

# Vendor (& Partner)

## Information Security Risk Management

How do you tell what you need to tell?

How do you know what you need to know?

**PivotPoint**  
SECURITY  
SIMPLIFIED

# Outsourcing Provides Notable Rewards



- ▶ Reduced Operating Costs
- ▶ Streamlined Operations
- ▶ Time to Market
- ▶ Flexibility





Rewards don't come without Risk .....

# Outsourcing Creates Notable Risks

- ▶ Data Breach Requiring Notification
- ▶ Failure to Comply with Laws/Regulations



- ▶ Intellectual Property Disclosure
- ▶ Failure to meet Service Level Agreements

Douglas Curling, President of Choicepoint



ISO 27001  
CERTIFIED



# NLST



**Increasing pressure from  
Regulators/ Auditors to ensure that  
we can prove that key vendors are  
secure and compliant ...**

**One key point ...**

You can Outsource ... your Call Center



You can Outsource ...

your Application Development Center





You can even Outsource ... your Entire IT Operation



PivotPoint  
SECURITY  
SIMPLIFIED

But you **CAN'T** Outsource Responsibility or Liability



# Responsibility Isn't Always Obvious

- ▶ Offshore the dev/hosting of an app that processes ePHI/accepts credit card payments
  - Dev shop colo's the application in US
    - EC2 leveraged for redundancy/capacity
  - Payments via separate third party transaction
  - Dev shop & we enjoy privileged access to app
  - Managed security provided by 3<sup>rd</sup> Party Soc
  - Oracle personnel manage RAC implementation



# Responsibility Isn't Always Obvious

How do I know we/they are secure?

How do I prove we/they are compliant?

What attestation do I ask for ?

From whom?



# What's left that I am Responsible for?

## ▶ Infinite Outsourcing Scenarios -

some can get very interesting

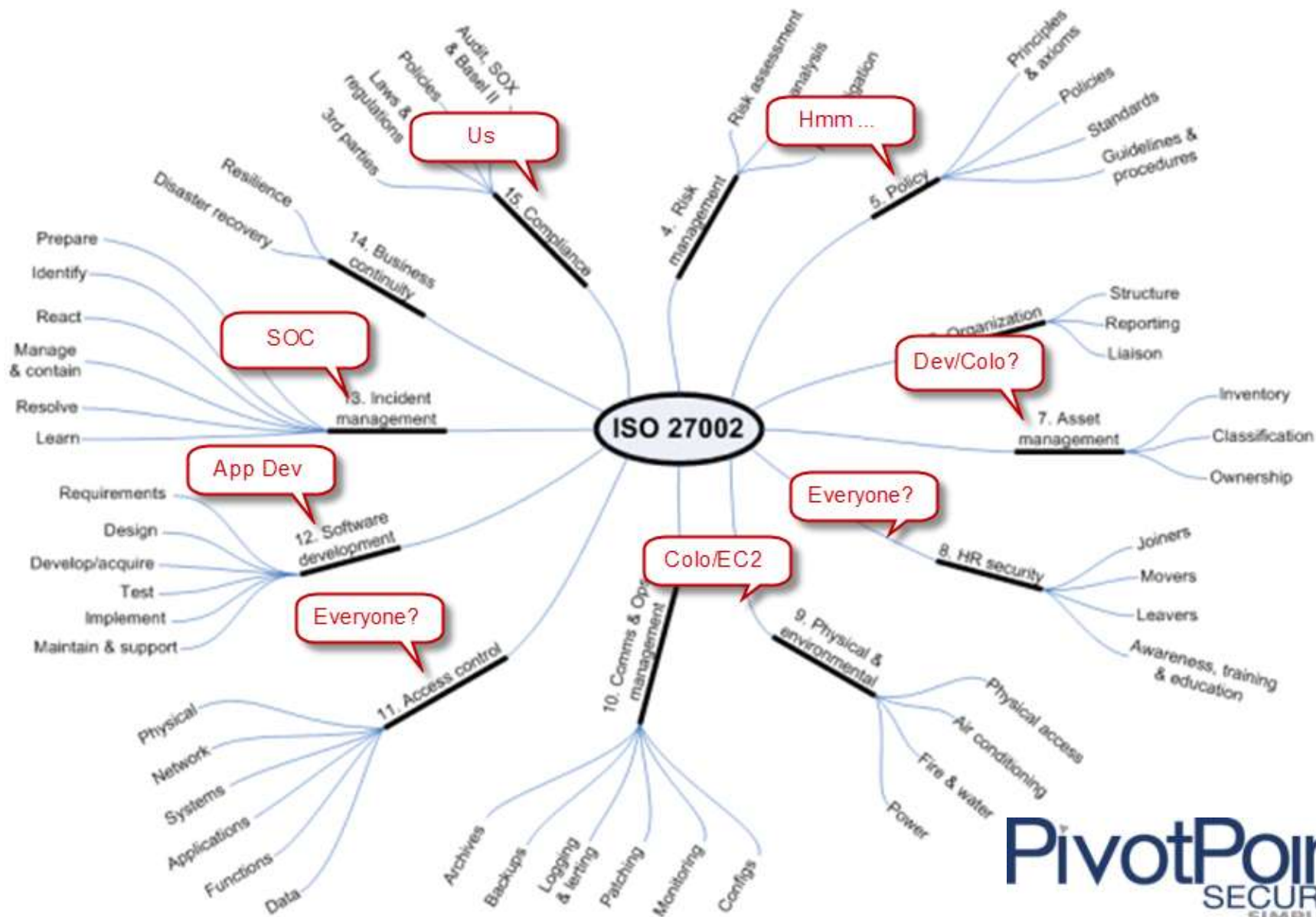
- A G2000 that has outsourced its entire IT operations?
- What happens when SOX auditors discover that AD accounts for key IP stakeholders (that were fired for cause) have been re-enabled?



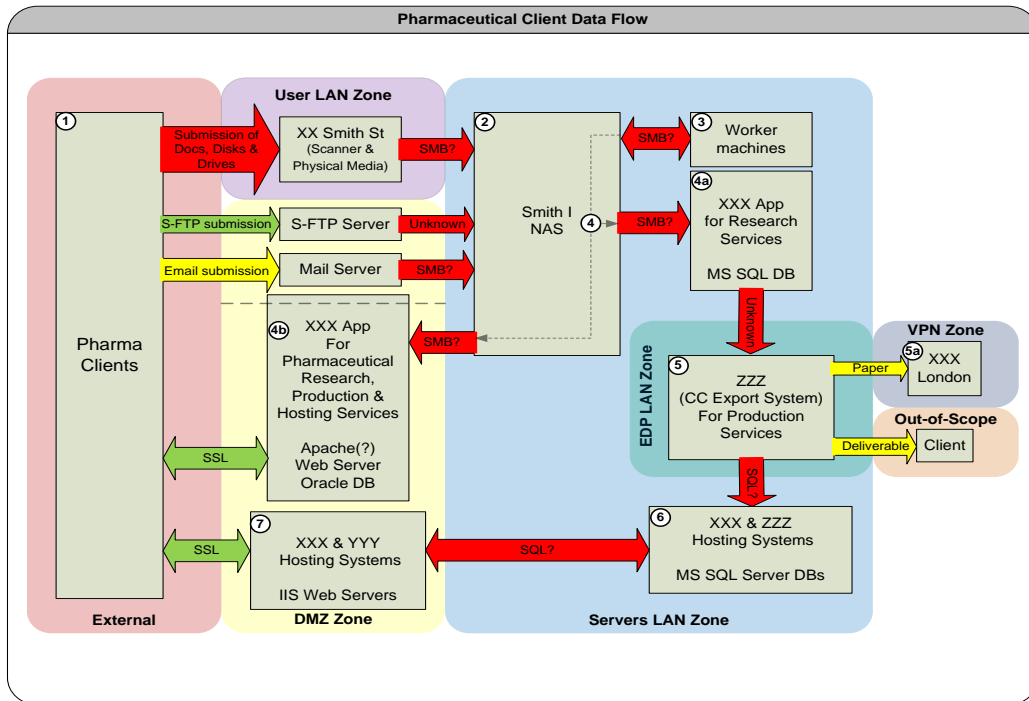
# Whose ISMS is it Anyway?



# Perhaps more granularity will help ...



# Remind me again what an ISMS is ?

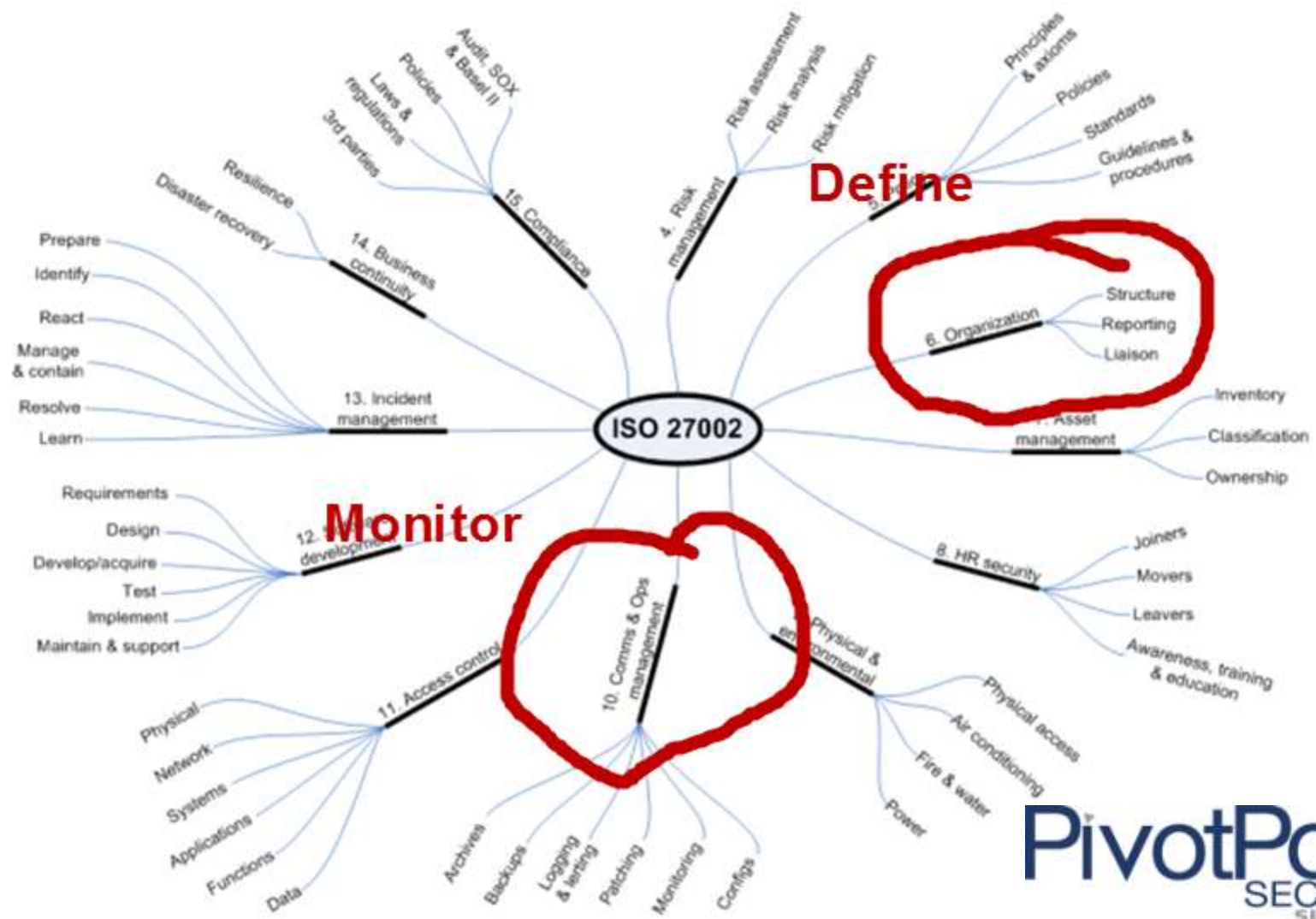


- Understanding information security requirements and the need to establish policy and objectives
- Implementing/operating controls to manage information security risks
- Monitoring/reviewing the ISMS's effectiveness
- Continual Improvement



It's always your ISMS !

(and theirs)





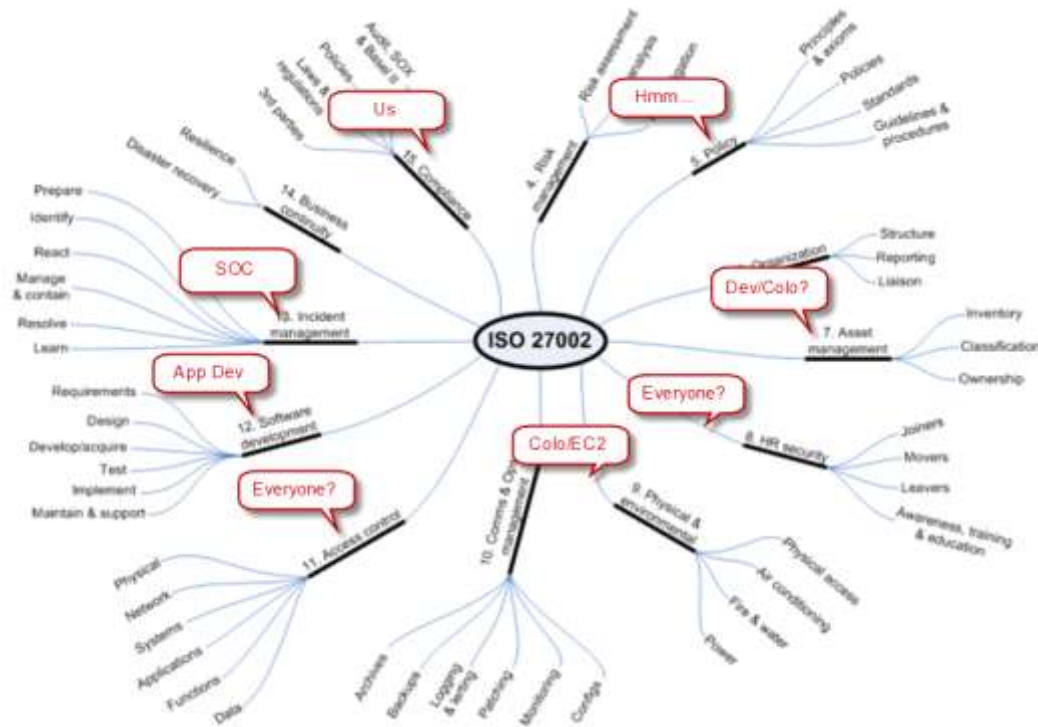
# ISMS's are not a Zero Sum Game

## ▶ Inter-related ISMS's will have overlap

- You & Vendor/Partner
- Across multiple vendors/partners

## ▶ Common Overlaps

- Risk Assessment
- Incident Response
- Security Awareness & Training
- Managing 3<sup>rd</sup> Party Relationships



# Define What You Expect



## ▶ **A.6.2 External Parties**

- *Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.*
  - A.6.2.1 Identification of Risks Related to External Parties
  - A.6.2.2 Addressing Security When Dealing with Vendors/Customers/Partners
  - A.6.2.3 Addressing Security in Third Party Agreements
- ▶ Defining used to be hard ... but it's gotten much easier ...

# Define: “Old School” vs. “New School”

## Old School:

\$1B+ eCommerce Refresh

- Custom Security Standard
- Defined 100+ Controls
- Many man-months of effort
- Potential Vendors resisted RFP response
- Ongoing maintenance effort is notable (refine controls)
- Prohibitively expensive
- Project is stalled

## New School:

Major City eCommerce Refresh

- Leveraged 27001, OWASP
- Defined 15 Risks/Monitoring
- Several man-weeks of effort
- Vendor immediately embraced model
- Ongoing maintenance effort is minimal (refine risks)
- Relatively inexpensive
- Project is gaining momentum



# Validate What You Get

















































## ▶ A.10.2 Third Party Service Delivery Management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

- A.10.2.1 Service Delivery Control
- A.10.2.2 Monitoring & Review of Third Party Services
- A.10.2.3 Managing Changes to Third Party Services

## ▶ Validating can be challenging if risk/compliance is high

- What form of testing is most suitable for the risks defined? (Design, Compliance, Substantiative)
- What form of assurance/attestation is best? (us, them, third party, certification)
- What direct access/testing is required for incident response/monitoring?
- What reporting and SLA's (think beyond Availability) do we need to monitor?

VENDOR OPTION*	VENDOR COST	LEVEL OF ASSURANCE	INDUSTRY ACCEPTANCE	VENDOR RESOURCES	TIME TO PERFORM	TYPE OF TESTING
VULNERABILITY ASSESSMENT			Acceptable but Penetration Test more commonly used			<b>Compliance</b> - Proves the "net" solution is not vulnerable
PENETRATION TEST			Widely accepted as validation of overall security level. Can be used independently or in concert with design/compliance tests to provide much higher levels of assurance			<b>Substantive</b> - Proves the "net" solution cannot be impacted by a malicious individual
SECURITY ROADMAP			Widely used to help a vendor reach a much more stringent set of security requirements to demonstrate compliance			<b>Design</b> - Likely only acceptable when coupled with a substantive form of proof as well
SECURE DATA FLOW DIAGRAM			Excellent mechanisms to succinctly demonstrate security. Generally paired with other forms of assurance or where more formal documentation of controls are not available.			<b>Design</b> - Proves that the design of the environment is reasonable and appropriate
SYSTEM SECURITY PLAN or InfoSec Policy Doc			Widely accepted - many firms request this information in the form of control questionnaires			<b>Design</b> - High level of assurance that the design of the environment is reasonable & appropriate
DESIGN REVIEW Network, Application, Solution, SDLC, Incident Response			Low to High (dependent upon the vendor and ability of critical risks to be mitigated by a small set of controls)			<b>Design</b> - High level of assurance that solution element reviewed will mitigate specific risks to acceptable level
GAP ASSESSMENTS against Client, Regulatory or Best Practices Standards			Moderate to high level of acceptance dependent upon the extent/rigor of the assessment, the "relevance" of the standard chosen, and the independence of the entity conducting the assessment.			<b>Design</b> - High level of assurance that the design of the controls achieve the reference standards
BITS SHARED ASSESSMENT			Widely used/highly regarded in the financial sector. See Gap Assessments. This is an ISO 27002 based standard.			<b>Design</b> - Assurance that design of environment is consistent with Shared assessment (essentially ISO 27002)
ISO 27002 GAP ASSESSMENT			Internationally recognized as the leading information security "standard" for more than a decade (formerly ISO 17799).			<b>Design &amp; Compliance</b> - Assurance that design of environment is consistent with industry best practice (ISO 27002)
ISO 27002 COMPLIANCE ASSESSMENT			Validates both the design and operation of 27002 controls providing a very high level of assurance			<b>Design &amp; Compliance</b> - Assurance that the controls are in place and operating as intended.
SAS-70			Validates that the documented controls are in place and operating as intended as well as providing some assurance of the design.			<b>Compliance</b> - Assurance that the controls are in place and operating as intended.
ISO 27001 CERTIFICATION			Internationally recognized certification of the design/operation of the technical controls (27002) AND the Information Security Management System that governs them.			<b>Design &amp; Compliance</b> - Internationally recognized certification that design & operation of environment are secure.

# High Level Process

- ▶ Integrate InfoSec into your existing Vendor/Risk Management Program
  - You likely have one that measures “business risk” (financials, insurance)
- ▶ Conduct a “Risk Assessment”
- ▶ Define your compliance/security requirements
  - Preferably leveraging a risk and standards based approach
- ▶ Define the monitoring, attestation, and SLAs needed to govern the relationship and assure risk is mitigated to an acceptable level
- ▶ Use security incidents coupled with monitoring to improve internal and external processes



# Define, Monitor, Improve.

**You can't outsource your responsibility/liability/ISMS**



+



=

