Compliance: How to Manage (Lame) Audit Recommendations

Brian V. Cummings
Tata Consultancy Services Ltd
brian.cummings@tcs.com

Tuesday, August 9, 2011 1:30 p.m.

Session 9221

Security & Compliance Risk Landscape

Presentation addresses the management of Audit recommendations from the perspective of the CISO

Hacking, Phishing, Social Engineering

Sophisticated, automated, stealthy

International and Inter-Enterprise Information Theft

"Information warfare " and competition is real and not confined to critical infrastructure.

Internal Fraud and Abuse

Still acknowledged as the most prevalent and serious threat.

CyberX Activities

X = Crime, Terrorism, Warfare

Sophisticated, automated, and stealthy by organized crime, ad hoc criminals, corporate enterprises, and international intelligence agencies with varying motivations, but all employing highly skilled hackers.

Legal and regulatory action

Privacy laws, regulations, sanctions, and penalties can jeopardize enterprise viability

Employees

"Loose lips" and careless security behaviors

Security & Compliance Risk Landscape

Hacking, Phishing, Social Engineering
Sophisticated, automated, stealthy

"Information warfare " and competition is real and not confined to critical infrastructure.

International and Inter-Enterprise Information Theft

Internal Fraud and Abuse
Still acknowledged as the most prevalent and serious threat.

Sophisticated, automated, and stealthy by organized crime, ad hoc criminals, corporate enterprises, and international intelligence agencies with varying motivations, but all employing highly skilled hackers.

CyberX Activities
X = Crime, Terrorism, Warfare

Legal and regulatory action
Privacy laws, regulations, sanctions, and penalties can jeopardize enterprise viability

Employees
"Loose lips" and careless security behaviors

Auditors
Irrelevant, time-diluting recommendations

What do you do? What can you do?

If everyone in an entity is not pulling in the same direction, then you won't get to where you need to be as fast as you need to be there.

Business Alignment

Good Information Security Practices

ISMS Certification

Protection, Enablement, Compliance, Productivity

What do you do? What can you do?

If everyone in an entity is not pulling in the same direction, then you won't get to where you need to be as fast as you need to be there.

Audit Comment to CISO:

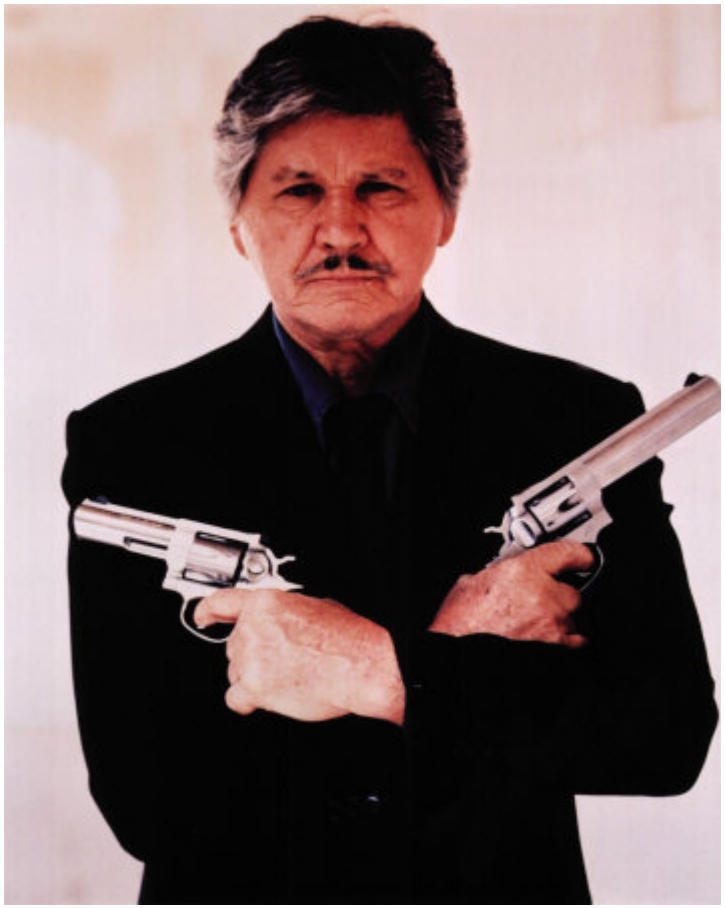
Make sure that all Ethernet ports are disabled if they are not in use to avoid unauthorized intrusion from the Intranet.

Beleaguered CISO

What is wrong with that Audit Recommedation?

- Is it addressed to the person who has the authority to do something about it?
- Is it addressed to the person who can implement and operationalize it?
- What is the real risk relative to other risks the entity may face?
- Is it consistent with the security objectives of the entity and the current plan and budget?
- Is it feasible (solutions, budget, resources)?

What about your Auditor?



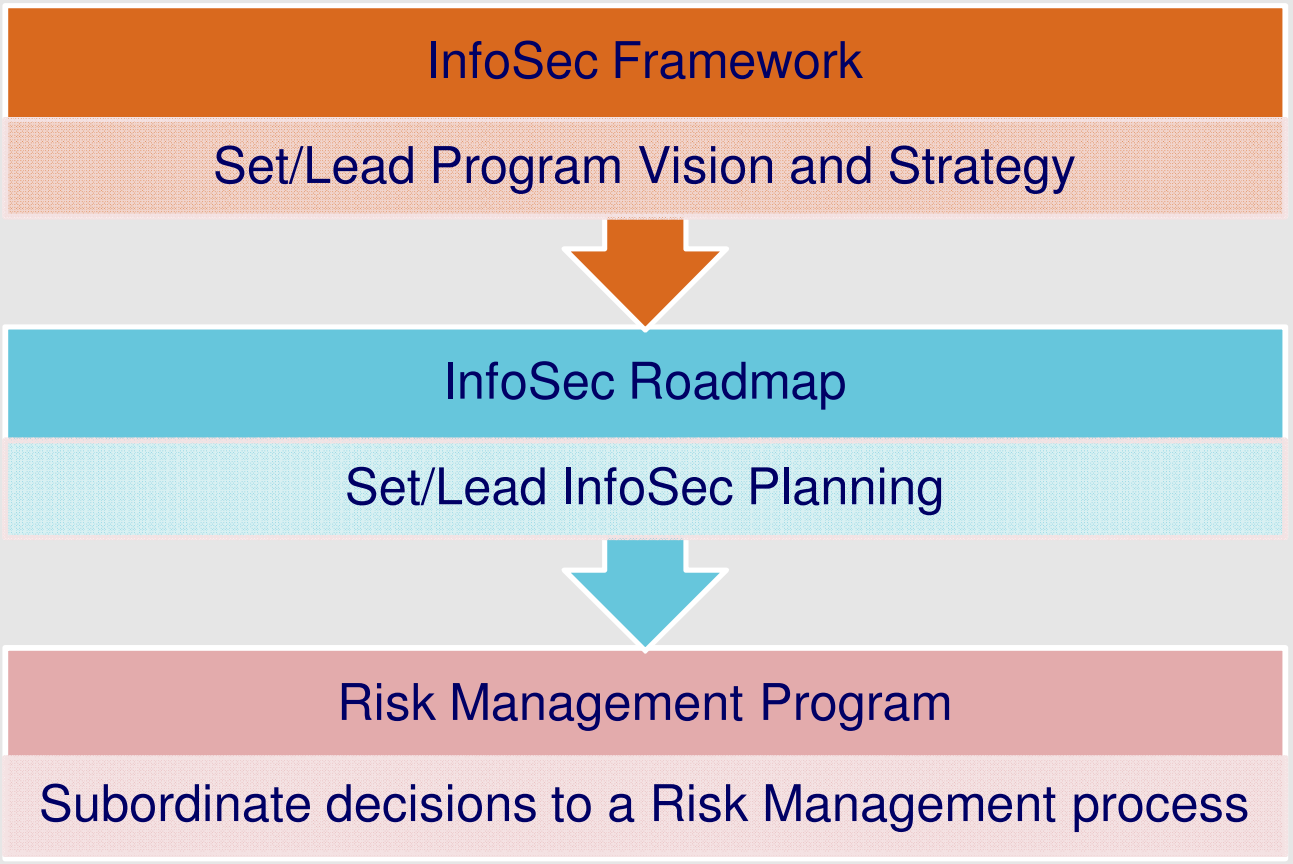
What about your Auditor?

- Is your auditor a bully?
- Is your auditor knowledgeable?
- Is your auditor on the right page?
- What is your organization's attitude toward audit recommendations?

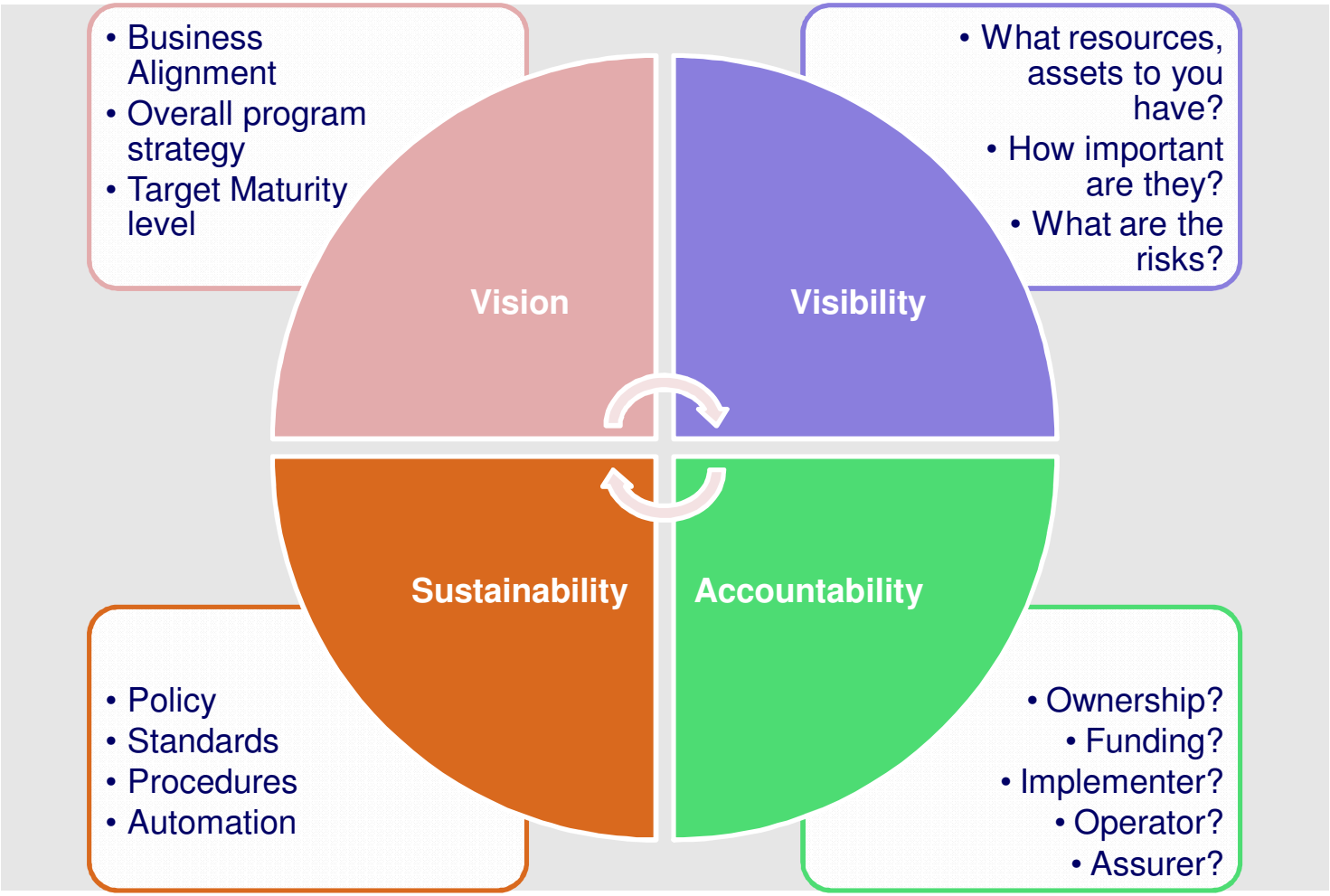
How to manage (all of) your auditors

Take charge and leverage the things you should be doing anyway to help manage your auditors

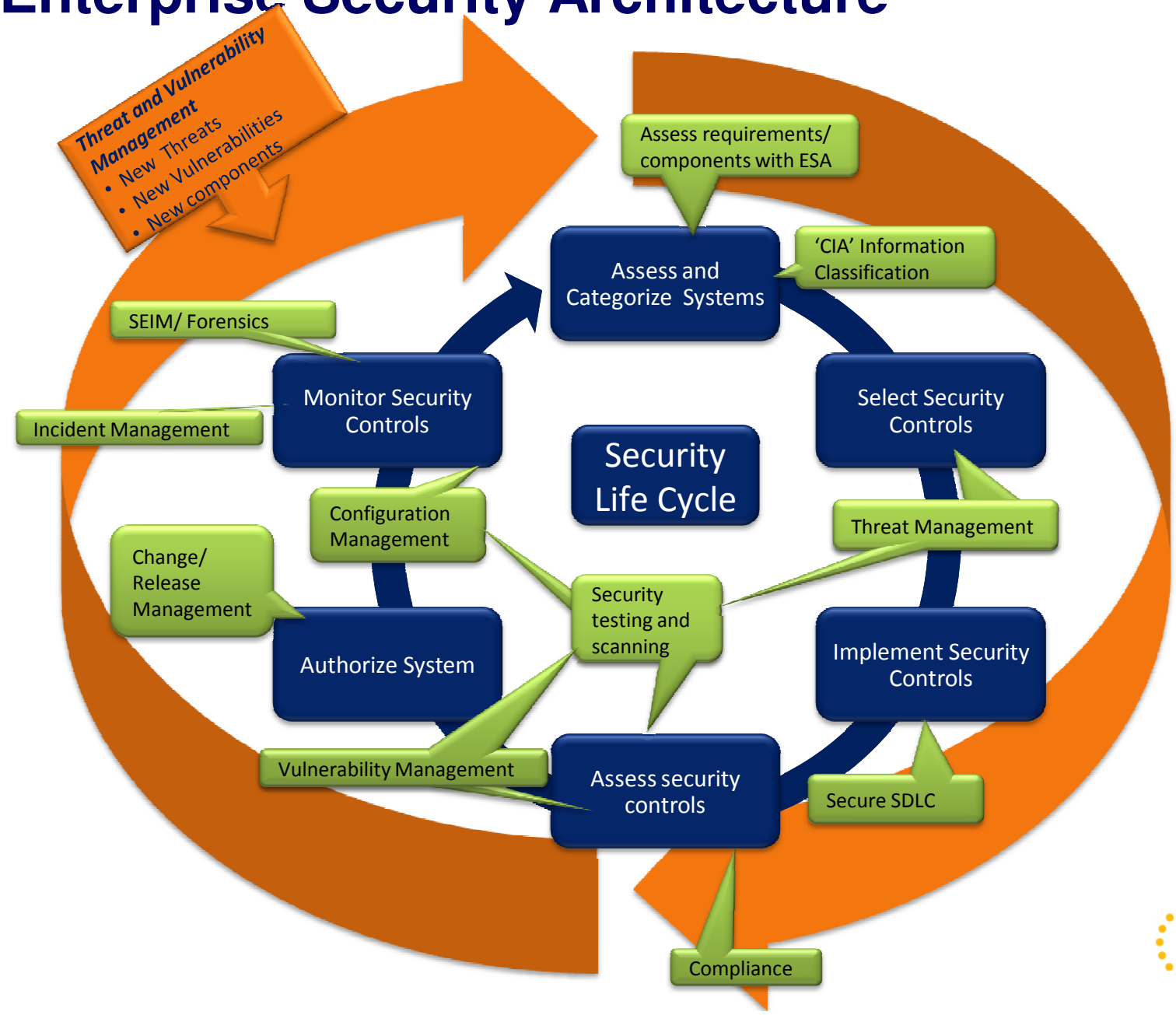
How to manage (all of) your auditors



Information Security Framework



Enterprise Security Architecture



InfoSec Roadmap - Strategic

Program Domain	2011	2012	2013	2014	2015
Governance					
Compliance					
Networks					
Servers					
Desk Top					
Applications					
Data/Database					
SIEM					
Insider Threat					
Physical & Environmental					

Multi-Year Planned Milestones

InfoSec Roadmap - Strategic

	2011				2012				2013				2014		2015
Program Domain	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	H1	H2	Year
Governance															
Compliance															
Networks															
Servers															
Desk Top															
Applications															
Data/Database															
SIEM															
Insider Threat															
Physical & Environmental															

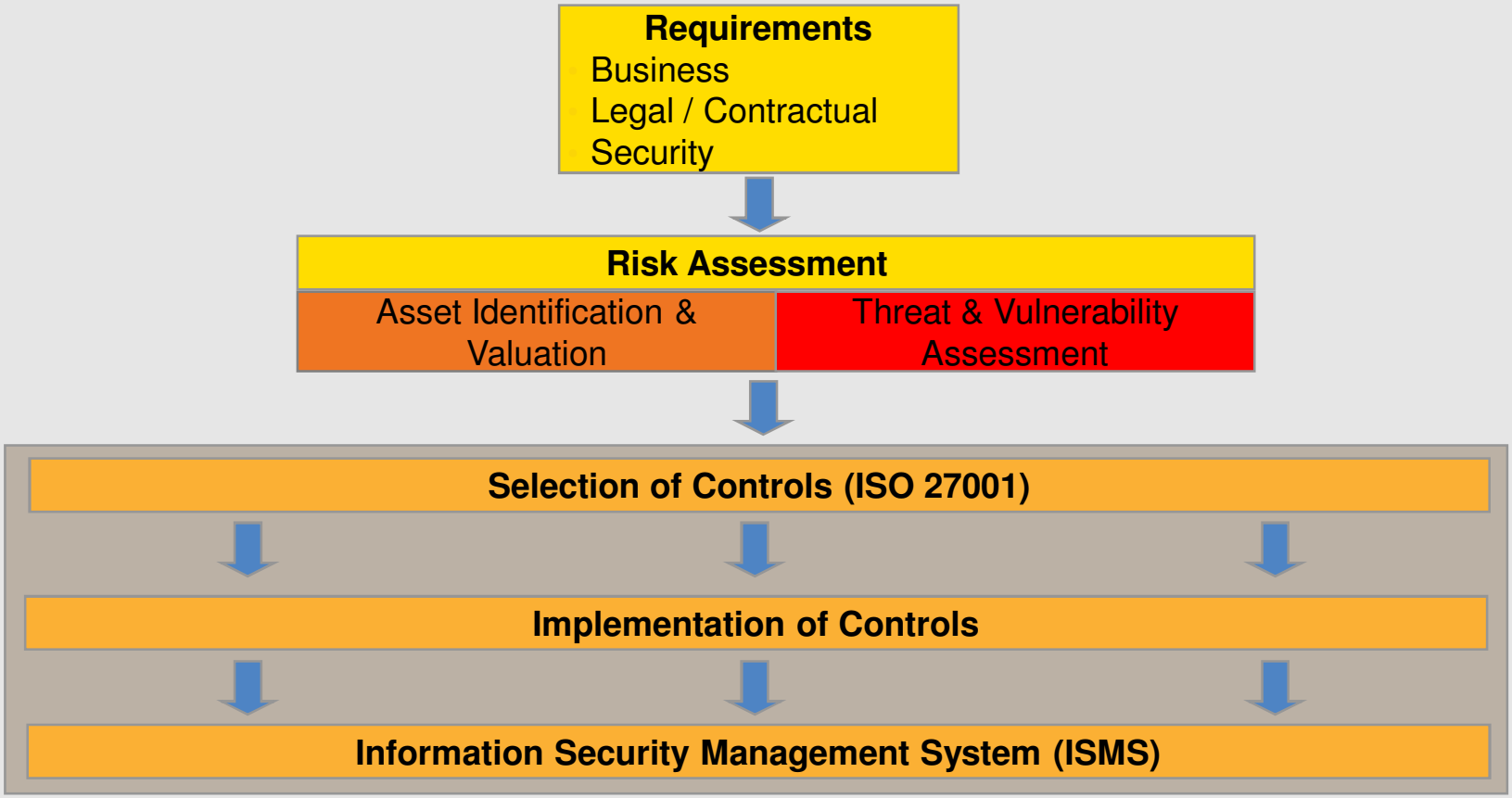
Or, if you can, plan Q by Q

InfoSec Roadmap - Tactical

	2011												2012		2013
Program Domain	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	H1	H2	Year
Governance															
Compliance															
Networks															
Servers															
Desk Top															
Applications															
Data/Database															
SIEM															
Insider Threat															
Physical & Environmental															

For Current Year, planned and budgeted milestones, allowing for long term projects.

Risk Management Program



Auditor Buy-In

Auditor Buy-In

First Best Thing To Do

Get Auditor Input and Approval

Second Best Thing To Do

Audit Briefing Paper

Summary: Manage Your Auditors

Establish a collaborative relationship

Leverage your good practices (or establish same)

Communicate frequently


Critical situations. Ruthless competition. Unforgiving customers. Thankfully you can be absolutely sure of your IT solutions with Tata Consultancy Services (TCS). As one of the world's fastest growing technology and business solutions providers, TCS has built a reputation of delivery excellence based on world-class IT solutions that are on time, within budget and consistently deliver superior quality. So, it comes as no surprise that we pioneered the concept of the Global Network Delivery Model. Developed Innovation Labs and Solution Accelerators. Achieving a level of delivery excellence that provides greater value to our customers and is the industry benchmark. Enabling our clients to experience certainty.
TATA CONSULTANCY SERVICES
Experience certainty.
IT Services • Business Solutions • Outsourcing
To learn how your business can experience certainty, visit www.tcs.com
Promise what we deliver.
Deliver what we promise. That's
certainty
Thank You