draft International Standard (DIS) or ISO/TS (Technical Specification); ISO/TR (Technical Report) for non-normative documents
4	Enquiry	Up to 24 months; 5 months once ballot is initiated	DIS registered; DIS ballot initiated; Enquiry on DIS (Draft International Standard); 2/3 P-member approval vote across all ISO member bodies	Final text for processing as FDIS (Final Draft International Standard)
5	Approval	Up to 33 months; 2 months once ballot is initiated	FDIS registered for formal approval; FDIS ballot initiated; Formal Vote on FDIS (proof check by secretariat); 1 vote per country; 75% to approve	Final text of International Standard
6	Publication	Up to 36 months	Publication of International Standard	ISO International Standard

ISO/IEC JTC 1/SC 27

- ***International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Joint Technical Committee 1/Subcommittee 27 (ISO/IEC JTC1/SC 27)*** – Information Technology Security Techniques (2700x series of ISMS standards)
  - Study period on Cloud Computing Security and Privacy to investigate the requirements for cloud computing and a feasible program of standards work to meet requirements, involving 3 WGs:
    - WG 1 (Information Security Management) leading the coordinating efforts on this study period in conjunction with the following working groups:
    - WG 4 – Security Control and Services
    - WG 5 – Identity Management, Privacy Technology and Biometrics
  - Topics for consideration – information security management, risk management, application and network security, cybersecurity, business continuity, privacy and identity management.

CSA's International Standardization Council

ISO International Organization for Standardization IEC

WG 1 – **27017** (Cloud Controls)
WG 4 – **27036-5** (Cloud Supply Chain Risk)
WG 5 – **27018** (Public Cloud Privacy)

+ 2 Study Periods

CSA Security Guidance for Critical Areas of Cloud Computing Version 3.0

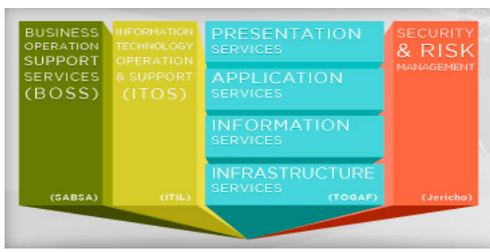
GRC™ GRC Stack

CTP™ Promoting Elements of Transparency in the Cloud

Cloud Audit™ Automated Audit, Assertion, Assessment, and Assurance

CAI™ Research Tools and Processes to Assess Cloud Providers

CCM™ Security Controls Framework For Cloud Providers & Consumers
Cloud Controls Matrix



reference ARCHITECTURE

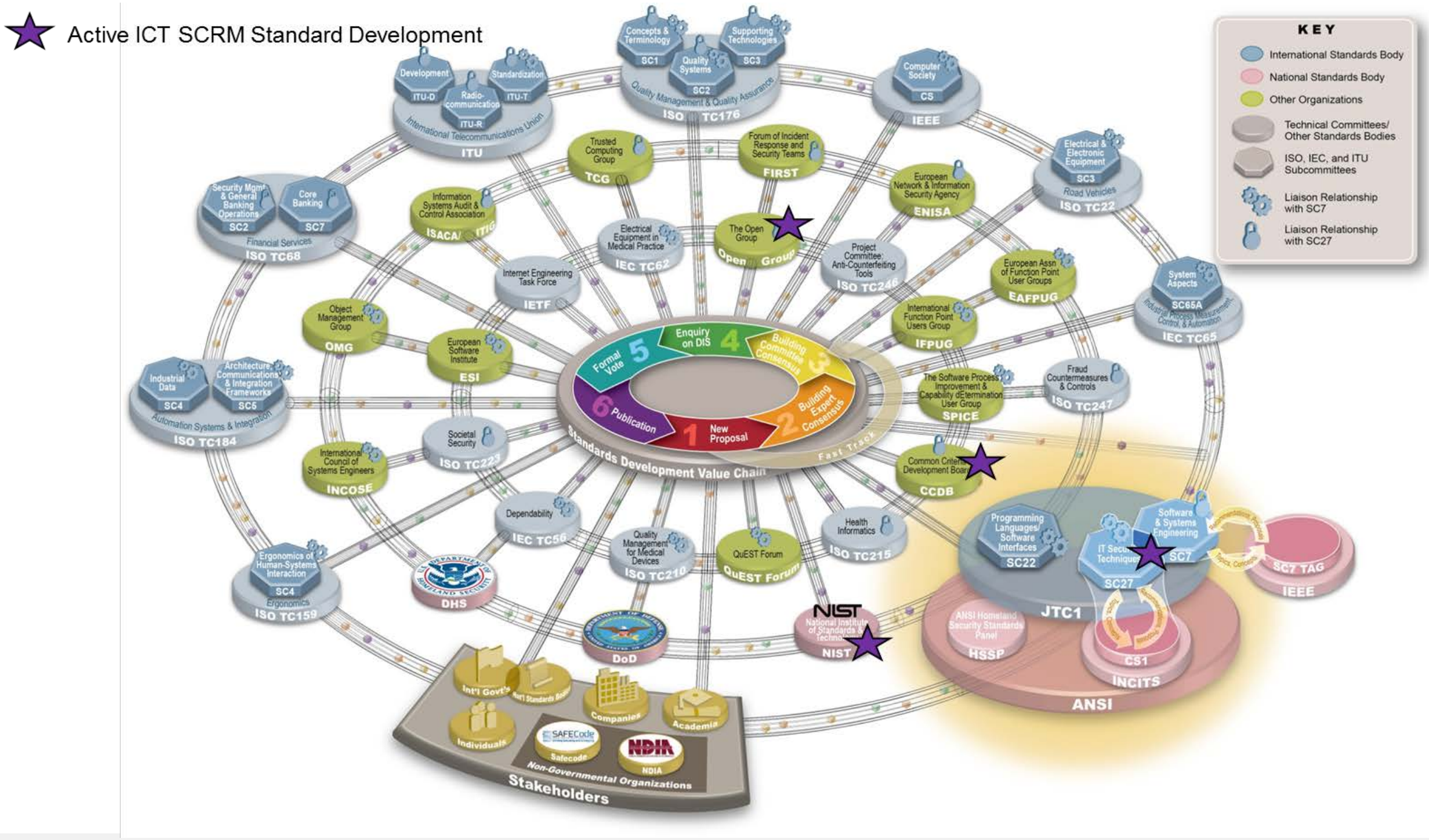
TCI TRUSTED CLOUD INITIATIVE

Promoting Education, Research and Certification of Secure and Interoperable Identity in the Cloud

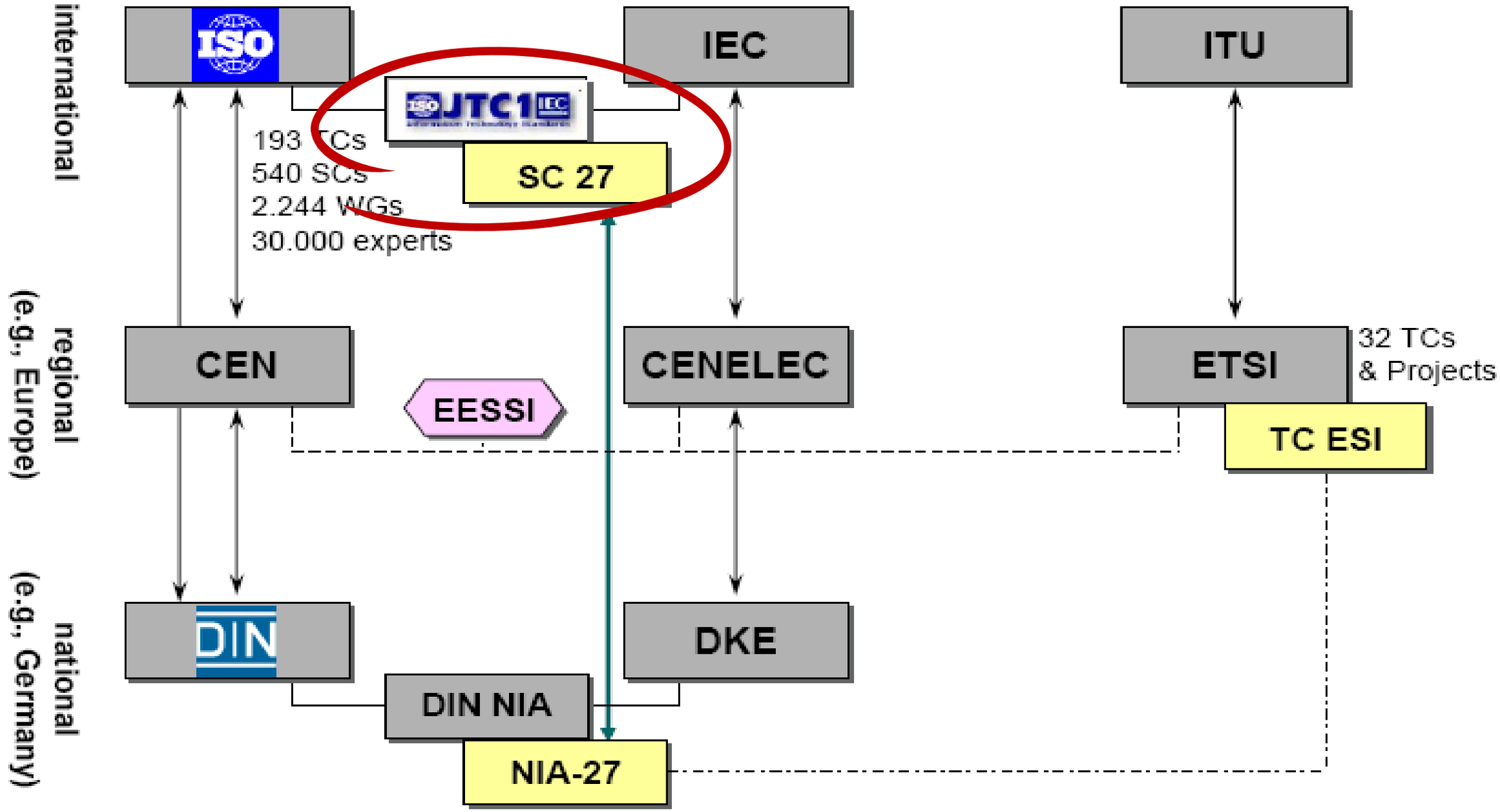
International Standardization Council

CSA cloud security alliance℠

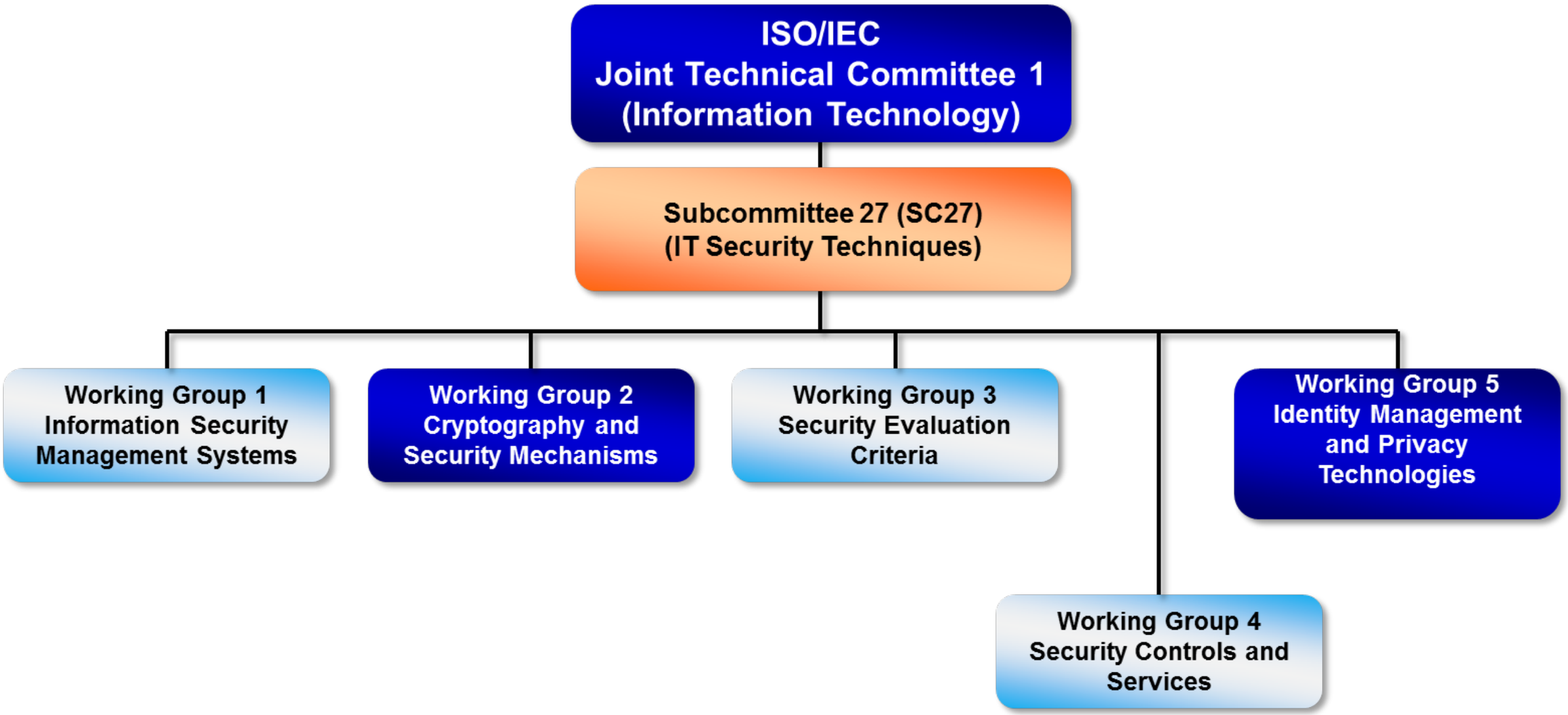
ICT SCRM SDO Landscape



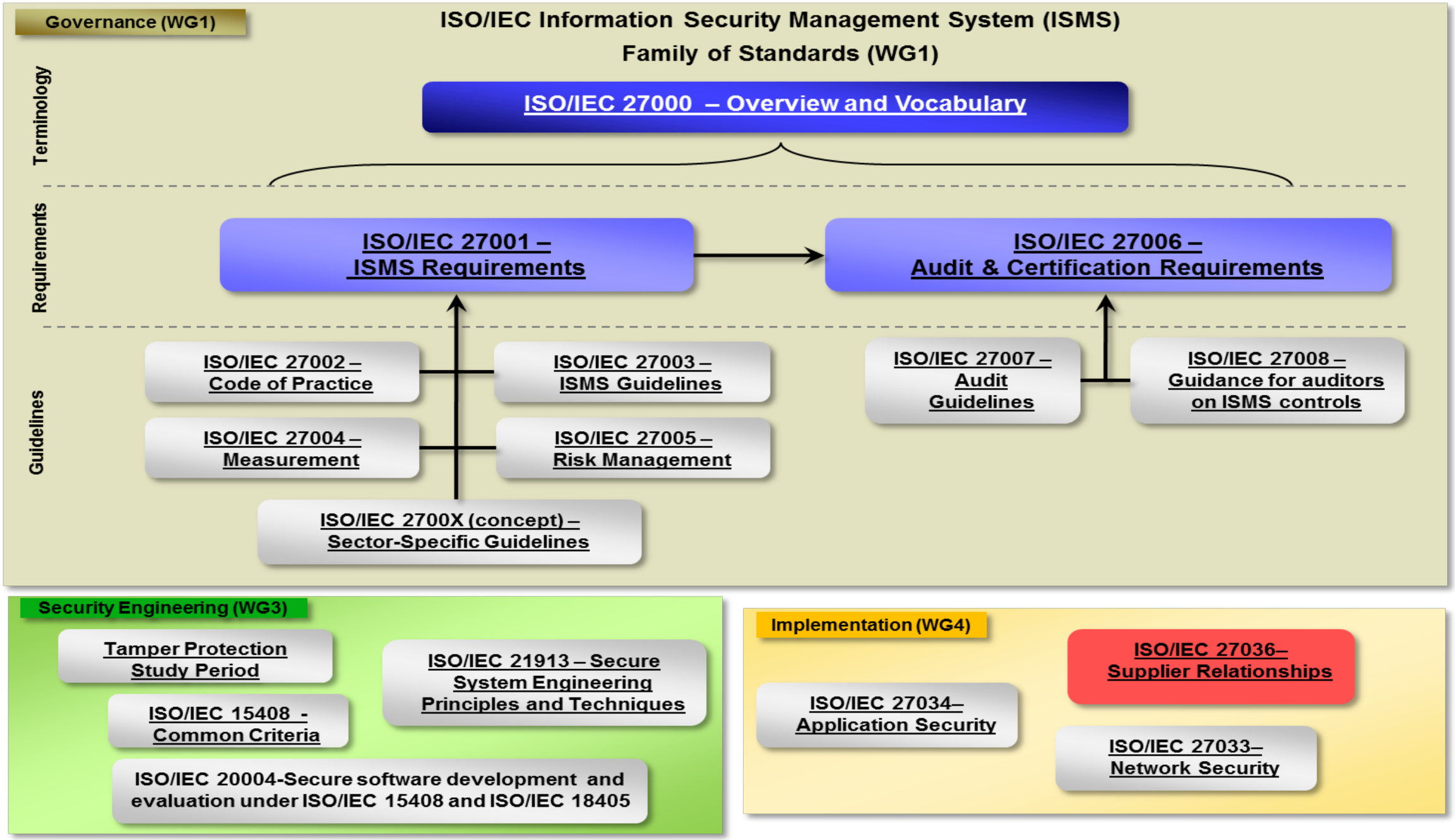
SDO Collaboration



ISO/IEC / JTC1 / SC27



ISO/IEC / JTC1 / SC27 (cont.)



ISO/IEC 27036: Information technology – Security techniques – Information Security for Supplier Relationships

- Information security in relationships between acquirers and suppliers
- All types of organizations e.g., commercial, public sector, non-profit
- All types of supplier relationships, including outsourcing, product and service acquisition, ICT, and cloud computing, that may have security implications

Includes definitions used in all Parts

Part 1 – Overview and Concepts
Includes Definitions for terms used in all parts

Part 2 – Common requirements

Each document includes definitions that are used in that specific document

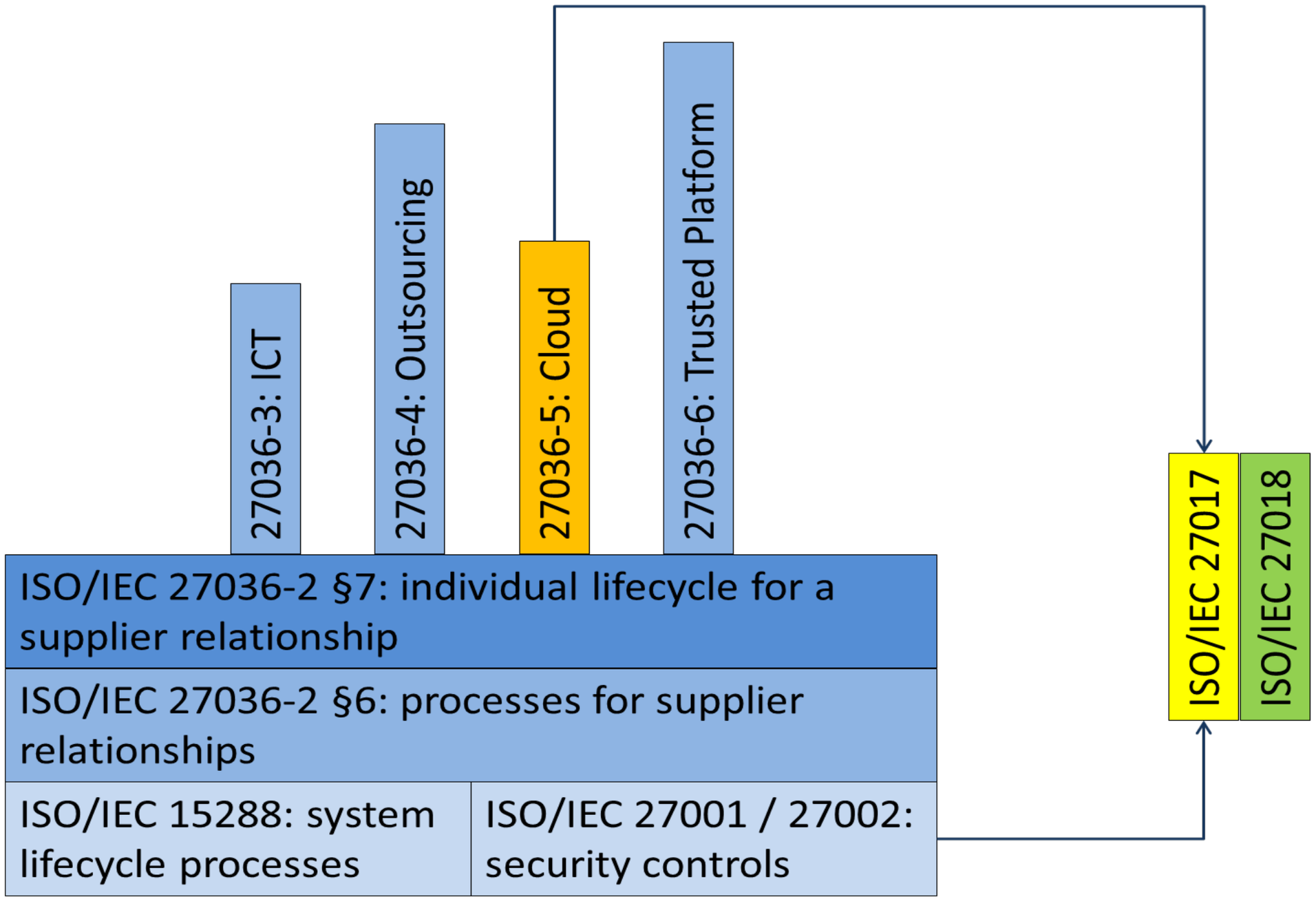
Part 3 – ICT Supply Chain

Part 4 – Outsourcing

Part 5 – Cloud Computing

Part 6 – Placeholder for OTTF

ISO/IEC 27036 & Cloud Context



AICPA

- **The American Institute of Certified Public Accountants**
  - Founded in 1887 and world's largest association representing the accounting profession, with nearly 377,000 members in 128 countries.
  - Members represent many areas of practice, including business and industry, public practice, government, education and consulting; membership is also available to accounting students and CPA candidates.
  - Sets ethical standards for the profession and U.S. auditing standards for audits of private companies, non-profit organizations and federal, state and local governments
  - Develops and grades the Uniform CPA Examination

SOC (Formerly SAS 70)

- With the retirement of the SAS 70 standard, traditional SAS 70 reports are being replaced by Service Organization Control Reports (or “SOC” reports.)
- SAS 70 report was intended to assist service organizations’ customers and their auditors in the context of a financial statement audit.
- 3 SOC Reports (Types 1 and 2)
  - **SOC 1** Report on Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting
  - **SOC 2** Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
  - **SOC 3** Trust Services Report for Service Organizations

SOC Report Comparison

Figure 1—SOC Reports Comparison

REPORT	GUIDANCE	SUBJECT MATTER (SERVICE ORGANIZATIONS)	USERS
SOC 1	SSAE 16, *Reporting on Controls at a Service Organization* *AICPA Guide: Service Organizations—Applying SSEA No. 16, Reporting on Controls at a Service Organization (SOC 1)*	Controls relevant to user entities' internal controls over financial reporting	User entities' auditors; user entities' management; service organizations' management
SOC 2	AT 101, *Attestation Engagements* *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2)*	Controls relevant to security, availability, processing integrity, confidentiality or privacy (if privacy, also compliance with the service organization's statement of privacy practices)	User entities' management and parties understanding: 1) The nature of the service provided 2) The interaction of systems among the service organization, user entities, subservice organizations and other parties 3) Internal control and its limitations 4) The applicable trust service criteria and risks/controls that address such criteria
SOC 3	AT 101, *Attestation Engagements* AICPA Technical Practice Aid, *Trust Services Principles, Criteria, and Illustrations*	Controls relevant to security, availability, processing integrity, confidentiality or privacy (if privacy, also compliance with the service organization's statement of privacy practices)	Anyone

Source: ISACA Journal 2012, Volume 3, Article: "SOC Progress Report"

Trust Services Principles & Criteria (TSP)

- **Principles & Related Criteria:**
  - ***Security*** – The system is protected against unauthorized access (both physical and logical).
  - ***Availability*** – The system is available for operation and use as committed or agreed.
  - ***Processing Integrity*** – System processing is complete, accurate, timely, and authorized.
  - ***Confidentiality*** – Information designated as confidential is protected as committed or agreed.
  - ***Privacy*** – Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and CICA.

- **Organized by:**
  - ***Policies*** – The entity has defined and documented its policies relevant to the particular principle.
  - ***Communications*** – The entity has communicated its defined policies to responsible parties and authorized users of the system.
  - ***Procedures*** – The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.
  - ***Monitoring*** – The entity monitors the system and takes action to maintain compliance with its defined policies.

Contact

Help Us Secure Cloud Computing

- *www.cloudsecurityalliance.org*
- *info@cloudsecurityalliance.org*
- *LinkedIn: www.linkedin.com/groups?gid=1864210*
- *Twitter: @cloudsa*

Thank You

cloud security alliance℠