

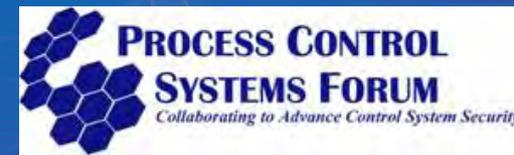
# Assessing Security Policies and Procedures

## Featuring Process Control IT Incident Management

[www.ins.com](http://www.ins.com)



**Chris Sandford**  
**Principal Consultant**  
**International Network Services**  
**Chris.Sandford@ins.com**



# Agenda

- ❖ Introduction
- ❖ IT Governance
- ❖ NSA
- ❖ Incident Management
- ❖ TrustCheck



# Agenda

- ❖ Introduction
- ❖ IT Governance
- ❖ NSA
- ❖ Incident Management
- ❖ TrustCheck

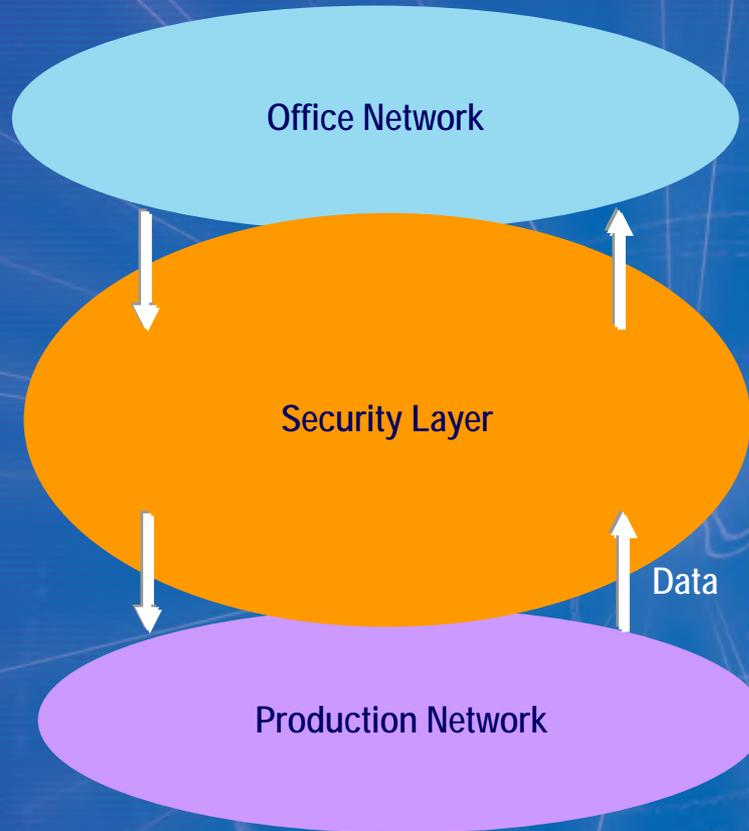


# Industry Security Drivers

- ❖ **Increased focus on information security**
- ❖ **Failures in technology to protect information**
- ❖ **Proliferation of standards, regulations and legislation**
- ❖ **Threat of legal liability**
- ❖ **Business partners and stakeholders demanding security**

# Introduction

IT Governance  
Standard Infrastructure  
Security Policy & Standards  
IT Incident Management



Production Governance  
HSE Governance  
Production Incident Management  
Strict Policy & Procedures

# Agenda

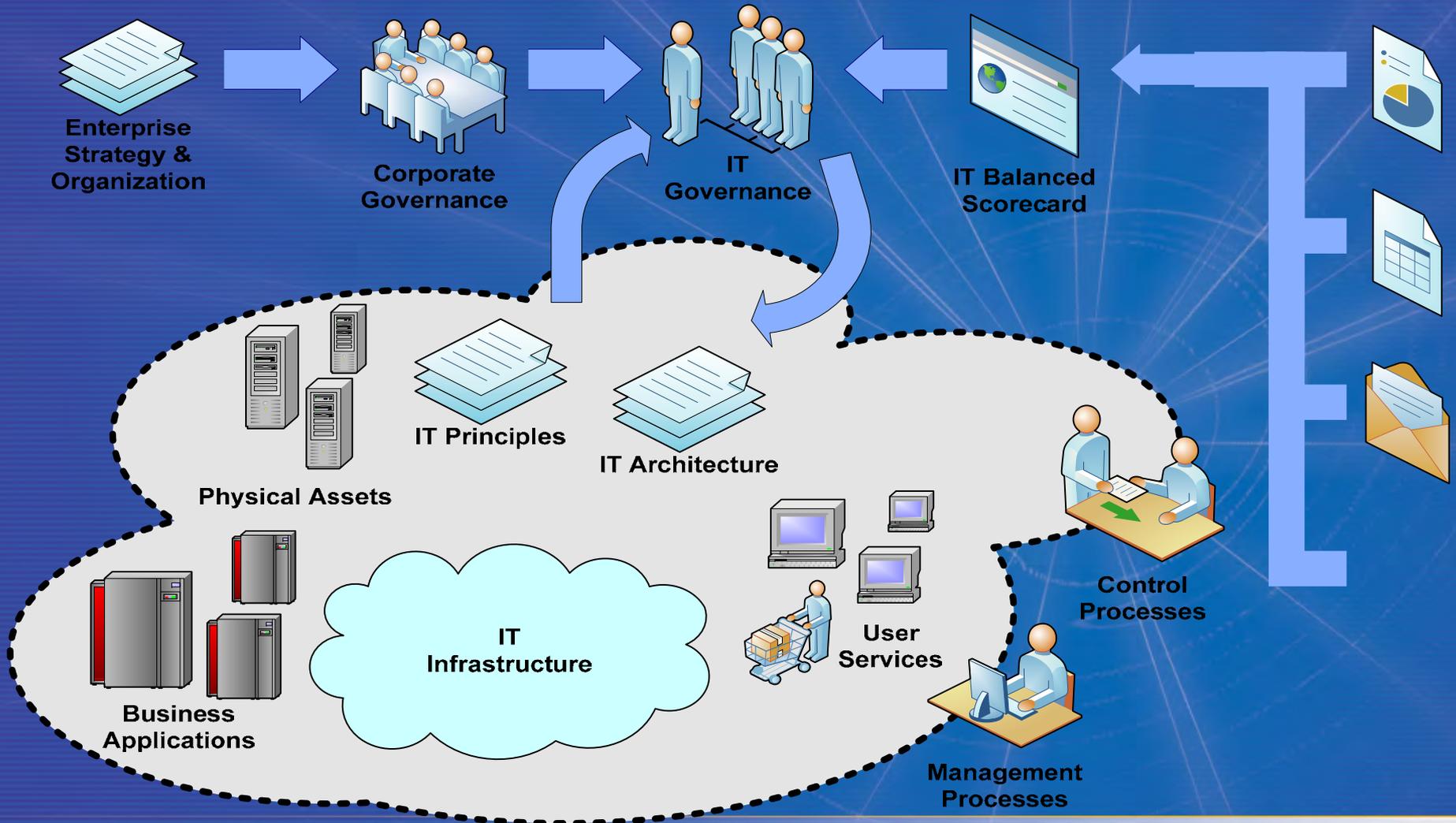
- ❖ Introduction
- ❖ IT Governance
- ❖ NSA
- ❖ Incident Management
- ❖ TrustCheck



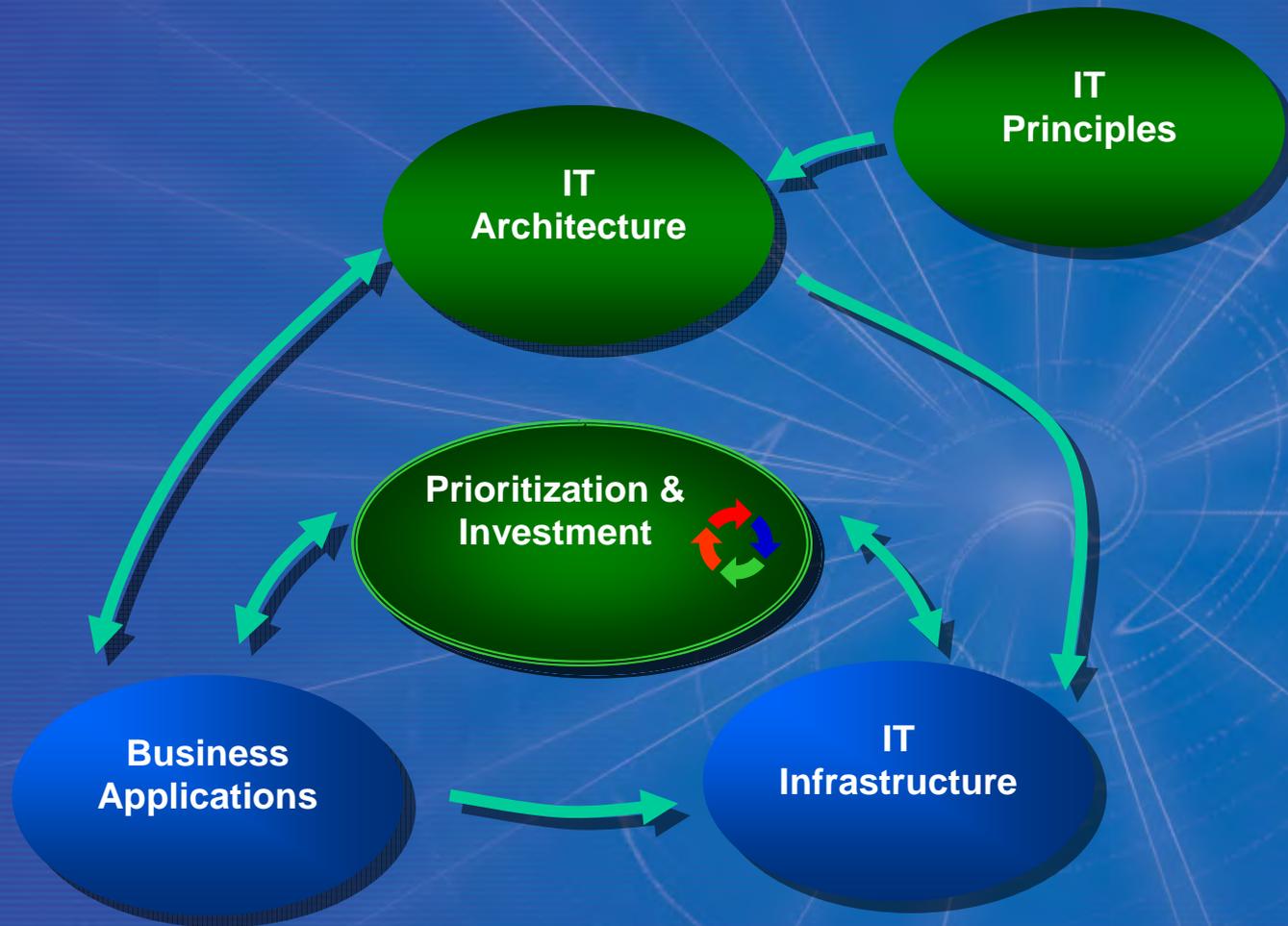
# What is IT Governance?

- ❖ **The process of identifying what IT should do in terms of:**
  - *New initiatives( e.g. new/amended services or applications)*
  - *Improving/maintaining current performance (e.g. improving security, increasing capacity or improving resilience)*
- ❖ **Allocating resources (primarily money and staff time, but also assets and facilities) to achieve the selected goals**
- ❖ **Comprises of 5 areas**
  - *Business value delivered by IT*
  - *Alignment between IT and business strategy*
  - *Effective risk management*
  - *Resource Management*
  - *Performance Measurement*

# IT Governance in Context



# Scope of IT Governance



# Governance in Process Control Security

- ❖ **Aligning security to the business requirements**
- ❖ **Managing a common security infrastructure and process (where possible)**
- ❖ **Ensuring alignment throughout the business**
- ❖ **Ensuring conformity for new projects**
- ❖ **Common procurement methodology**

# IT Governance in Process Control Security

- ❖ **Standardising on security, it becomes easier to prevent & manage security incidents**
- ❖ **By having governance, its easier to standardise**
- ❖ **Standardising on security policies and infrastructure will enable the organisation to react quicker and smarter**

# Agenda

- ❖ Introduction
- ❖ IT Governance
- ❖ **NSA**
- ❖ Incident Management
- ❖ TrustCheck



# NSA Overview

- ❖ NSA established the INFOSEC Assurance Training and Rating Program (IATRP) to support the security of public and private industries
- ❖ IATRP sets the standards for INFOSEC Assurance services via the INFOSEC assurance methodologies
- ❖ IATRP certifies organizations in the methodologies, and rates them via the standard metric INFOSEC Assurance Capability Maturity Model (IA-CMM)
- ❖ NSA provides this information to private and public consumers so they are better informed when selecting security service providers

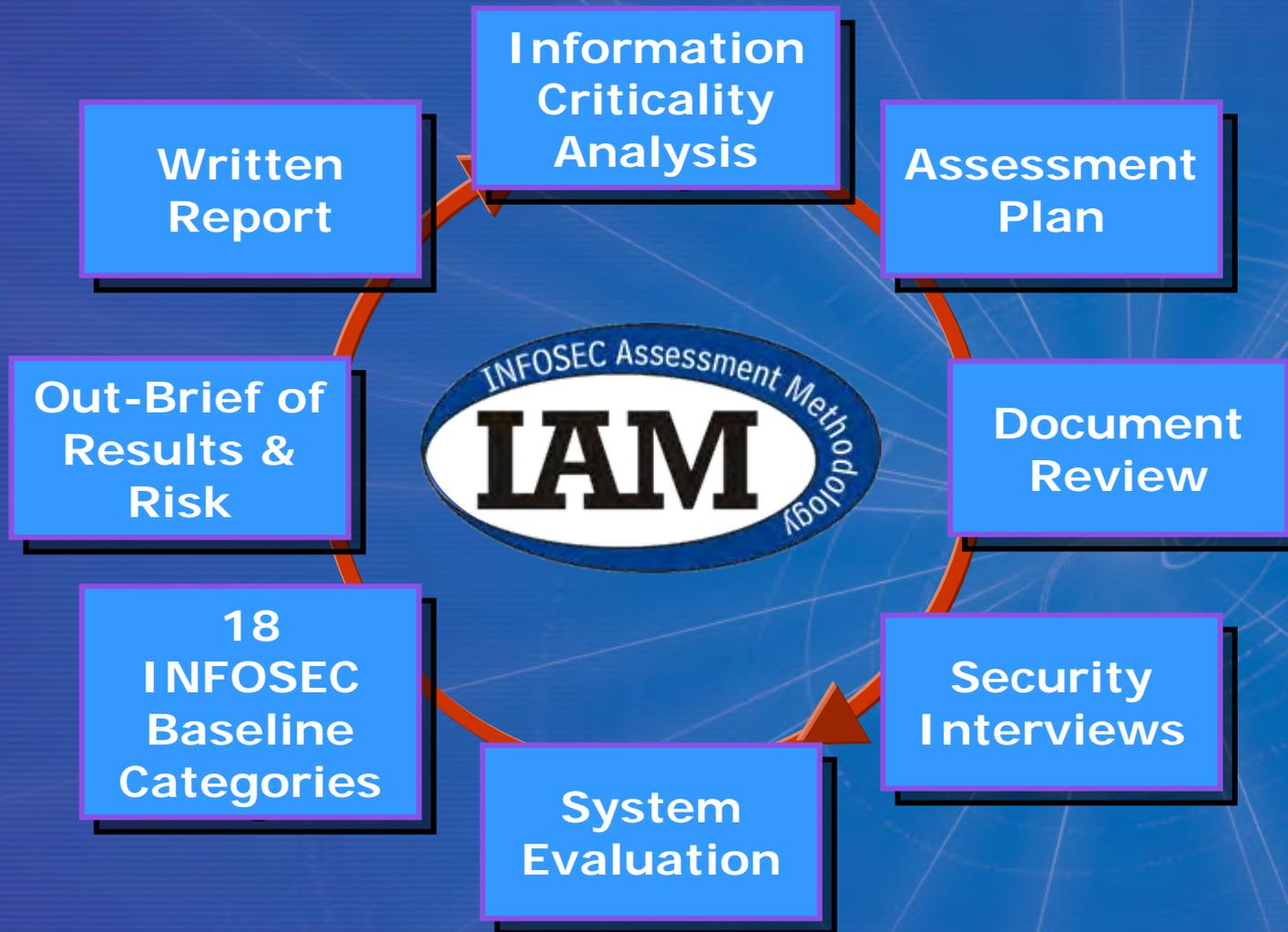
# NSA Overview

- ❖ **Developed through a collaboration between the NSA, DoD, and NIST**
- ❖ **Obtaining clear visibility into the state of security and risk is critical for sound decision making**
- ❖ **Security assessment strategies that start with information protection, end with high-valued, pragmatic security solutions that are focused on business risk**
- ❖ **Assessments must be performed according to a prescriptive, repeatable, and proven method to ensure effectiveness of results and sound remediation**

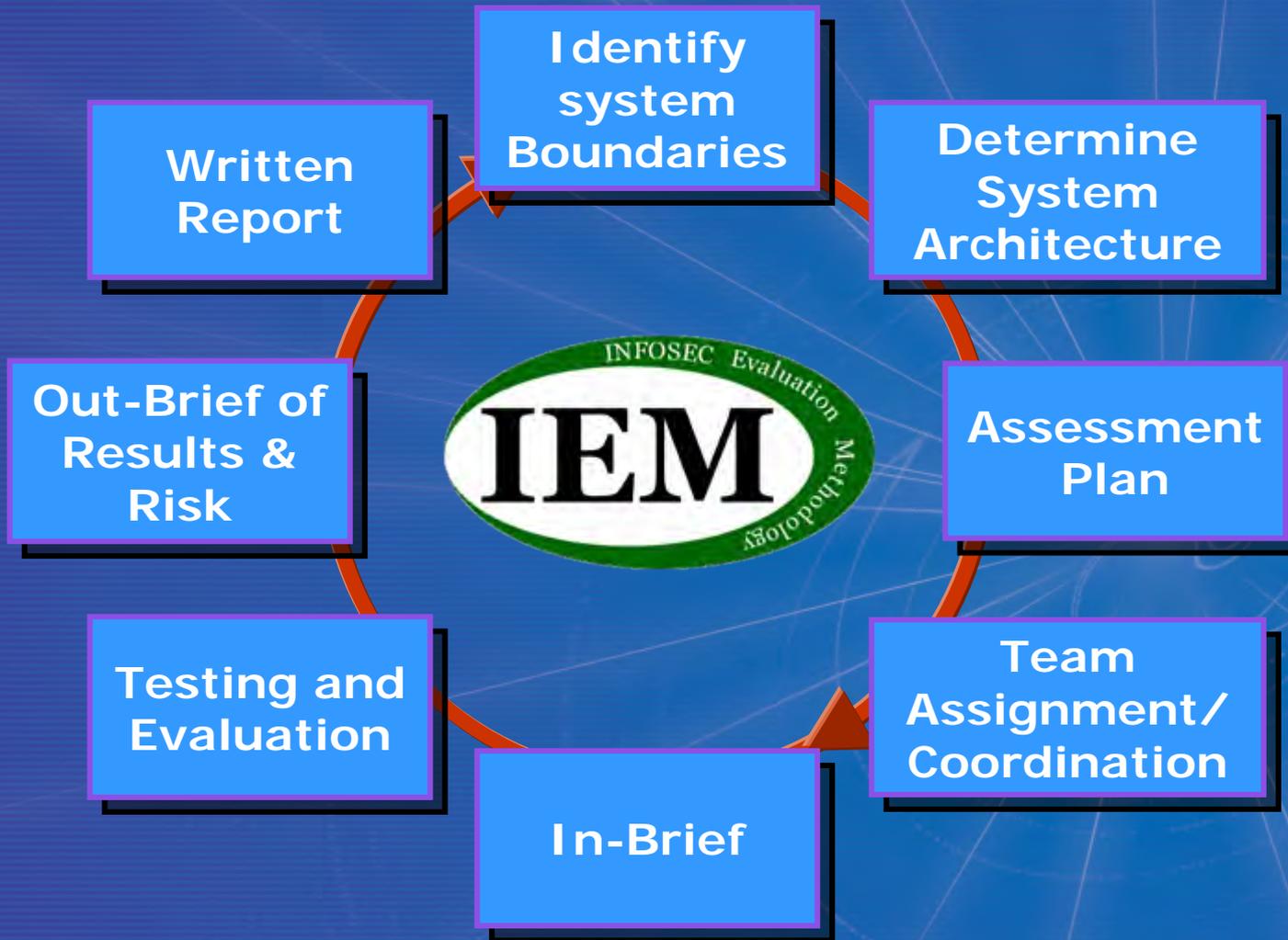
# The Methodologies

- ❖ **Defines a detailed prescription of activities, processes, and procedures for performing security assessments**
  
- ❖ **INFOSEC Assessment Methodology (IAM)**
  - ❑ *An analysis based on the protection of key information assets*
  - ❑ *Defines criticality, value, and impact to information systems*
  - ❑ *Articulates risk based on business needs and requirements*
  
- ❖ **INFOSEC Evaluation Methodology (IEM)**
  - ❑ *A technical vulnerability analysis*
  - ❑ *Focuses on key systems containing critical information*
  - ❑ *Presents the vulnerability risk to the organization*

# INFOSEC Assessment Activities



# INFOSEC Evaluation Activities



# IAM and IEM Criticality Alignment

INS Overall Vulnerability Criticality Matrix (OVCM) and INFOSEC Posture Rating (IPR)

IPR=		6.04		Critical Impacts →												
						H	H	H	M	M	M	L	L	L		
Vulnerability	CVE	Type (Technical, or Non-Technical Vul.)	Finding Number	Affected System	Computer Network Defense (CND)	Severity	Vulnerability Weight	EMR System	Customer Processing System	E-Mail System	E-Mail System	E-Commerce System	SCOT System	Facilities Management System	SCOT System	Telmetry System
Security Policy	NA	N	1	1	P	H	4.5	9.00	9.00	9.00	7.50	7.50	7.50	6.00	6.00	6.00
Patch Management	NA	N	2	1	P	H	4.5	9.00	9.00	9.00		7.50		6.00		6.00
SQL Injection	CVE-2006-3213	T	3	1	P	H	6	9.00		9.00	8.00	8.00	8.00	7.00	7.00	7.00
Security Organization	NA	N	4	2	D	H	4.5	9.00		9.00				6.00		
Database Security	CVE-2006-3311	T	5	2	D	H	6	9.00	9.00	9.00	8.00	8.00	8.00	7.00	7.00	7.00
Router Vulnerability	CVE-2006-1237	T	6	3	R	M	4	7.00	7.00	7.00	6.00	6.00	6.00	5.00	5.00	5.00
This is a vulnerability	CVE-2006-1138	T	7	2	S	M	4	7.00	7.00	7.00	6.00				5.00	5.00
This is a vulnerability	CVE-2005-1239	T	8	3	R	M	4	7.00	7.00	7.00	6.00	6.00			5.00	5.00
Security Change Control	NA	N	9	4	S	M	3		7.50	7.50	6.00	6.00	6.00	4.50	4.50	4.50
JAVA Vulnerability	CVE-2005-1222	T	10	3	P	M	4		7.00	7.00	6.00	6.00	6.00	5.00	5.00	5.00
Account Havesting	CVE-2006-1242	T	11	2	D	M	4	7.00		7.00	6.00	6.00	6.00	5.00	5.00	5.00
Cross-Site Scripting	CVE-2005-3243	T	12	4	D	L	2	5.00	5.00	5.00	4.00	4.00	4.00			3.00
Web Server	CVE-2005-2141	T	13	3	R	L	2	5.00	5.00	5.00	4.00	4.00	4.00	3.00	3.00	3.00
Partner Access Controls	NA	N	14	2	R	L	1.5	6.00	6.00	6.00	4.50	4.50	4.50	3.00	3.00	3.00
Winows 2003 Server	NA	N	15	1	S	L	1.5	6.00	6.00	6.00	4.50	4.50	4.50	3.00	3.00	3.00

## INFOSEC Posture Rating



# Agenda

- ❖ Introduction
- ❖ IT Governance
- ❖ NSA
- ❖ Incident Management
- ❖ TrustCheck



# Traditional Incident Management

## ❖ Information Security Incident Management (IS-IM)

- ❑ *Focus on reducing impact, then restoring systems*
- ❑ *Data for forensics available*
- ❑ *Processes & procedures detailing actions*
- ❑ *After Incident review boards*

## ❖ Production Incident Management

- ❑ *Focus on reducing impact, then restoring production*
- ❑ *Limited data for forensics*
- ❑ *Detailed process for restoring production*
- ❑ *Limited review boards if production or HSE not affected*

# New Challenges

- ❖ **Some infrastructure overlaid (VPN/tunnel)**
- ❖ **Optimisation systems in non-production network**
- ❖ **Production infrastructure centrally managed**
- ❖ **Standardised IT infrastructure**
- ❖ **Remote maintenance support through office network**
- ❖ **More users requiring access to production data**
- ❖ **Security layer bordering the domains**
- ❖ **Availability of Internet patch / software downloads**

**These can create more security incidents  
and require a quicker response time**

# Detecting & Identifying a Security Incident

- ❖ Application failures, caused by jitter from a DOS
- ❖ 3<sup>rd</sup> party accessing without change authorisation
- ❖ CPU load on HMI very high, virus or normal activity?
- ❖ Vendor using an uncertified laptop
- ❖ A modem/WLAN appearing in the facility

**Security training required to help incident identification**

# Integrating IS-IM - Best Practices

- ❖ Risk detection, identification & notification plan
- ❖ Use a site contact desk for incident notification
- ❖ Have a place to report vulnerabilities
- ❖ Create an IS-IM governance model
- ❖ Integrated Change Management
- ❖ Ensure that the Backup & Restore Plan works
- ❖ Create business contingency plans
- ❖ Ensure the staff are aware and trained on IS
  
- ❖ Ensure the IS-IM plan is integrated within or alongside existing production and HSE plan

# Integrating IS-IM – Response Team

- ❖ Create the IM team from production and IT
- ❖ Have one person accountable for investigation
- ❖ Ensure roles are defined
- ❖ Ensure tools are available and people are trained
- ❖ Ensure incident data is gathered during the incident
- ❖ Practice using the plan
- ❖ Ensure there is an escalation procedure
- ❖ Complete an after incident review, and implement learning's

# Agenda

- ❖ Introduction
- ❖ IT Governance
- ❖ NSA
- ❖ Incident Management
- ❖ TrustCheck



# Why Assess your People & Processes

- ❖ Able to identify security slippages
- ❖ Able to recognise best practices and implement
- ❖ Able to show trends and comparisons
- ❖ Gives high-level reporting

Check out Scysag for more tools and information

[www.pcsforum.org/groups/68/library](http://www.pcsforum.org/groups/68/library)

# Part of the Security Lifecycle



TrustCheck

# Trustcheck

## ❖ Standards and Regulations

- ❑ *Assessment of controls defined by industry standards and regulations (ISO17799:2000&2005, HIPAA, & SOX)*
- ❑ *Assessment of controls per Customer-defined modules*

## ❖ New modules can be created for new standards

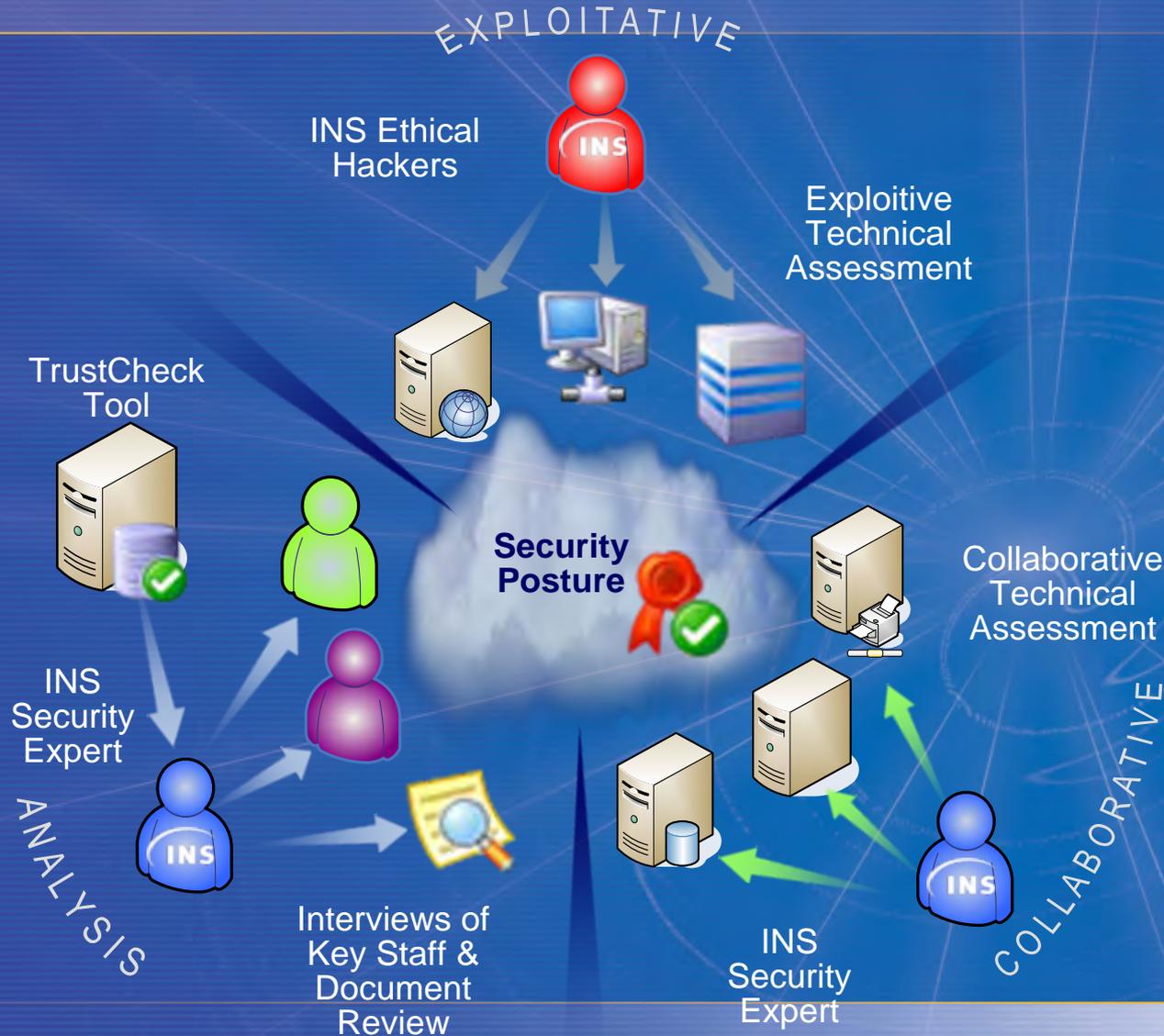
- ❑ *E.g. SP99, IEC-62443*

## ❖ Focus on people & processes

## ❖ Shows the strengths and weakness of your security

## ❖ Able to show improvements over time

# Part of the Security Lifecycle



# Addressing Challenges With TrustCheck



Clearly visualize the current status of compliance efforts



Prioritize investments and monitor positive impacts of remediation over time

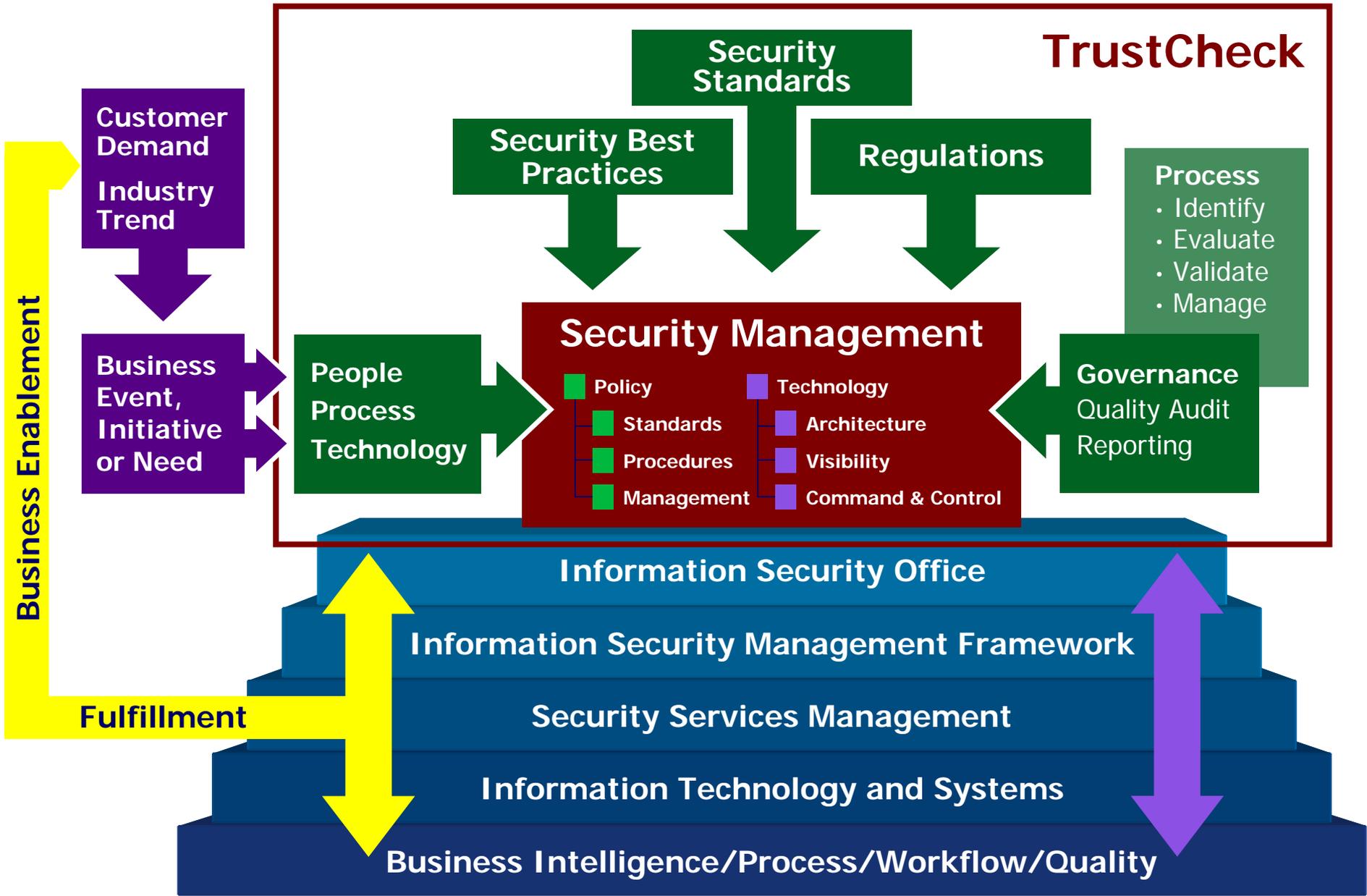


Quickly ascertain strengths and utilize resources to address areas for improvement



Customize the assessment process to your specific needs, expectations, and policies

# Security Program Capability



# TrustCheck's Metric Strategy Foundation

## ❖ System Security Engineering Maturity Model (SSE-CMM)

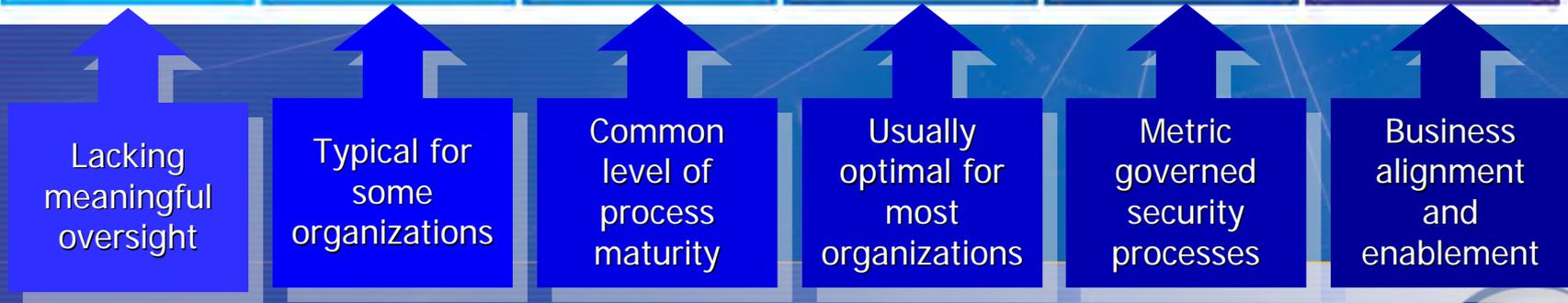
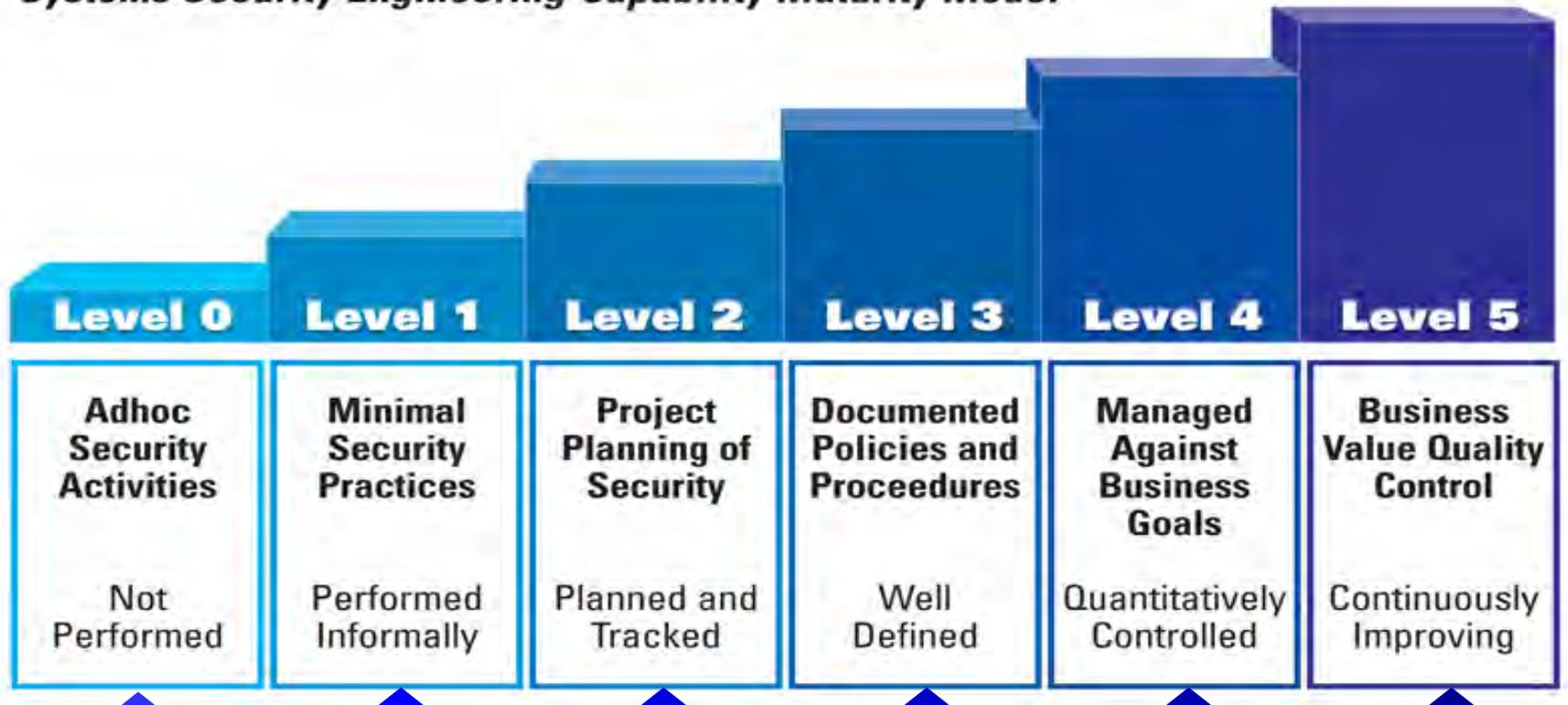
- *Process measurement and improvement framework*

## ❖ Modular framework

- *Precisely organized structure of assessment modules defining domains, elements, and sub-elements*
- *Questions/statements, evidence collection, review guidance, and maturity metrics*

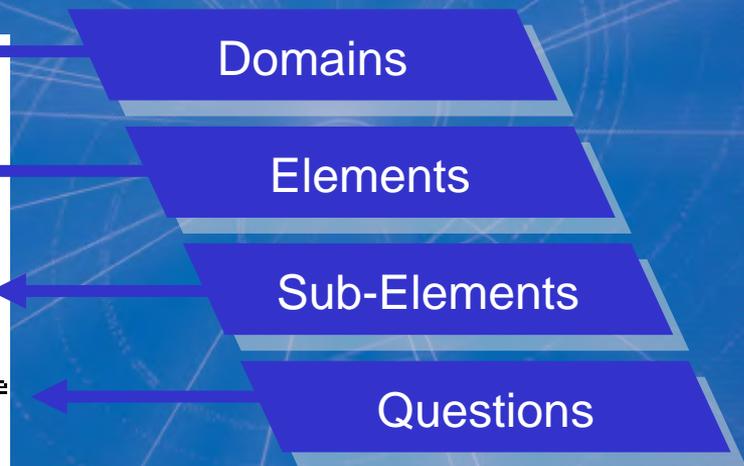
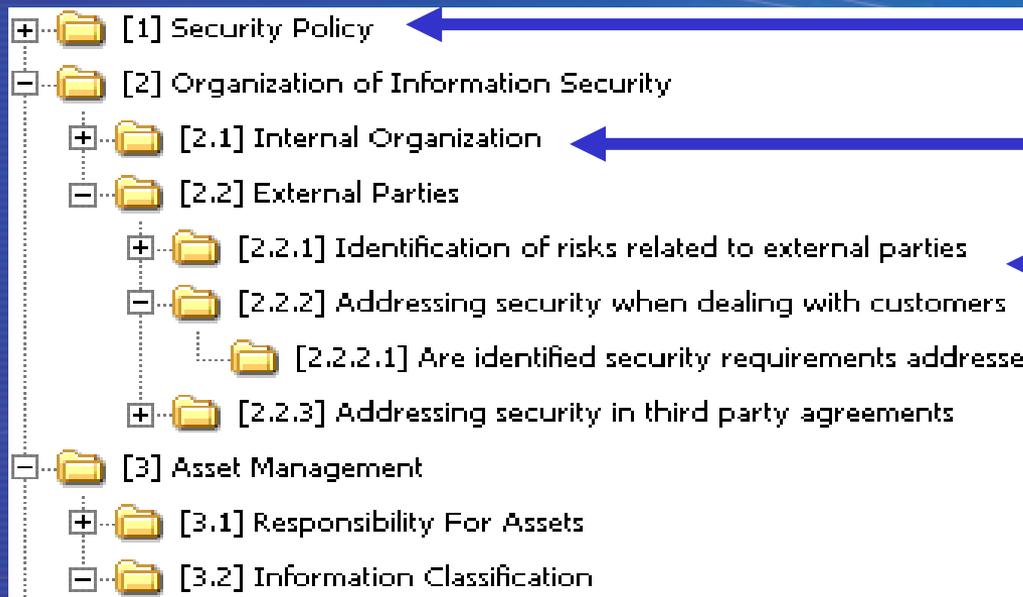
# Measuring the Maturity of Security

*Systems Security Engineering Capability Maturity Model*



# Module Integrity

- ❖ Domains organize control objectives
- ❖ Elements focus on key process areas
- ❖ Sub-Elements contain investigative points specific to a control
- ❖ Fully customizable



# Performing an Assessment

TrustCheck

Copyright © 2005  
International Network Services Inc.  
All Rights Reserved.  
Version 0.65

User: Jim Tiller  
Role: Administrator

Announcements

Assessments

Client Management

Modules

About

Logoff

## Assessment Center

Abc, Inc. -> Human Resources -> HR Assessment - [11/7/2005]

The screenshot shows the TrustCheck assessment interface. On the left, a tree view shows the client structure: Abc, Inc. > Human Resources > HR Assessment - [11/7/2005] > North America. The main area displays the assessment structure for "Assessment 'HR Assessment'", including sections for Security Policy, Organization of Information Security, and Asset Management. A callout box labeled "Standard, Regulation, or Policy" points to the "Asset Management" section. Another callout box labeled "Module Management" points to the "Modules" menu item in the top navigation bar. Below the assessment structure, a "Statistics - [3.2.1]" panel shows metrics for questions, answers, and scores. A callout box labeled "Assessment Statistics" points to this panel. The main content area shows a question: "Is information classified in terms of its value, legal requirements, sensitivity, and criticality to the organization?". Below the question is a response scale from 0 to 5, with 2 selected. A callout box labeled "Evidence and CMM Matrix" points to the question text. Below the response scale is a table of "Existing Notes". A callout box labeled "Multiple entries and notes" points to this table. The table has columns for Note, Type, Date, Author, and Publish. Two notes are listed, both dated 11/8/2005 and authored by Jim Tiller. The first note is about information security co-ordination, and the second is about management definitions. Below the table is a "New Note" form with a text area and a "Note Type" dropdown set to "Point of Interest". A checkbox "This Note is Publishable" is checked. A callout box labeled "Assessment Management" points to the "HR Assessment" folder in the tree view.

Note	Type	Date	Author	Publish
Information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel and specialist skills.	Strength	11/8/2005	Jim Tiller	Yes
Depending on the size of the organization, management can be defined as one individual, a dedicated management forum, or even the board of directors.	Point of Interest	11/8/2005	Jim Tiller	Yes

# Evidence and CMM Matrix Guidance

## ❖ Each investigative point contains unique information:

- ❑ *Guidance on what evidence to collect in order to validate the control, processes, and activities*
- ❑ *Definition of the required attributes that must exist to achieve a specific SSE-CMM score*

Question:

Are identified security requirements addressed before giving customers access to the organization's information or assets?

Additional Information:



Response:

N/A  0  1  2  3  4  5

CMM Score



Provides access to specific information to support the scoring of the question according to the SSE-CMM

Provides access to information guiding the user in the collection of documents and processes for review to answer the question

# Comprehensive Reporting

## TrustCheck

Copyright © 2005  
International Network Services Inc.  
All Rights Reserved.  
Version 0.65

User: Jim Tiller  
Role: Administrator

Announcements

Assessments

Client Management

Modules

About

Logoff

### Assessment Charts

Abc, Inc. -> Human Resources -> HR Assessment - [11/7/2005]

#### Client(s)

- Abc, Inc.
  - Human Resources
    - HR Assessment - [11/7/2005]
    - North America

#### Assessment Charts

If you would like to change details of the graphs click the icon 

Select the number of Comparisons you would like to make.

Your Assessment

HR Assessment - [11/7/2005]

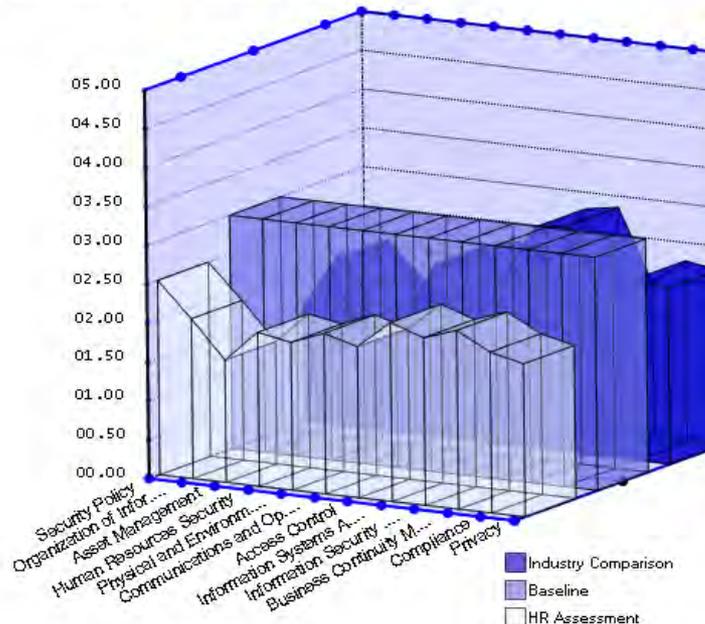
First Comparison

Baseline

Second Comparison

Industry Comparison

HR Assessment overall score is: 2.07



Copyright © 2005  
International Network Services Inc.  
All Rights Reserved.  
Version 0.65

User: Jim Tiller  
Role: Administrator

### System Security Engineering Comparability Maturity Model

0 Not Performed    1 Performed Informally    2 Planned & Tracked    3 Well Defined    4 Quantitative Controlled

Base practices performed	Committing to perform Planning performance Disciplined performance Tracking performance Verifying performance	Defining a standard process Tailoring standard process Using data Perform a defined process	Establishing measurable quality goals Determining process capability to achieve goals Objectively manage performance
--------------------------	---	--	--

# Comprehensive Reporting

- ❖ Provides visual representation of the level of maturity of security governance
- ❖ Identifies strengths within the security program as well s areas for improvement
- ❖ Offers a unique perspective on systemic issues where focused efforts may have broad, positive, cost-effective impacts

# The Real Power of TrustCheck

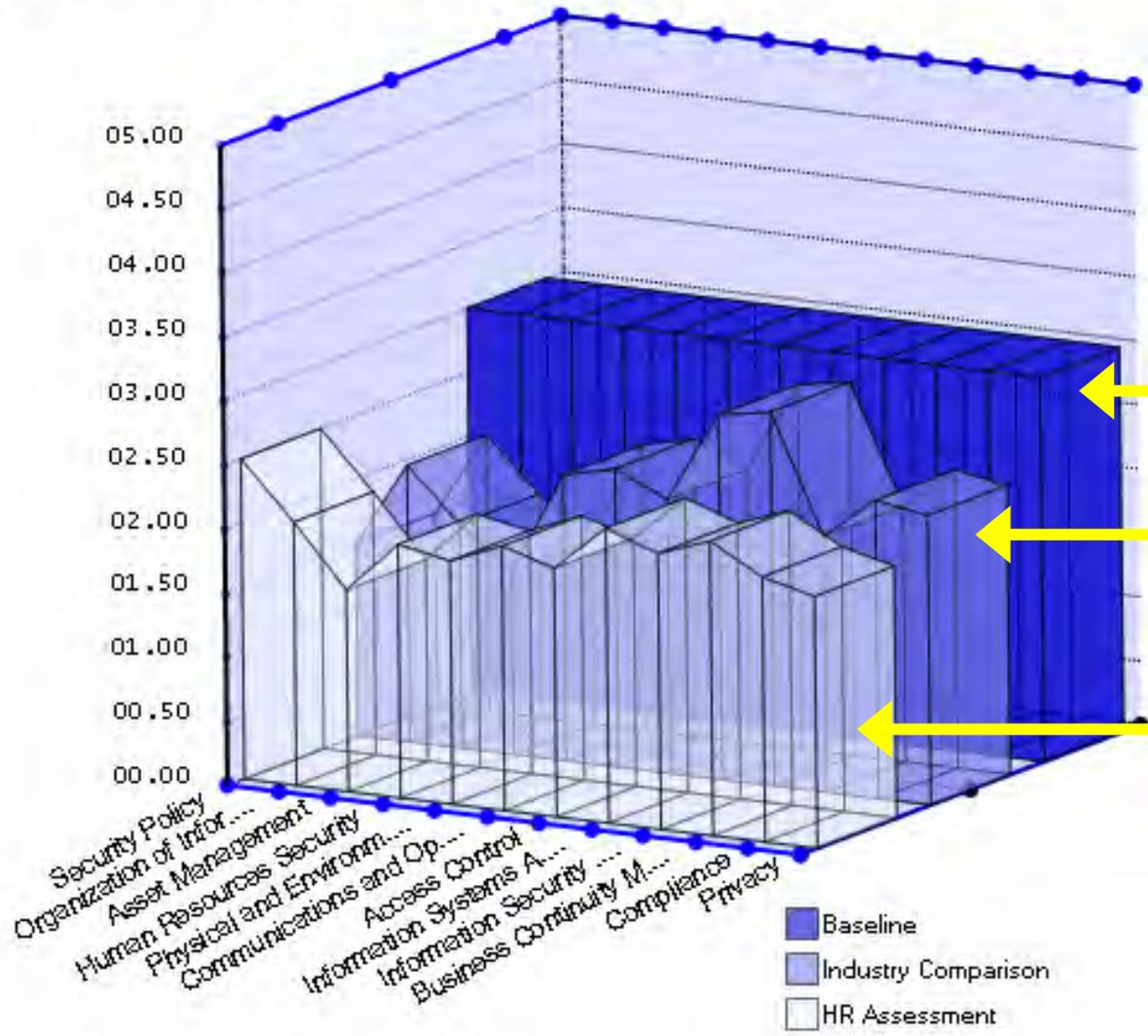
## ❖ Comparisons

### ❖ You can compare a customer's assessment to:

- ❑ *Other assessments they have performed*
- ❑ *Combinations of compiled assessments from INS's TrustCheck database*
- ❑ *Established expectations*

HR Assessment overall score is: 2.07

# Overall Chart

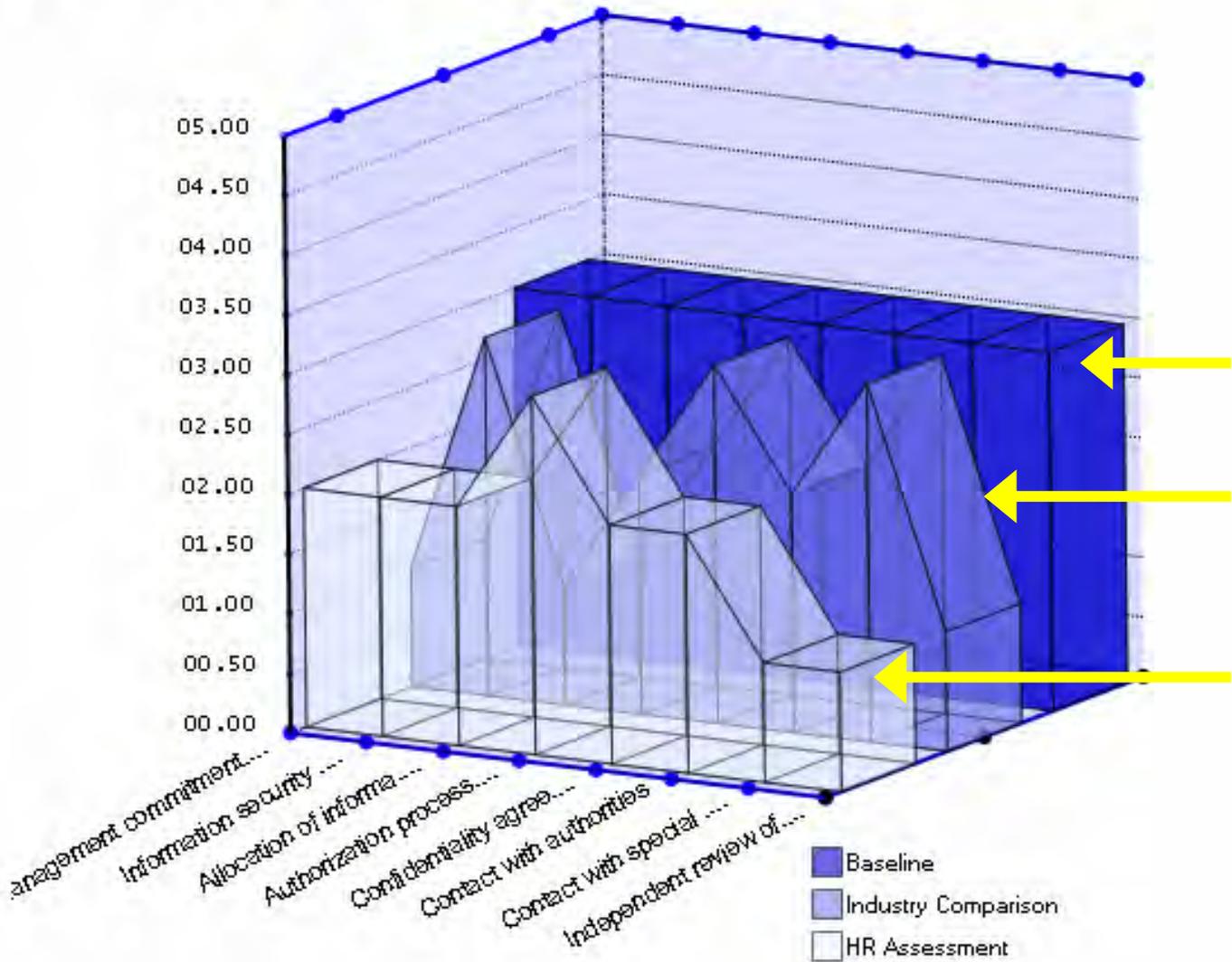


Customizable baseline or stated objective

Industry baseline, previous assessment, or custom

Assessment results per domain

# A Deeper Look



Baseline for this Element

Industry average for this Element

Assessment results for the Element

- Baseline
- Industry Comparison
- HR Assessment

# Summary

- ❖ **Technology is not always the answer and can be the problem**
- ❖ **Ensure that the business drives IT for its needs**
- ❖ **COTS products are getting lower into control networks**
- ❖ **Ensure your production and IT staff are trained**
- ❖ **Have an incident management plan and team**
- ❖ **Monitoring your security posture over time will help improve your security**

# INS Security History



**Thank You**

**Questions?**

**[Chris.Sandford@ins.com](mailto:Chris.Sandford@ins.com)**



# INS in the Industry

