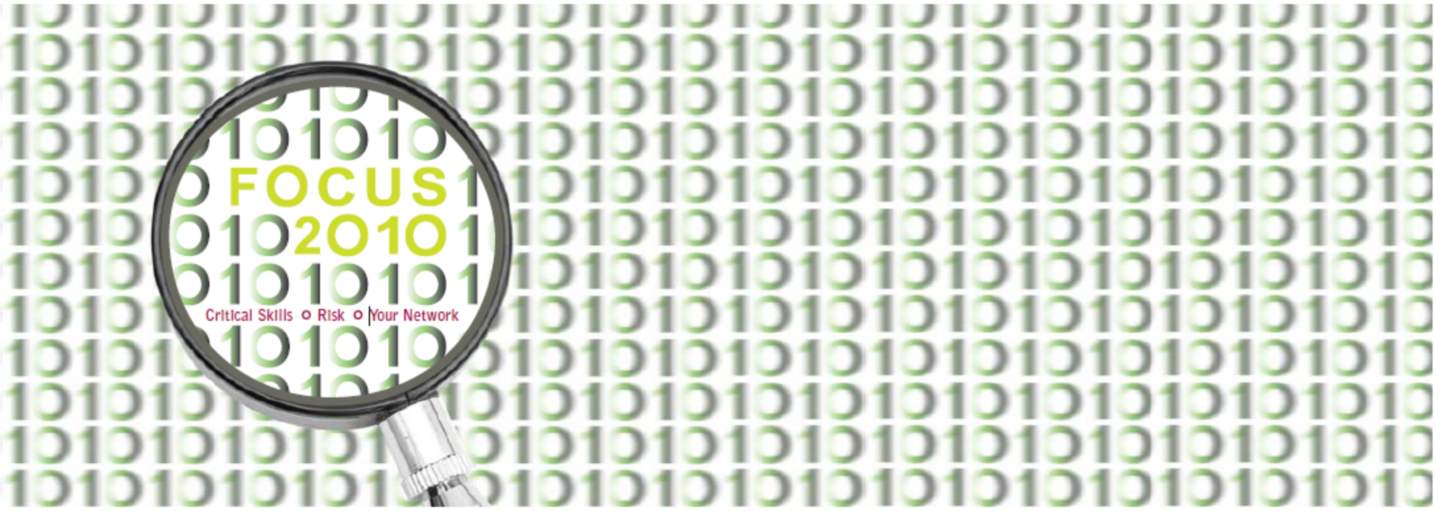
10th Annual SF ISACA Fall Conference

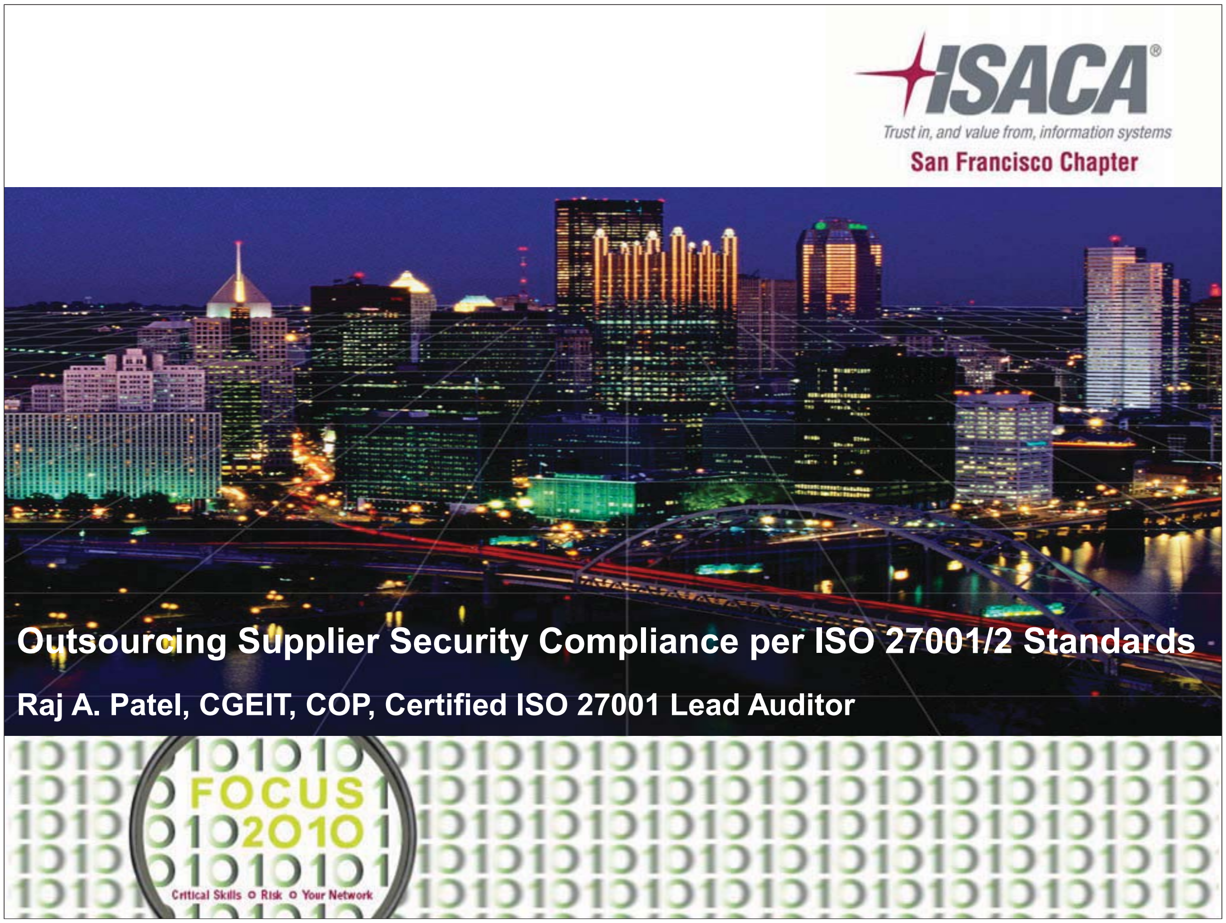
October 4 – 6, 2010



G33: "Enterprise Information Security Compliance" and "Outsourcing Security Compliance" per ISO 27001/2 Standards

Raj Patel, Oracle Corporation

ISACA®
Trust in, and value from, information systems
San Francisco Chapter



ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Outsourcing Supplier Security Compliance per ISO 27001/2 Standards

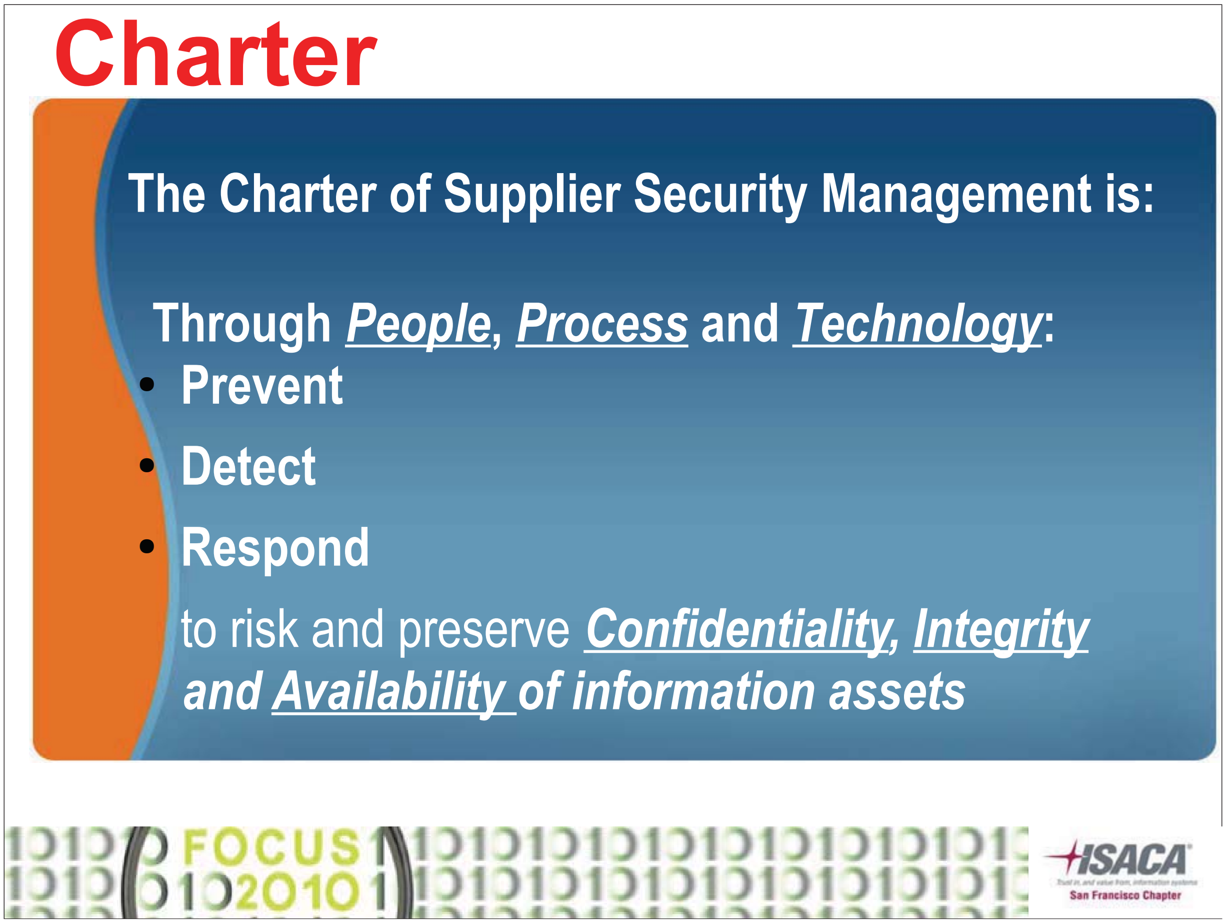
Raj A. Patel, CGEIT, COP, Certified ISO 27001 Lead Auditor

FOCUS
2010
Critical Skills ○ Risk ○ Your Network

Table of Contents

- **Section I:** **Enterprise Information Security Compliance**
- **Section II:** **Outsourcing Supplier Security Compliance**
- ***Section III:*** ***ISO 27001 Audit and Compliance***
- ***Section IV:*** ***Appendices***

FOCUS
ISACA
San Francisco Chapter



Charter

The Charter of Supplier Security Management is:

Through ***People***, ***Process*** and ***Technology***:

- Prevent
- Detect
- Respond

to risk and preserve ***Confidentiality***, ***Integrity*** ***and Availability of information assets***

Section I:

Enterprise Security Compliance

Outline

- What is Security Compliance
- Why Do we Care?
- How Should we Comply?
- Compliance Road-map

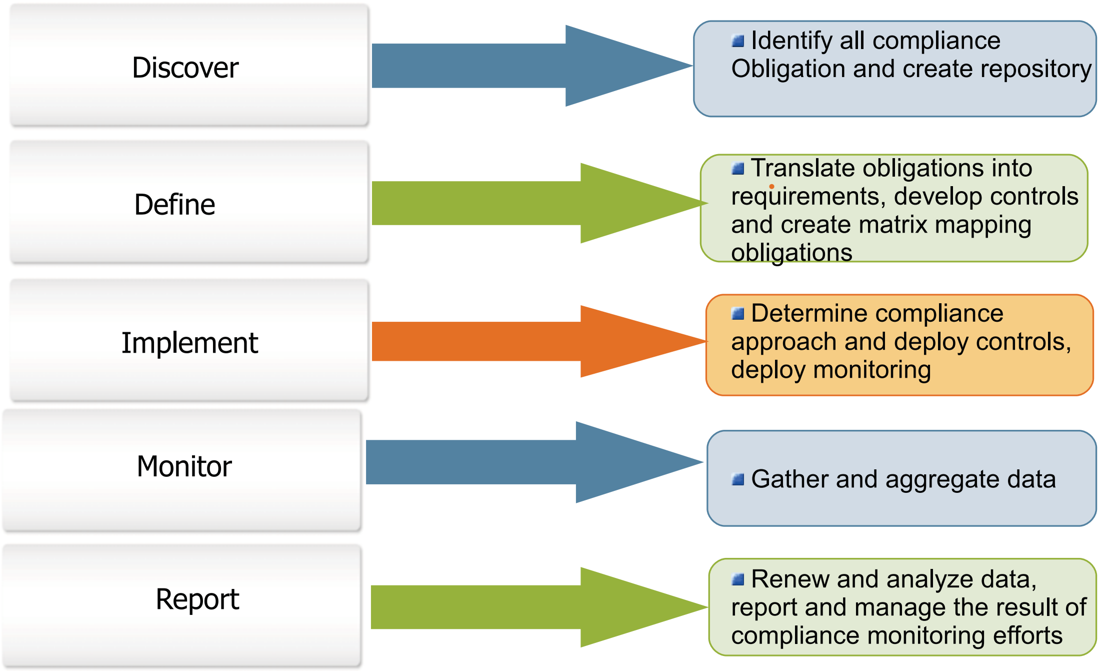
InfoSec Compliance

- Information Security Compliance is defined as conformance with obligation that govern the need to ensure the confidentiality Integrity and Availability of an organization's information assets
  - Source: IREC

Importance of Compliance

- Financial penalties
  - Governmental
  - Private
- Legal liabilities
- Reputation risks with shareholders, customers and business partners
- Inability to do business with customers
- Inability to do business with business partners
- Executives say “Keep us out of jail”

Compliance Process



Discover

Identify all compliance Obligation and create repository

Define

Translate obligations into requirements, develop controls and create matrix mapping obligations

Implement

Determine compliance approach and deploy controls, deploy monitoring

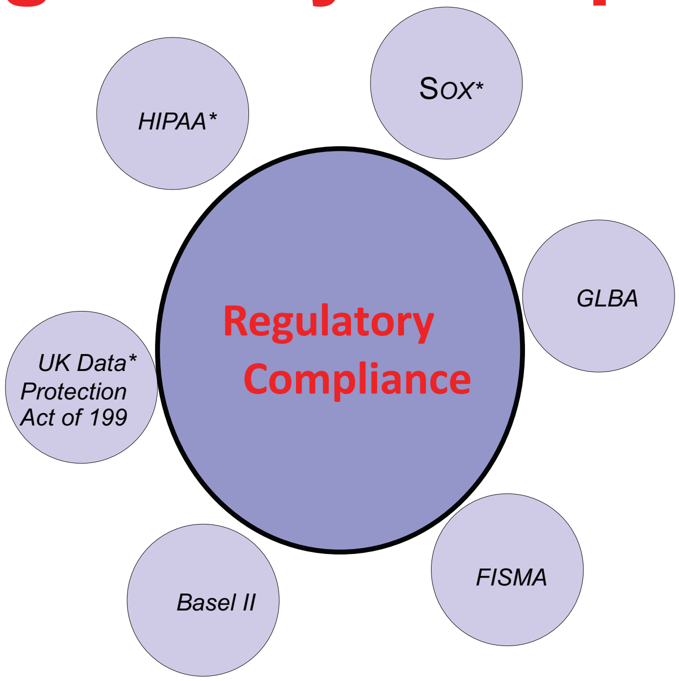
Monitor

Gather and aggregate data

Report

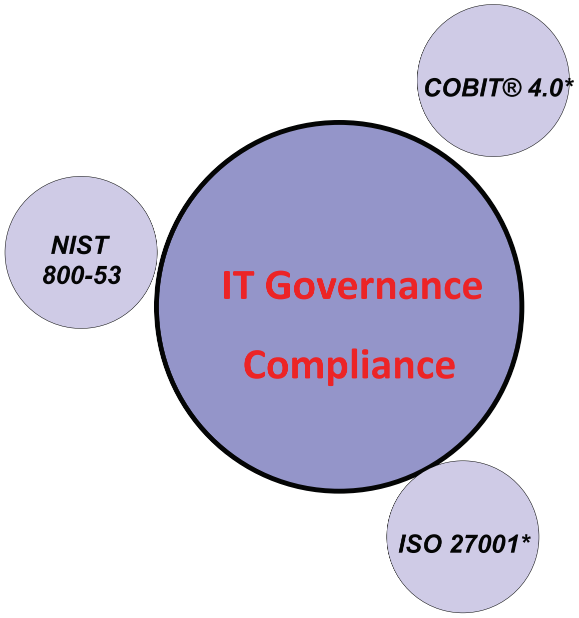
Renew and analyze data, report and manage the result of compliance monitoring efforts

Regulatory Compliance



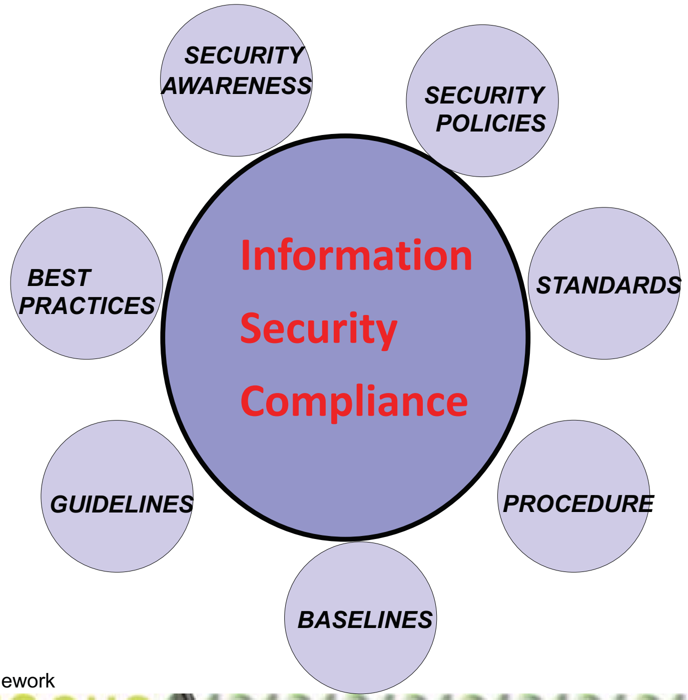
- Source: ISF & Qualys

IT Governance Compliance



- Source: ISF & Qualys

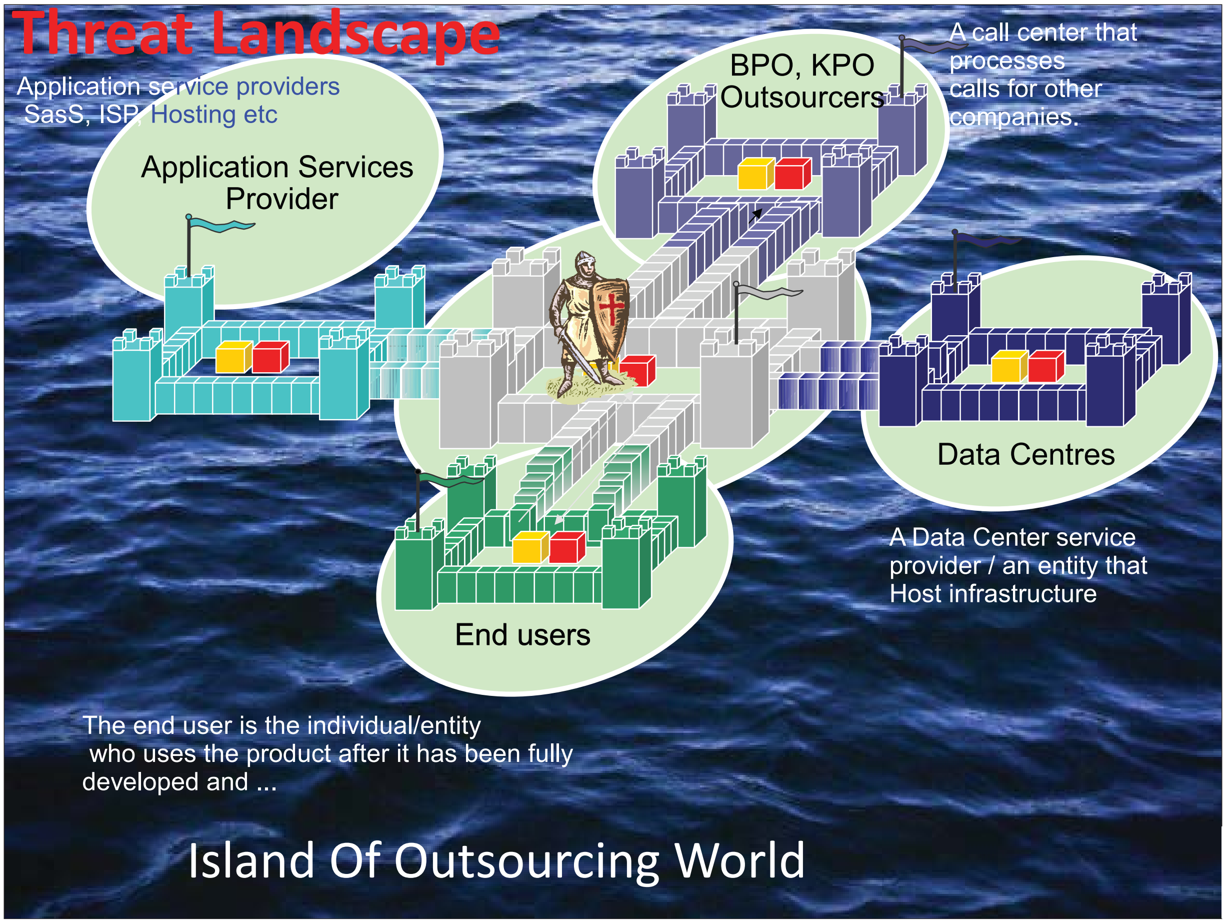
Information Security Compliance



– ISO 27001 Framework

Section II:

Outsourcing Supplier Security Compliance



Threat Landscape

Application service providers
SasS, ISP, Hosting etc

Application Services Provider

BPO, KPO Outsourcers

A call center that processes calls for other companies.

Data Centres

A Data Center service provider / an entity that Host infrastructure

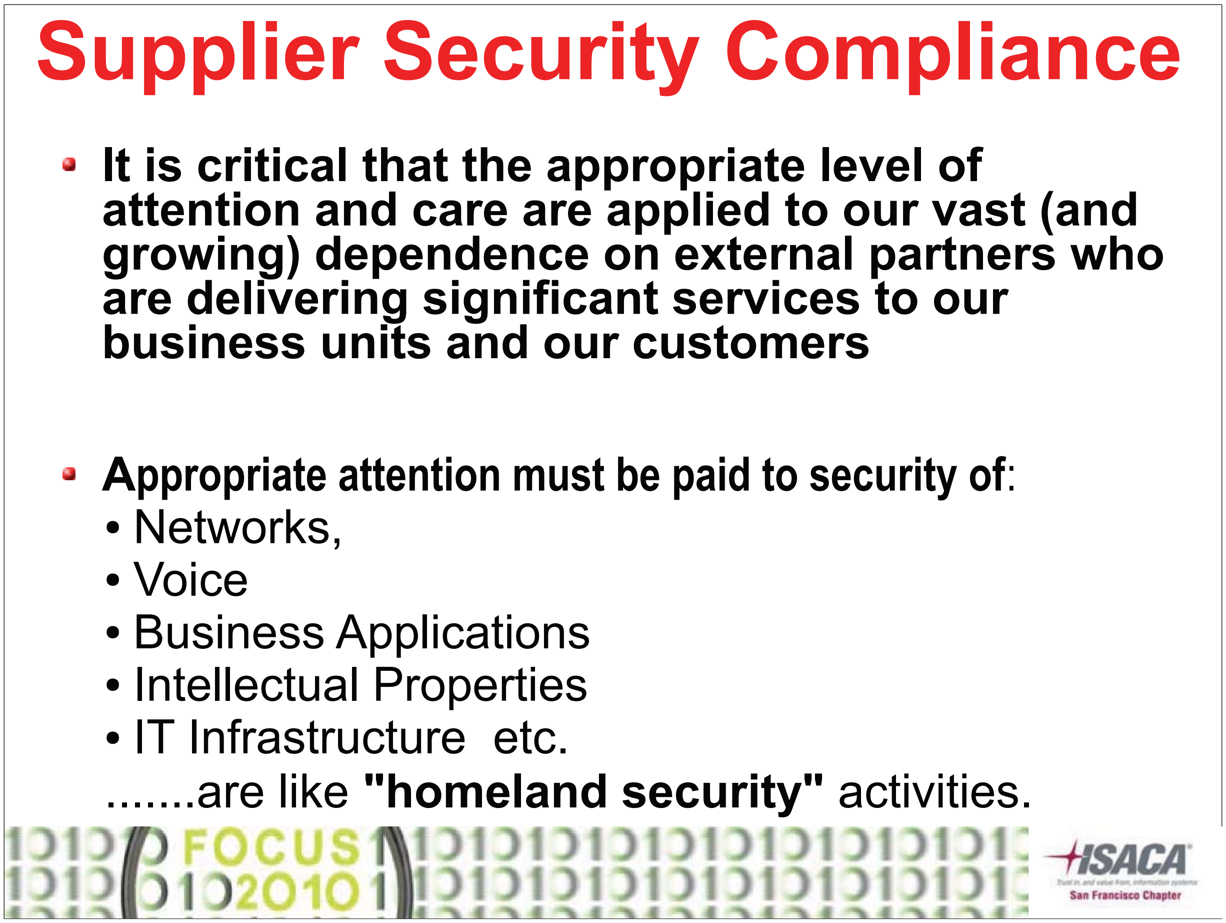
End users

The end user is the individual/entity who uses the product after it has been fully developed and ...

Island Of Outsourcing World

Mission

Effectively manage external business partner/supplier security through audit, Assessment and GRC tool to ensure critical risks are addressed while optimizing cost, consistency and speed of integration.

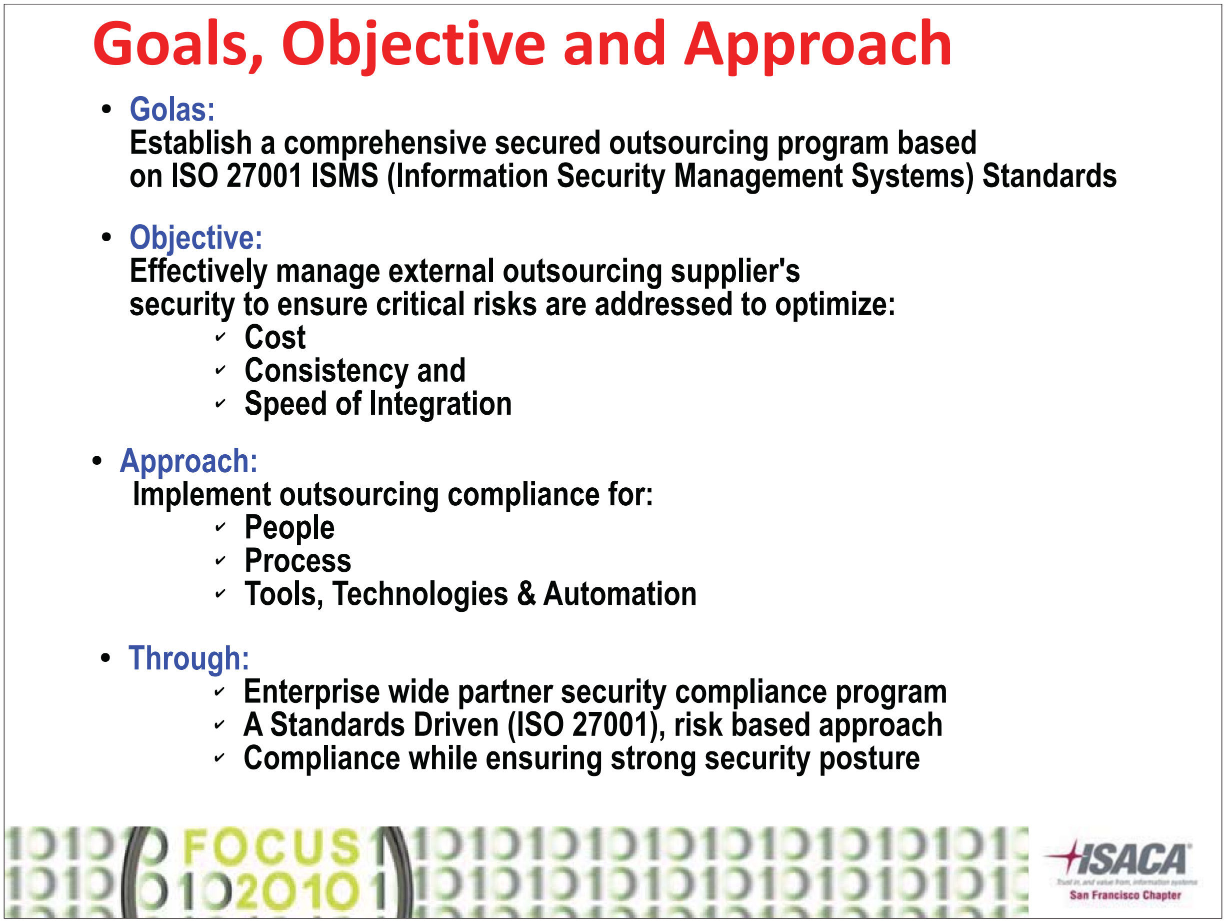


Supplier Security Compliance

- **It is critical that the appropriate level of attention and care are applied to our vast (and growing) dependence on external partners who are delivering significant services to our business units and our customers**

- **Appropriate attention must be paid to security of**:
  - Networks,
  - Voice
  - Business Applications
  - Intellectual Properties
  - IT Infrastructure etc.

  ....are like **"homeland security"** activities.



Goals, Objective and Approach

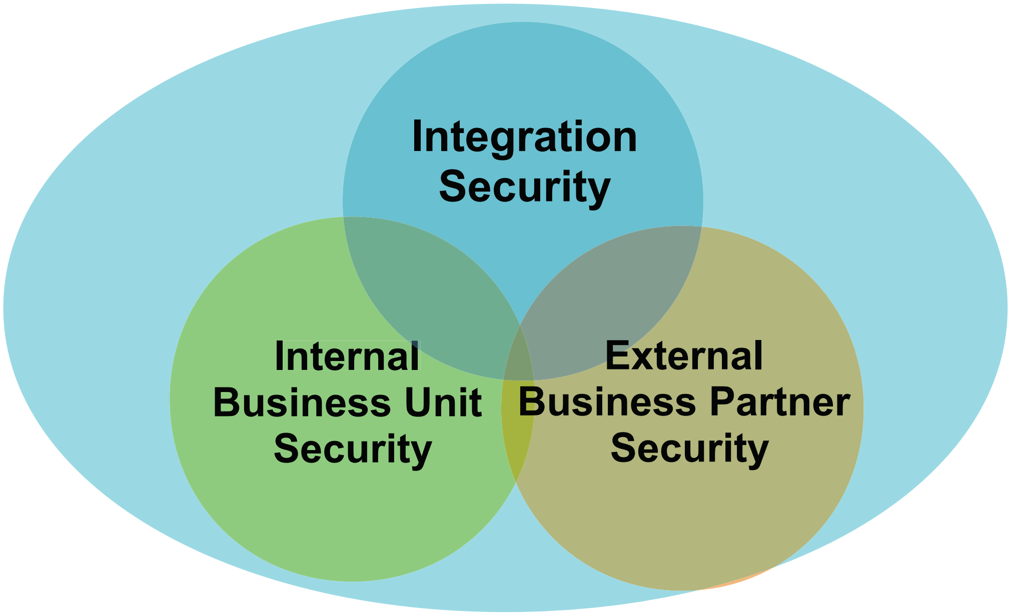
- **Golas:**
  Establish a comprehensive secured outsourcing program based on ISO 27001 ISMS (Information Security Management Systems) Standards

- **Objective:**
  Effectively manage external outsourcing supplier's security to ensure critical risks are addressed to optimize:
  - ✓ **Cost**
  - ✓ **Consistency and**
  - ✓ **Speed of Integration**

- **Approach:**
  Implement outsourcing compliance for:
  - ✓ **People**
  - ✓ **Process**
  - ✓ **Tools, Technologies & Automation**

- **Through:**
  - ✓ **Enterprise wide partner security compliance program**
  - ✓ **A Standards Driven (ISO 27001), risk based approach**
  - ✓ **Compliance while ensuring strong security posture**

Integration Strategy for Outsourcing Security



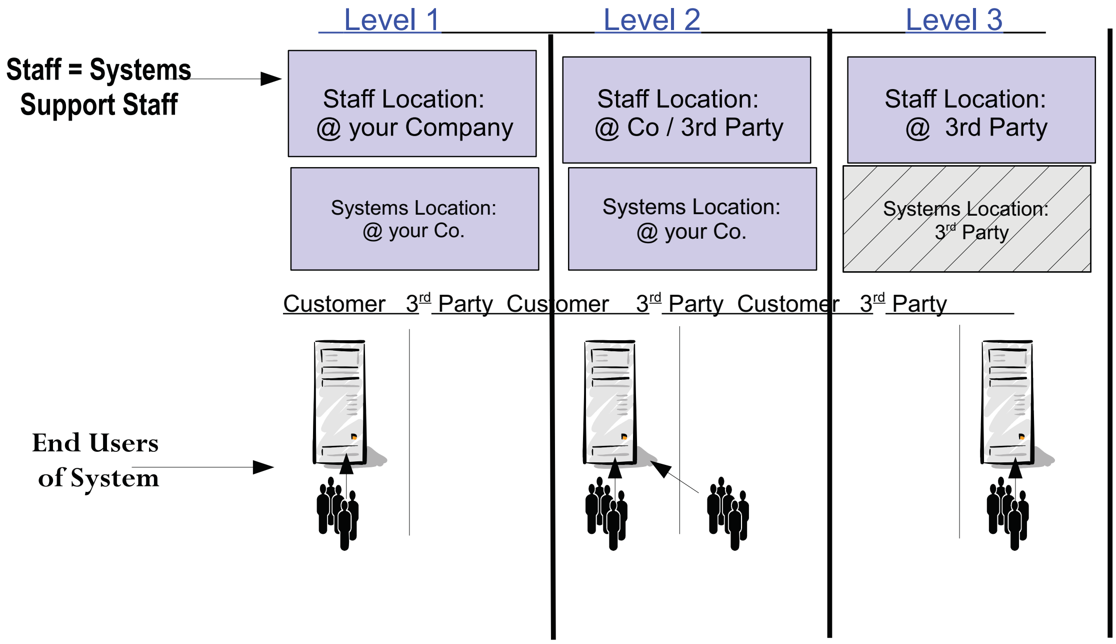
Integration Security

Internal Business Unit Security

External Business Partner Security

Security is a key requirement for successful outsourcing

Extended Enterprise Security

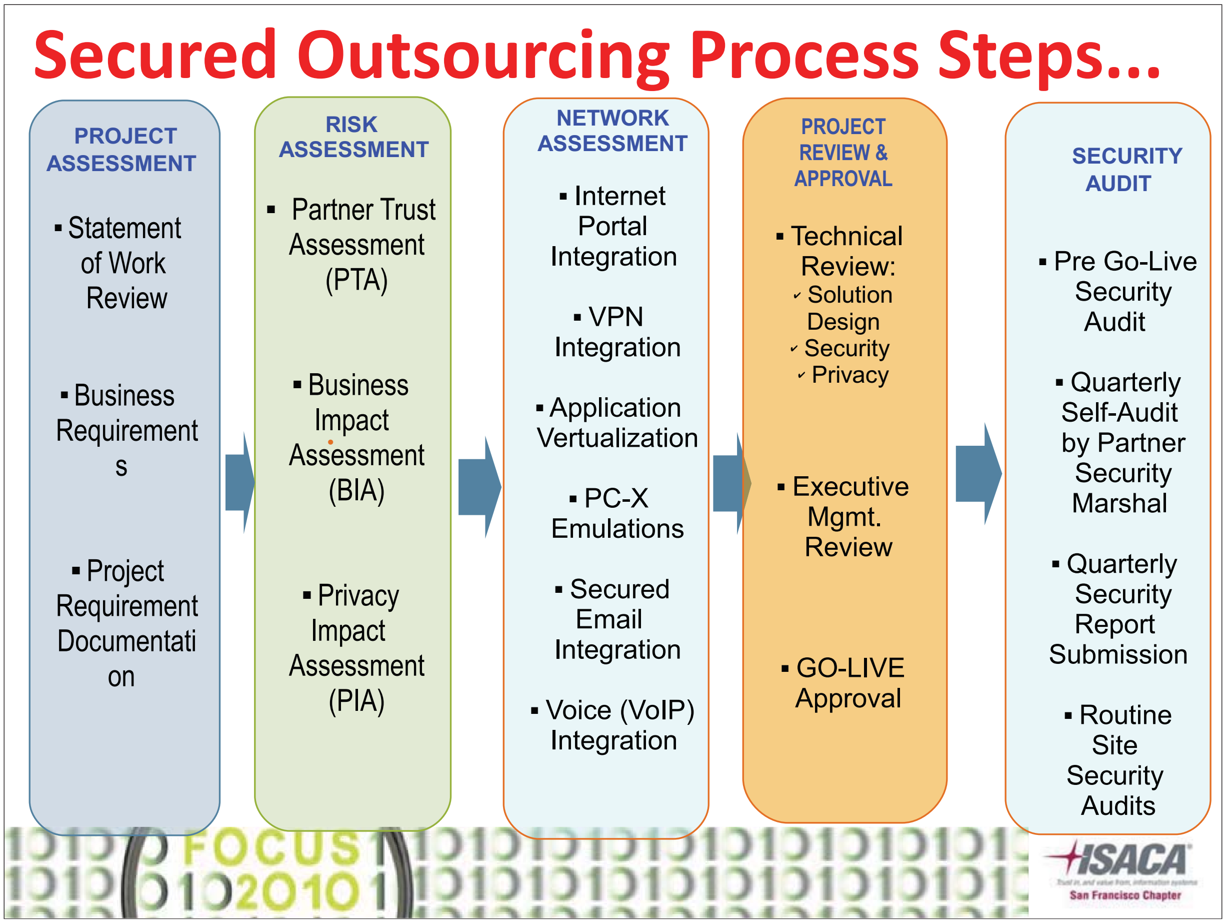


Staff = Systems Support Staff

Level 1	Level 2	Level 3
Staff Location: @ your Company	Staff Location: @ Co / 3rd Party	Staff Location: @ 3rd Party
Systems Location: @ your Co.	Systems Location: @ your Co.	Systems Location: 3rd Party

Customer 3rd Party Customer 3rd Party Customer 3rd Party

End Users of System



Secured Outsourcing Process Steps...

PROJECT ASSESSMENT

- Statement of Work Review
- Business Requirements
- Project Requirement Documentation

RISK ASSESSMENT

- Partner Trust Assessment (PTA)
- Business Impact Assessment (BIA)
- Privacy Impact Assessment (PIA)

NETWORK ASSESSMENT

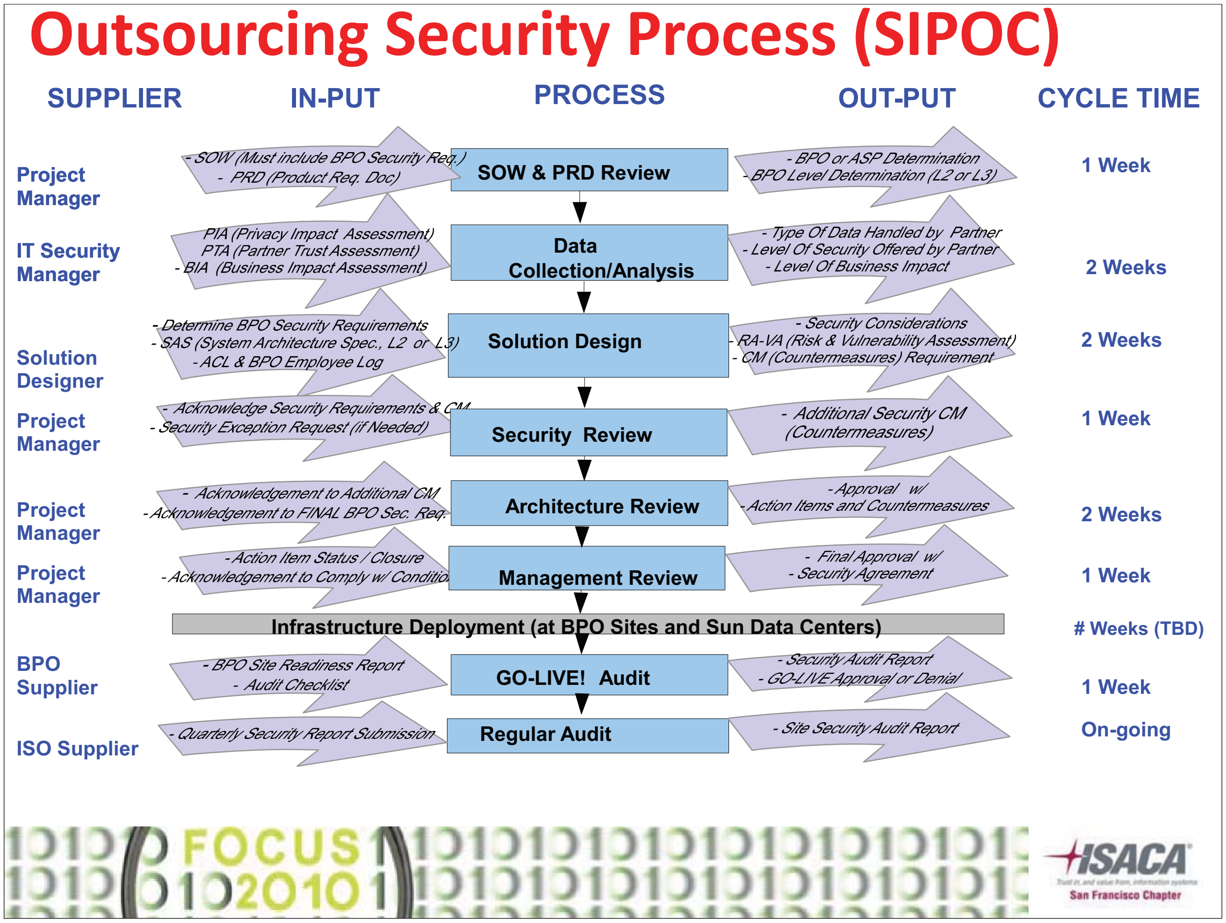
- Internet Portal Integration
- VPN Integration
- Application Vertualization
- PC-X Emulations
- Secured Email Integration
- Voice (VoIP) Integration

PROJECT REVIEW & APPROVAL

- Technical Review:
  - ✓ Solution Design
  - ✓ Security
  - ✓ Privacy
- Executive Mgmt. Review
- GO-LIVE Approval

SECURITY AUDIT

- Pre Go-Live Security Audit
- Quarterly Self-Audit by Partner Security Marshal
- Quarterly Security Report Submission
- Routine Site Security Audits



Outsourcing Security Process (SIPOC)

SUPPLIER	IN-PUT	PROCESS	OUT-PUT	CYCLE TIME
Project Manager	- SOW (Must include BPO Security Req.) - PRD (Product Req. Doc)	SOW & PRD Review	- BPO or ASP Determination - BPO Level Determination (L2 or L3)	1 Week
IT Security Manager	PIA (Privacy Impact Assessment) PTA (Partner Trust Assessment) - BIA (Business Impact Assessment)	Data Collection/Analysis	- Type Of Data Handled by Partner - Level Of Security Offered by Partner - Level Of Business Impact	2 Weeks
Solution Designer	- Determine BPO Security Requirements - SAS (System Architecture Spec., L2 or L3) - ACL & BPO Employee Log	Solution Design	- Security Considerations - RA-VA (Risk & Vulnerability Assessment) - CM (Countermeasures) Requirement	2 Weeks
Project Manager	- Acknowledge Security Requirements & CM - Security Exception Request (if Needed)	Security Review	- Additional Security CM (Countermeasures)	1 Week
Project Manager	- Acknowledgement to Additional CM - Acknowledgement to FINAL BPO Sec. Req.	Architecture Review	- Approval w/ - Action Items and Countermeasures	2 Weeks
Project Manager	- Action Item Status / Closure - Acknowledgement to Comply w/ Conditio	Management Review	- Final Approval w/ - Security Agreement	1 Week
		Infrastructure Deployment (at BPO Sites and Sun Data Centers)		# Weeks (TBD)
BPO Supplier	- BPO Site Readiness Report - Audit Checklist	GO-LIVE! Audit	- Security Audit Report - GO-LIVE Approval or Denial	1 Week
ISO Supplier	- Quarterly Security Report Submission	Regular Audit	- Site Security Audit Report	On-going

Outsourcing Risk Assessment

Risk Assessment Methodology

Security controls shall be adjusted based on risk associated with the outsourcing project in conjunction with selected supplier.

Hence per **"Risk Based Methodology"** three different types of security requirements must be mandated for suppliers.

Supplier Security Assessment

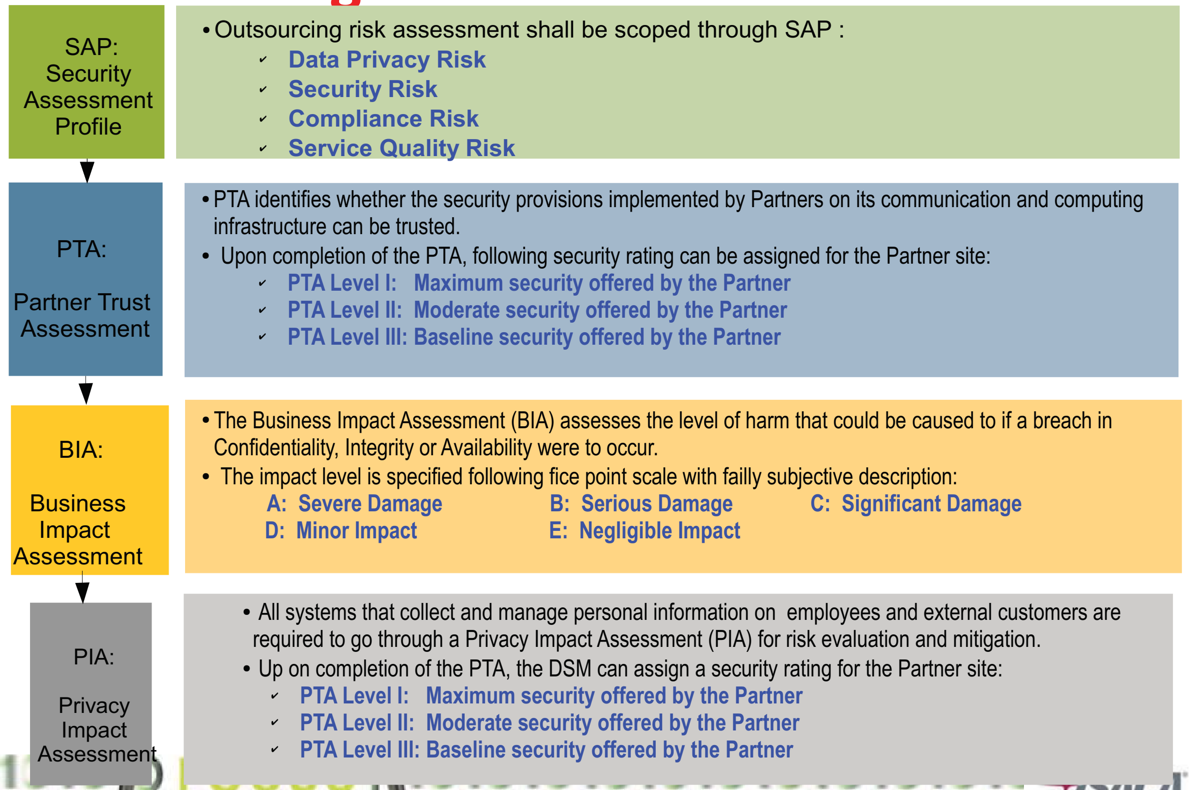
- Prior to finalization of Master Service Agreement (MSA), the Supplier must support the undertaking of
- Partner Trust Assessment (PTA)
- Security Assessment Profile (SAP)
- Business Impact Assessment (BIA)
- TVCA (Threats and Vulnerability Assessment (TVCA)
- Privacy Impact Assessment (PIA)

- Supplier must acknowledge and agree to comply with Customer's Supplier Security Policies, Standards and Requirements
  - Site and remote Audits conducted based on above Policies and Requirements document above Policies and Requirements documents

Outsourcing Risk Assessment with Risk Based Methodology

	RISK BASED METHODOLOGY MATRIX	Supplier/Partner Trust Level		
		PTA Level – I (Maximum Security Offered by the Partner)	**PTA Level – II** (Moderate Security Offered by the Partner)	**PTA Level – III** (Baseline Security Offered by the Partner)
^^^^^^^^ -------DATA SENSITIVITY-------vvvvvvv	**Risk& Impact Level I:** **DATA TYPE:** Critical **IMPACT:** Severe / Serious Impact. **SAP** (Security Assessment Profile), **BIA** (Business Impact Assessment), **TVCA** (Threats & Vulnerability Assessment), **PIA** (Privacy Impact Assessment)	**MED RISK OUTSOURCING** Partner to comply with ***"Medium Risk Security Requirements",***	**HIGH RISK OUTSOURCING** Partner to comply with ***"High Risk Security Requirements",***	NOT PERMITTED (BECAUSE VERY VERY HIGH RISK)
	Risk& Impact Level II: **DATA TYPE:** Enhanced **IMPACT:** Significant **SAP** (Security Assessment Profile), **BIA** (Business Impact Assessment), **TVCA** (Threats & Vulnerability Assessment), **PIA** (Privacy Impact Assessment)	**MED RISK OUTSOURCING** Partner to comply with ***"Medium Risk Security Requirements",***	**MED RISK OUTSOURCING** Partner to comply with ***"Medium Risk Security Requirements",***	**HIGH RISK OUTSOURCING** Partner to comply with ***"High Risk Security Requirements",***
	Risk& Impact Level III: **DATA TYPE:** Standard **IMPACT:** Minor **SAP** (Security Assessment Profile), **BIA** (Business Impact Assessment), **TVCA** (Threats & Vulnerability Assessment), **PIA** (Privacy Impact Assessment)	**LOW RISK OUTSOURCING** Partner to comply with ***"Low Risk Security Requirements",***	**LOW RISK OUTSOURCING** Partner to comply with ***"Low Risk Security Requirements",***	**LOW RISK OUTSOURCING** Partner to comply with ***"Low Risk Security Requirements",***

Outsourcing Risk Assessment Process



SAP: Security Assessment Profile

- Outsourcing risk assessment shall be scoped through SAP :
  - ✓ **Data Privacy Risk**
  - ✓ **Security Risk**
  - ✓ **Compliance Risk**
  - ✓ **Service Quality Risk**

PTA: Partner Trust Assessment

- PTA identifies whether the security provisions implemented by Partners on its communication and computing infrastructure can be trusted.
- Upon completion of the PTA, following security rating can be assigned for the Partner site:
  - ✓ **PTA Level I: Maximum security offered by the Partner**
  - ✓ **PTA Level II: Moderate security offered by the Partner**
  - ✓ **PTA Level III: Baseline security offered by the Partner**

BIA: Business Impact Assessment

- The Business Impact Assessment (BIA) assesses the level of harm that could be caused to if a breach in Confidentiality, Integrity or Availability were to occur.
- The impact level is specified following fice point scale with failly subjective description:

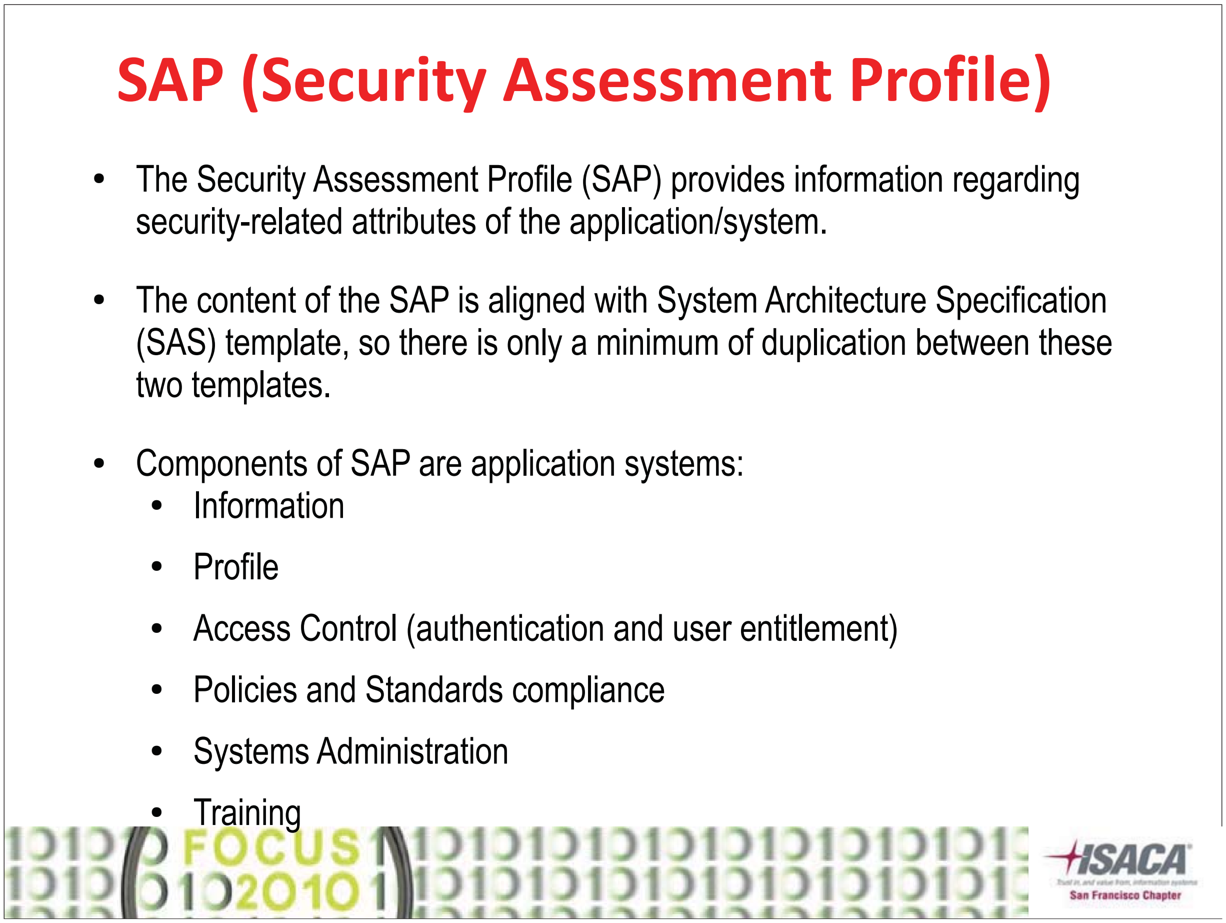
A: Severe Damage **B: Serious Damage** **C: Significant Damage**
D: Minor Impact **E: Negligible Impact**

PIA: Privacy Impact Assessment

- All systems that collect and manage personal information on employees and external customers are required to go through a Privacy Impact Assessment (PIA) for risk evaluation and mitigation.
- Up on completion of the PTA, the DSM can assign a security rating for the Partner site:
  - ✓ **PTA Level I: Maximum security offered by the Partner**
  - ✓ **PTA Level II: Moderate security offered by the Partner**
  - ✓ **PTA Level III: Baseline security offered by the Partner**

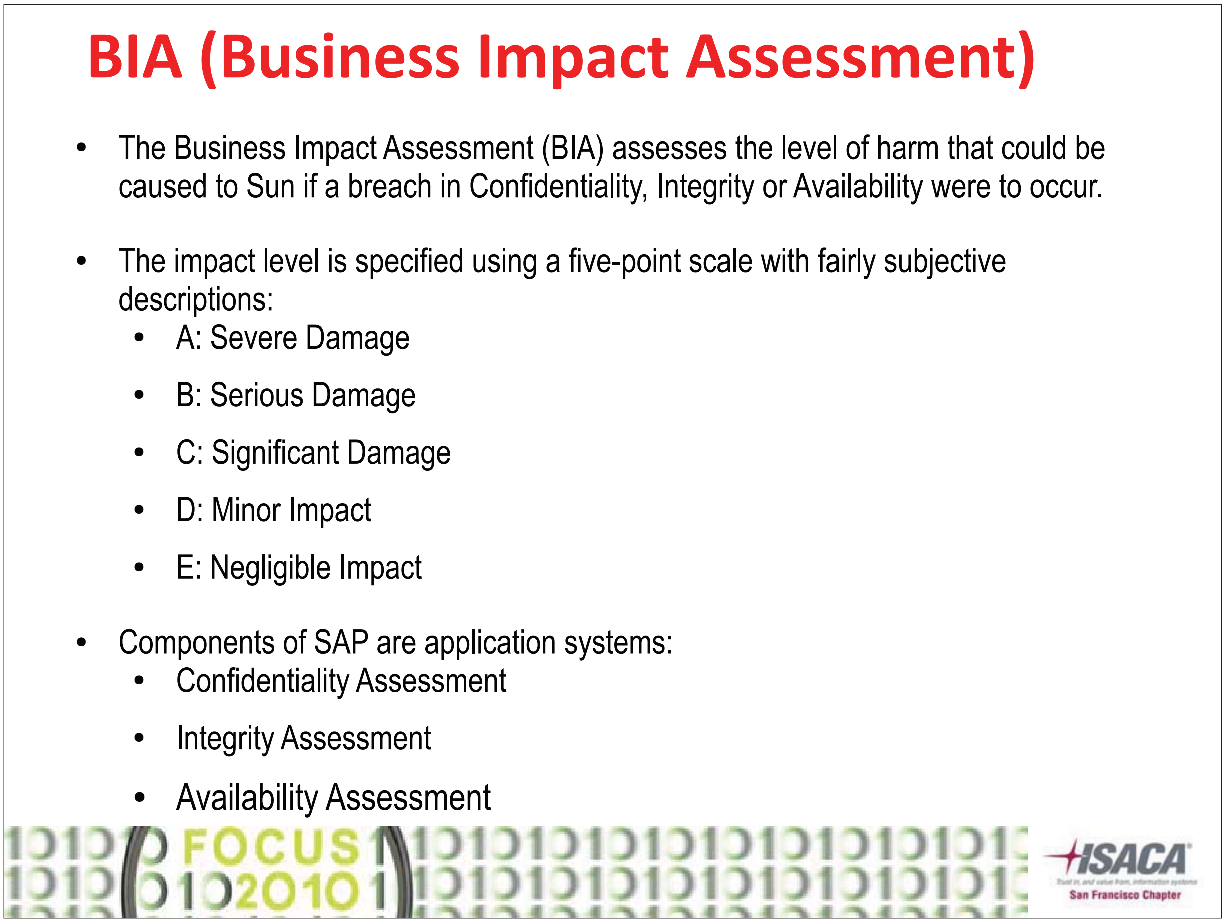
PTA (Partner Trust Assessment)

- PTA is required if an external parter is involved in the project.
- Customer requires different levels of security controls to be implemented at the Partner's sites, depending upon the type of service(s) provided and/or type of data handled by the Partner. In order to determine the level of security controls already present at a Partner site, a Partner Trust Assessment (PTA) is required.
- PTA identifies whether the security provisions implemented by Partners on its communication and computing infrastructure can be trusted.
- Upon completion of the PTA, the DSM can assign a security rating for the Partner site:
  - **PTA Level I:** Maximum security offered by the Partner
  - **PTA Level II:** Moderate security offered by the Partner
  - **PTA Level III:** Baseline security offered by the Partner



SAP (Security Assessment Profile)

- The Security Assessment Profile (SAP) provides information regarding security-related attributes of the application/system.
- The content of the SAP is aligned with System Architecture Specification (SAS) template, so there is only a minimum of duplication between these two templates.
- Components of SAP are application systems:
  - Information
  - Profile
  - Access Control (authentication and user entitlement)
  - Policies and Standards compliance
  - Systems Administration
  - Training



BIA (Business Impact Assessment)

- The Business Impact Assessment (BIA) assesses the level of harm that could be caused to Sun if a breach in Confidentiality, Integrity or Availability were to occur.
- The impact level is specified using a five-point scale with fairly subjective descriptions:
  - A: Severe Damage
  - B: Serious Damage
  - C: Significant Damage
  - D: Minor Impact
  - E: Negligible Impact
- Components of SAP are application systems:
  - Confidentiality Assessment
  - Integrity Assessment
  - Availability Assessment

TVCA (Threats and Vulnerability Assessment)

- The purpose of the TVCA is to assess the vulnerability in business process and application/systems, in conjunction with the threats profile (as articulated in the worksheet) to Sun from a successful breach in Confidentiality, Integrity or Availability, as identified in the Business Impact Assessment.
- The assign vulnerability ratings to the likelihood of threats materializing, using the following ratings.
  - A: Probable (> 12 incidents/year)
  - B: Highly likely (5-12 incidents/year)
  - C: Possible (1-4 incidents/year)
  - D: Unlikely (< 1 incident/year)
  - E: Impossible (cannot occur)

Audit & Assurance

Audit Mission

To provide Senior Management with an independent and objective assessment of the Supplier's compliance with ISO 27001 framework and sustain a systematic approach to improve the effectiveness of the Supplier security compliance and governance processes.

Audit Goal

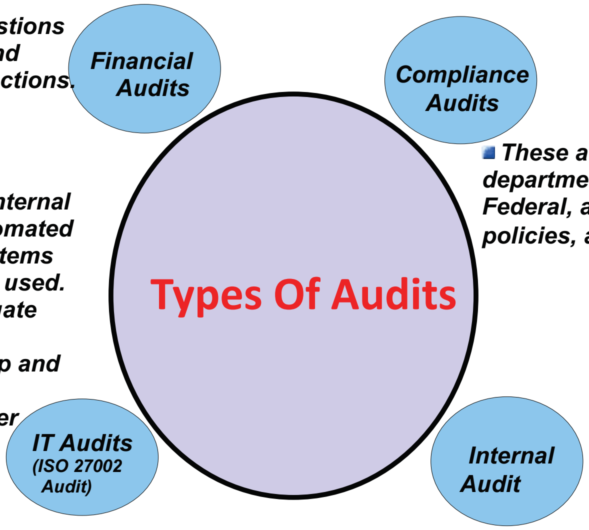
- Effectively and efficiently manage Supplier (aka: OD Data Centers, BPO Partners, Support/Services Vendors) security to ensure critical risks related to Supplier security models are addressed.
- Continuously improve the Supplier Security compliance through ISO 27001/2 aligned Standards, Policies, processes, tools and technologies.

Audit Objective

- Identify risks, vulnerabilities and nonconformities
- Eradicate risks and vulnerabilities through countermeasures
- Obtain and maintain confidence in security capability of Supplier
- Educate and train Supplier Security Marshal
- Contribute to Supplier's security compliance improvement

Types of Audit

- *These audits address questions of accounting, recording, and reporting of financial transactions.*



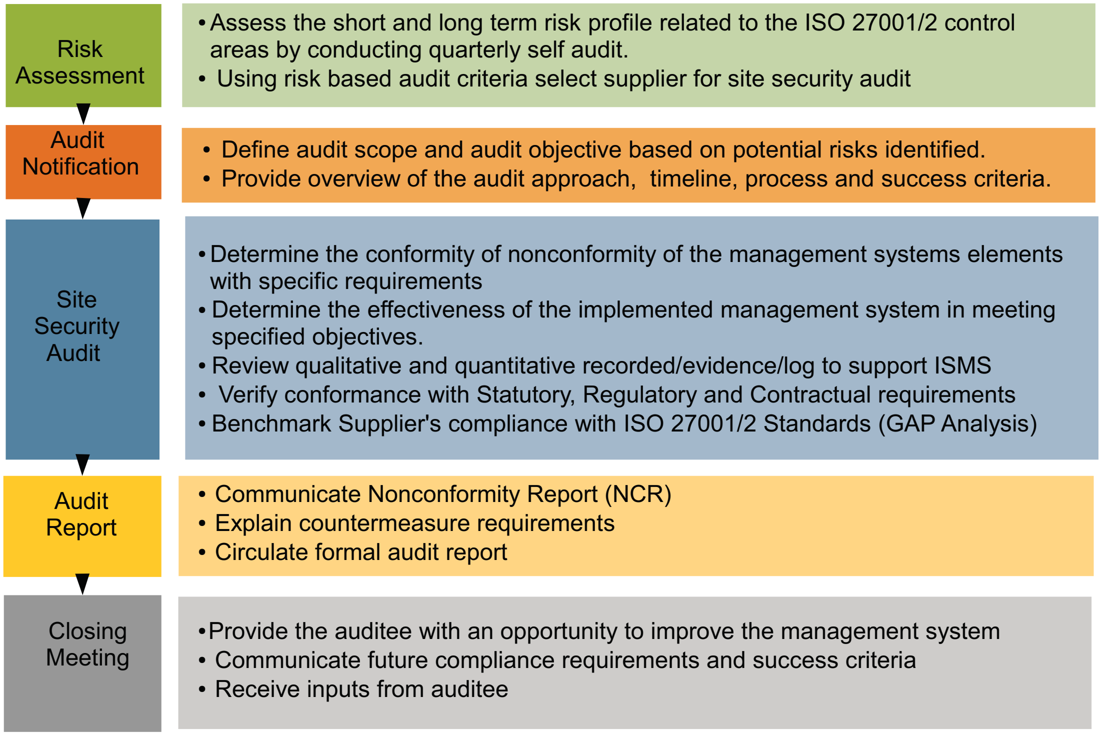
- *These audits seek to determine if departments are adhering to State, Federal, and U.T. System rules, policies, and procedures.*

- *These audit address the internal control environment of automated information processing systems and how these systems are used. These audits typically evaluate system input, output and processing controls, backup and recovery plans, and system security, as well as computer facility reviews.*

- *These audits review the adequacy of internal controls within the department and determines whether a control conscious environment exists.*

Source: Uni. Of Texas

Audit Process Overview



Risk Assessment

- Assess the short and long term risk profile related to the ISO 27001/2 control areas by conducting quarterly self audit.
- Using risk based audit criteria select supplier for site security audit

Audit Notification

- Define audit scope and audit objective based on potential risks identified.
- Provide overview of the audit approach, timeline, process and success criteria.

Site Security Audit

- Determine the conformity of nonconformity of the management systems elements with specific requirements
- Determine the effectiveness of the implemented management system in meeting specified objectives.
- Review qualitative and quantitative recorded/evidence/log to support ISMS
- Verify conformance with Statutory, Regulatory and Contractual requirements
- Benchmark Supplier's compliance with ISO 27001/2 Standards (GAP Analysis)

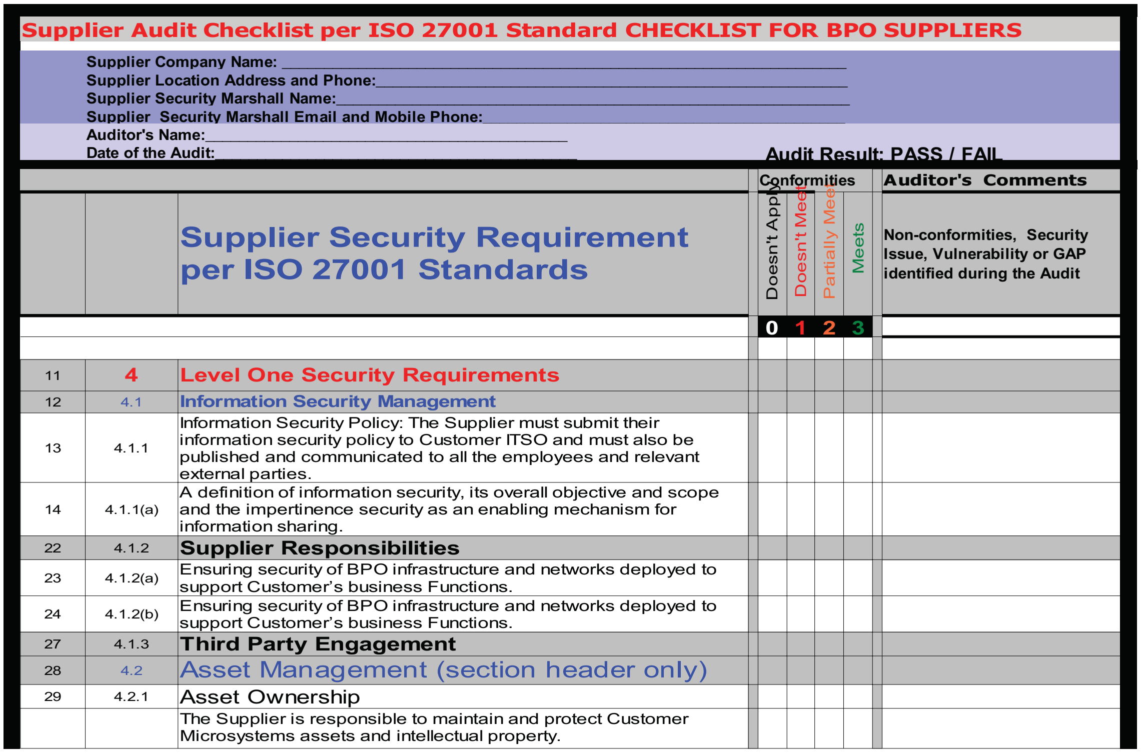
Audit Report

- Communicate Nonconformity Report (NCR)
- Explain countermeasure requirements
- Circulate formal audit report

Closing Meeting

- Provide the auditee with an opportunity to improve the management system
- Communicate future compliance requirements and success criteria
- Receive inputs from auditee

Audit Checklist with Success Criteria Scoring



Supplier Audit Checklist per ISO 27001 Standard CHECKLIST FOR BPO SUPPLIERS

Supplier Company Name: ____
Supplier Location Address and Phone:_______________________________________
Supplier Security Marshall Name:____
Supplier Security Marshall Email and Mobile Phone:____________________________
Auditor's Name:______________________________
Date of the Audit:______________________________

Audit Result: PASS / FAIL

			Conformities				Auditor's Comments
		Supplier Security Requirement per ISO 27001 Standards	Doesn't Apply	Doesn't Meet	Partially Meet	Meets	Non-conformities, Security Issue, Vulnerability or GAP identified during the Audit
			0	1	2	3	
11	4	**Level One Security Requirements**					
12	4.1	**Information Security Management**					
13	4.1.1	Information Security Policy: The Supplier must submit their information security policy to Customer ITSO and must also be published and communicated to all the employees and relevant external parties.					
14	4.1.1(a)	A definition of information security, its overall objective and scope and the impertinence security as an enabling mechanism for information sharing.					
22	4.1.2	**Supplier Responsibilities**					
23	4.1.2(a)	Ensuring security of BPO infrastructure and networks deployed to support Customer's business Functions.					
24	4.1.2(b)	Ensuring security of BPO infrastructure and networks deployed to support Customer's business Functions.					
27	4.1.3	**Third Party Engagement**					
28	4.2	Asset Management (section header only)					
29	4.2.1	Asset Ownership					
		The Supplier is responsible to maintain and protect Customer Microsystems assets and intellectual property.					

Risk Based Audit Methodology (ISO 27001)

ISO 27001 ISMS Controls	Partner's Risk Profile		
	L	M	H
Security Policy	X	X	X
Organization of information Security	X	X	X
Asset Management	X	X	
Human Resources Security	X	X	X
Physical and Environmental Security	X	X	X
Communications and Operations Management	X	X	X
Access Control	X	X	X
Information Systems Development and Maintenance	X	X	
Information Security Incident Management	X	X	
Business Continuity Management	X	X	
Compliance (Legal, Regulatory and Contractual)	X	X	

Partners are categorized into High, Medium, Low risk profile and audited against applicable ISO 27002 Controls (per "X" in above table)

Audit Success Criteria

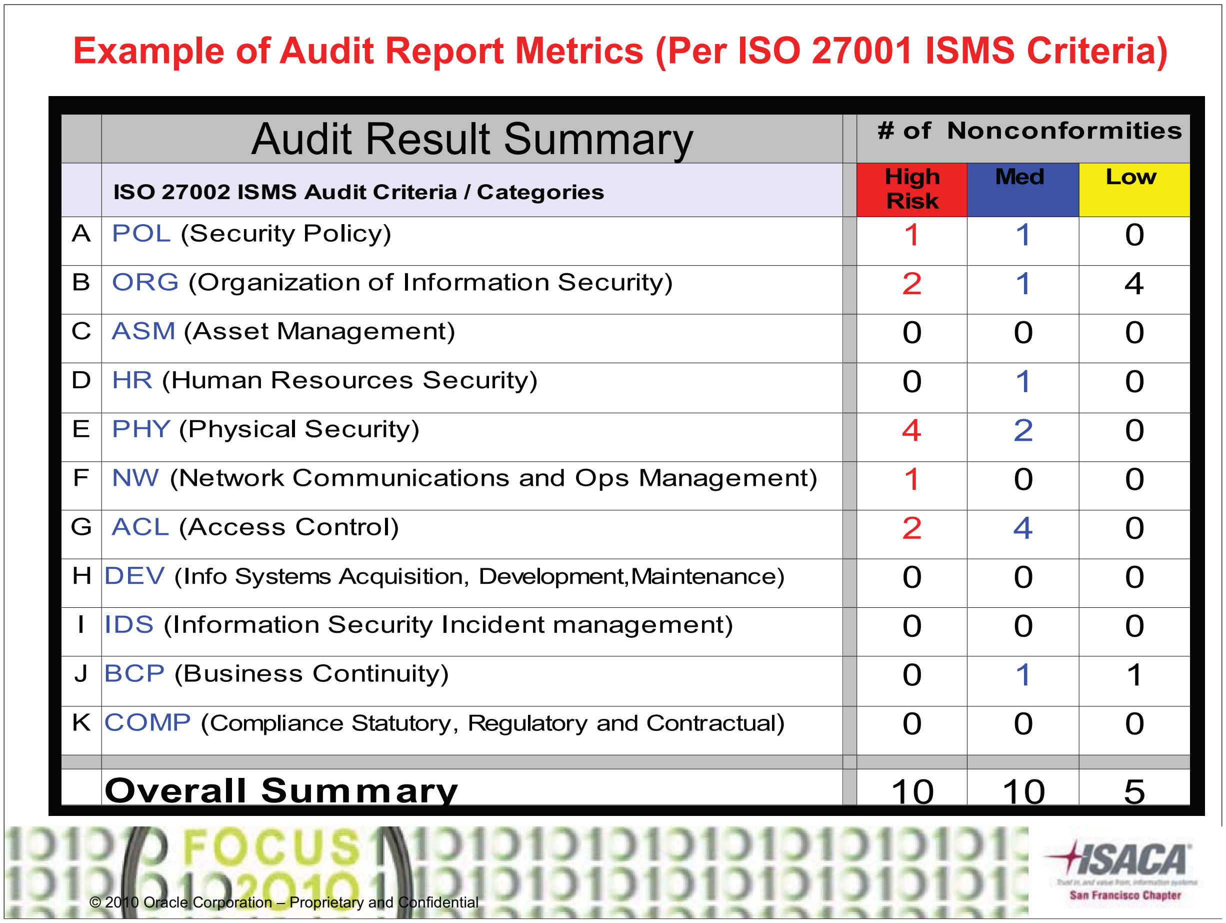
- Conformities against Policies, Procedures and Requirements
- Reference against Qualitative and Quantitative Audit Evidence (records, statements of fact or other information)
- The extent of Conformity with ISO 27001 - ISMS (Information Security Management System) Standards
- The effective Implementation, Maintenance and Improvement of the ISMS
- The Capability of the Management Review Process to ensure the continuing suitability, adequacy, effectiveness and improvement of the ISMS

What Constitute Audit Failure

- **3 or more NONCONFORMITIS (NC) with HIGH risk which may result into audit failure.**
- **Some example of HIGH risk Nonconformities:**
  - Noncompliance with OWAN connectivity architecture
  - Unauthorized method to access OWAN
  - Risking OWAN through possibility of Virus, Worm or malicious attack
  - Unsecured practices to handle Oracle's Intellectual Properties (Capital Equipments, Hardware/Software and Documentation)
  - Unauthorized or unintended access/disclosure of Oracle's intellectual property

Consequences of Audit Failure

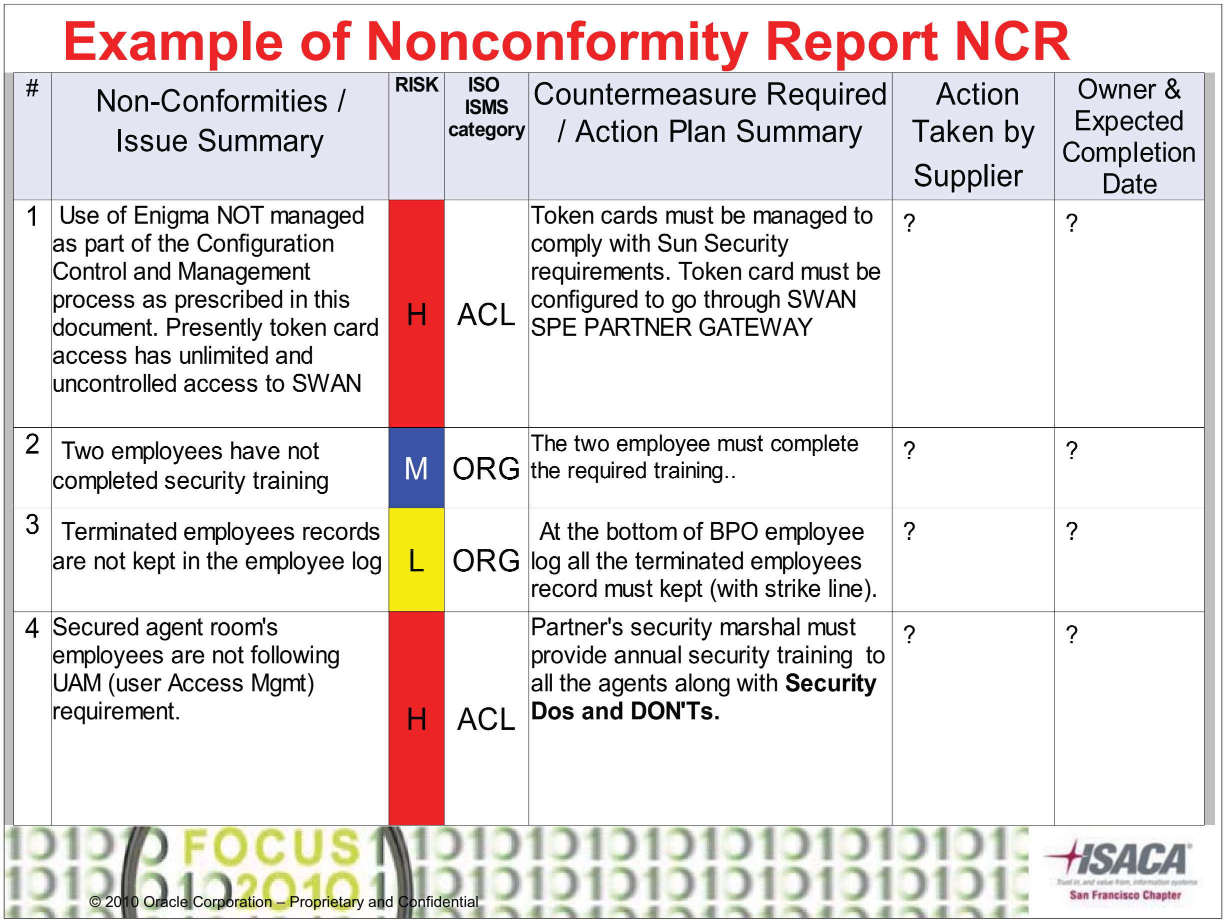
- **Contract Termination (If SLA/Contract mandates_**
- **Terminate Historic Exceptions and No Exceptions in the Future**
- **No / Limited Access to Customer's Intranet**
- **No Change Request**
- **Auditor conducts unannounced audit to verify countermeasure implementation**



Example of Audit Report Metrics (Per ISO 27001 ISMS Criteria)

	Audit Result Summary	# of Nonconformities		
	ISO 27002 ISMS Audit Criteria / Categories	High Risk	Med	Low
A	POL (Security Policy)	1	1	0
B	ORG (Organization of Information Security)	2	1	4
C	ASM (Asset Management)	0	0	0
D	HR (Human Resources Security)	0	1	0
E	PHY (Physical Security)	4	2	0
F	NW (Network Communications and Ops Management)	1	0	0
G	ACL (Access Control)	2	4	0
H	DEV (Info Systems Acquisition, Development,Maintenance)	0	0	0
I	IDS (Information Security Incident management)	0	0	0
J	BCP (Business Continuity)	0	1	1
K	COMP (Compliance Statutory, Regulatory and Contractual)	0	0	0
	Overall Summary	10	10	5

FOCUS 2010
ISACA
San Francisco Chapter



Example of Nonconformity Report NCR

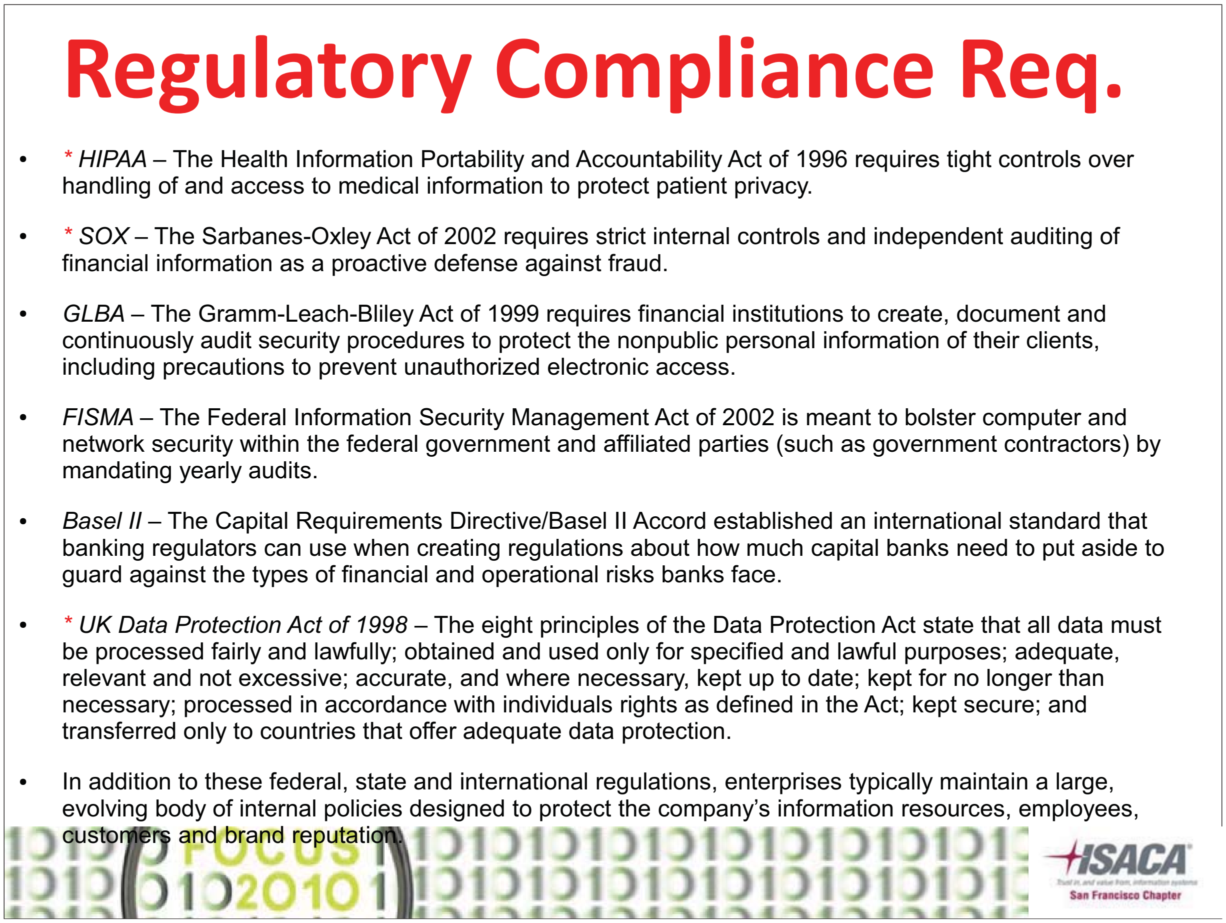
#	Non-Conformities / Issue Summary	RISK	ISO ISMS category	Countermeasure Required / Action Plan Summary	Action Taken by Supplier	Owner & Expected Completion Date
1	Use of Enigma NOT managed as part of the Configuration Control and Management process as prescribed in this document. Presently token card access has unlimited and uncontrolled access to SWAN	H	ACL	Token cards must be managed to comply with Sun Security requirements. Token card must be configured to go through SWAN SPE PARTNER GATEWAY	?	?
2	Two employees have not completed security training	M	ORG	The two employee must complete the required training..	?	?
3	Terminated employees records are not kept in the employee log	L	ORG	At the bottom of BPO employee log all the terminated employees record must kept (with strike line).	?	?
4	Secured agent room's employees are not following UAM (user Access Mgmt) requirement.	H	ACL	Partner's security marshal must provide annual security training to all the agents along with **Security Dos and DON'Ts.**	?	?

Section IV:

Appendices

Compliance Management Process

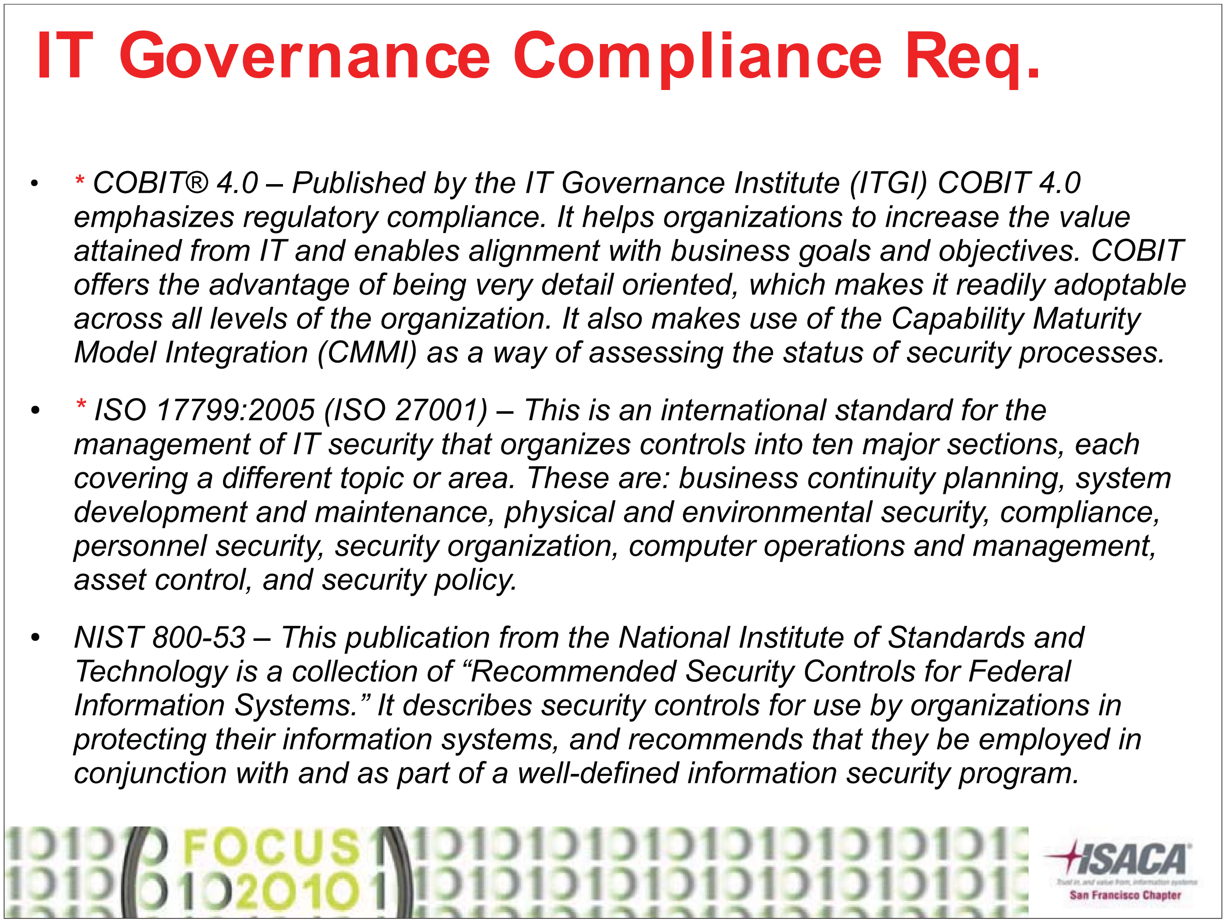
- Document your existing control framework and test plans, mapping them to applicable control standards, regulations and business processes.
- Configure data elements and modify the solution workflow to manage your company's specific compliance processes with no custom code or additional development.
- Determine which controls need to be tested during a given assessment period through risk-based scooping.
- Manage control testing processes, including control self-assessments, test plan execution, and automated evaluations captured through integration with third-party scanning tools.
- Inform testers of their tasks via rules-driven email notifications and a "My Tasks" list on role-specific home pages.
- Generate deficiencies automatically for non-compliant control activities, map those deficiencies to policies, regulations and risks, and resolve them through remediation or exception requests.
- Utilize Archer's real-time reporting and dashboard capabilities to form a consolidated picture of compliance efforts and remediation processes.



Regulatory Compliance Req.

- * *HIPAA* – The Health Information Portability and Accountability Act of 1996 requires tight controls over handling of and access to medical information to protect patient privacy.
- * *SOX* – The Sarbanes-Oxley Act of 2002 requires strict internal controls and independent auditing of financial information as a proactive defense against fraud.
- *GLBA* – The Gramm-Leach-Bliley Act of 1999 requires financial institutions to create, document and continuously audit security procedures to protect the nonpublic personal information of their clients, including precautions to prevent unauthorized electronic access.
- *FISMA* – The Federal Information Security Management Act of 2002 is meant to bolster computer and network security within the federal government and affiliated parties (such as government contractors) by mandating yearly audits.
- *Basel II* – The Capital Requirements Directive/Basel II Accord established an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face.
- * *UK Data Protection Act of 1998* – The eight principles of the Data Protection Act state that all data must be processed fairly and lawfully; obtained and used only for specified and lawful purposes; adequate, relevant and not excessive; accurate, and where necessary, kept up to date; kept for no longer than necessary; processed in accordance with individuals rights as defined in the Act; kept secure; and transferred only to countries that offer adequate data protection.
- In addition to these federal, state and international regulations, enterprises typically maintain a large, evolving body of internal policies designed to protect the company's information resources, employees, customers and brand reputation.

FOCUS
2010
ISACA
San Francisco Chapter



IT Governance Compliance Req.

- * *COBIT® 4.0 – Published by the IT Governance Institute (ITGI) COBIT 4.0 emphasizes regulatory compliance. It helps organizations to increase the value attained from IT and enables alignment with business goals and objectives. COBIT offers the advantage of being very detail oriented, which makes it readily adoptable across all levels of the organization. It also makes use of the Capability Maturity Model Integration (CMMI) as a way of assessing the status of security processes.*
- * *ISO 17799:2005 (ISO 27001) – This is an international standard for the management of IT security that organizes controls into ten major sections, each covering a different topic or area. These are: business continuity planning, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer operations and management, asset control, and security policy.*
- *NIST 800-53 – This publication from the National Institute of Standards and Technology is a collection of "Recommended Security Controls for Federal Information Systems." It describes security controls for use by organizations in protecting their information systems, and recommends that they be employed in conjunction with and as part of a well-defined information security program.*

Information Security Compliance Requirements

- ***SECURITY POLICIES*** – Security Policy is “Management's Security Statement” for the “Environment” in conjunction with Organizational Goals, Organizational Objectives, Shareholders Interests, Laws and regulations.
- ***STANDARDS*** – The Standards refer to hardware and software solutions that are selected to address a security risk being standardized throughout the enterprise. e,g: anti virus product usage,token card usage for VPN etc.
- ***PROCEDURE*** – The Procedure are the way to ensure that the intent of policy is enforced through a mandated series of steps that must be followed to accomplish a task. Procedure are statement of step-by-step actions to be performed to accomplish a security requirement, process or objective. They are one of the most powerful tools available in security arsenals.
- ***BASELINES*** – The Baselines are the benchmarks used to ensure that a minimum level security configuration is provided across multiple implementation of systems and many different products, Baselines are description of how to implement security mechanisms ensure that the implementation results into consistent level of security throughout the organization.
- ***GUIDELINES*** – The Guidelines are recommendations!!! Guidelines will remain as recommendations unless mandated by company policy and adopted as standards. They are white papers., best practices, or formats for a security programs.
- ***BEST PRACTICES*** – The Governance should follow internationally accepted “Best Practices.” A security program must have the supporting processes and procedures that will ensure a consistent and measurable level of protection.
- ***SECURITY AWARENESS –*** *The Security Awareness Training provides employees with a reminder of their security responsibilities. The Objective is to motivate personnel to comply with security requirements.*

Q & A

Thanks!

Raj A. Patel,

Oracle Corporation, USA

October 6, 2010