OT Cyber Security

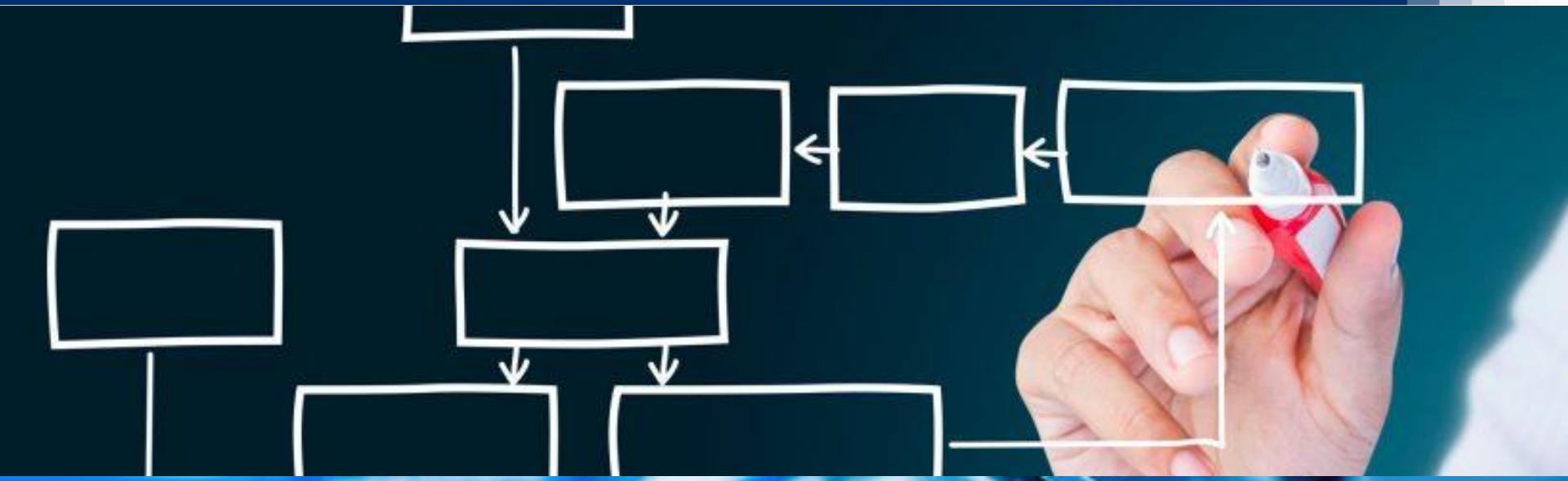
Organizational challenge or Technical challenge

Marcel Kelder

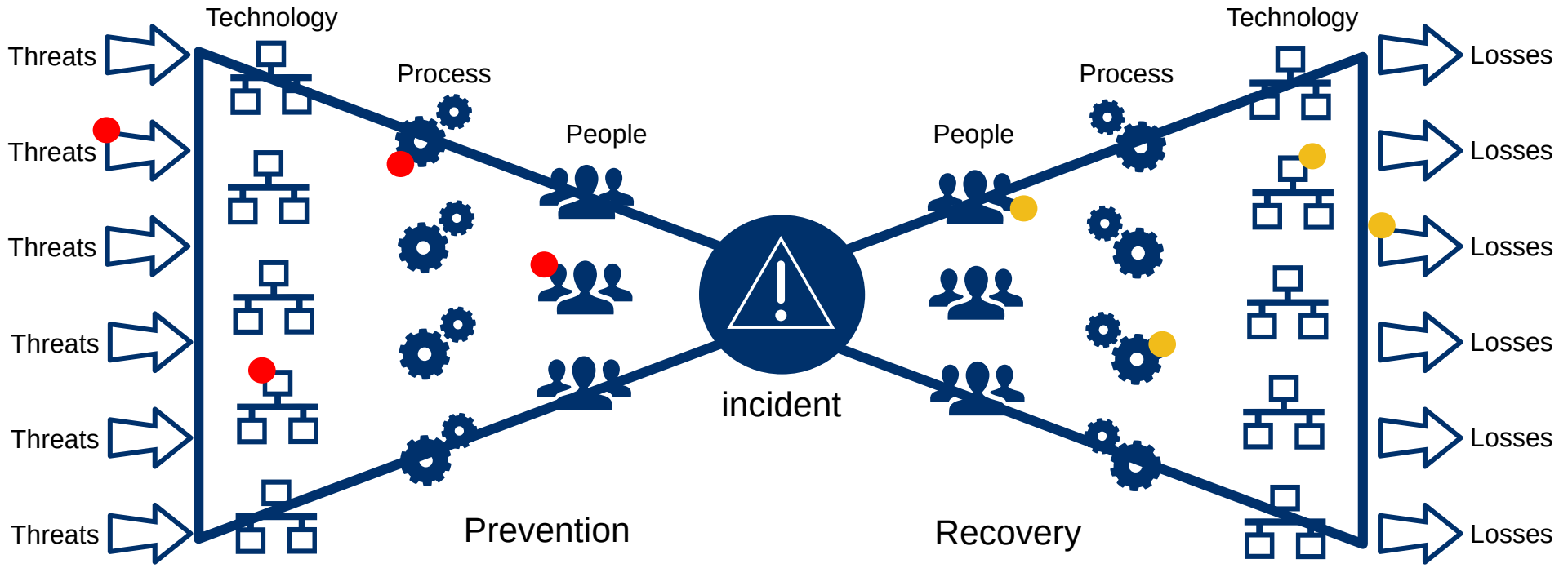
Director Advanced Solutions

April, 2018

The Challenge



What is Cyber Security

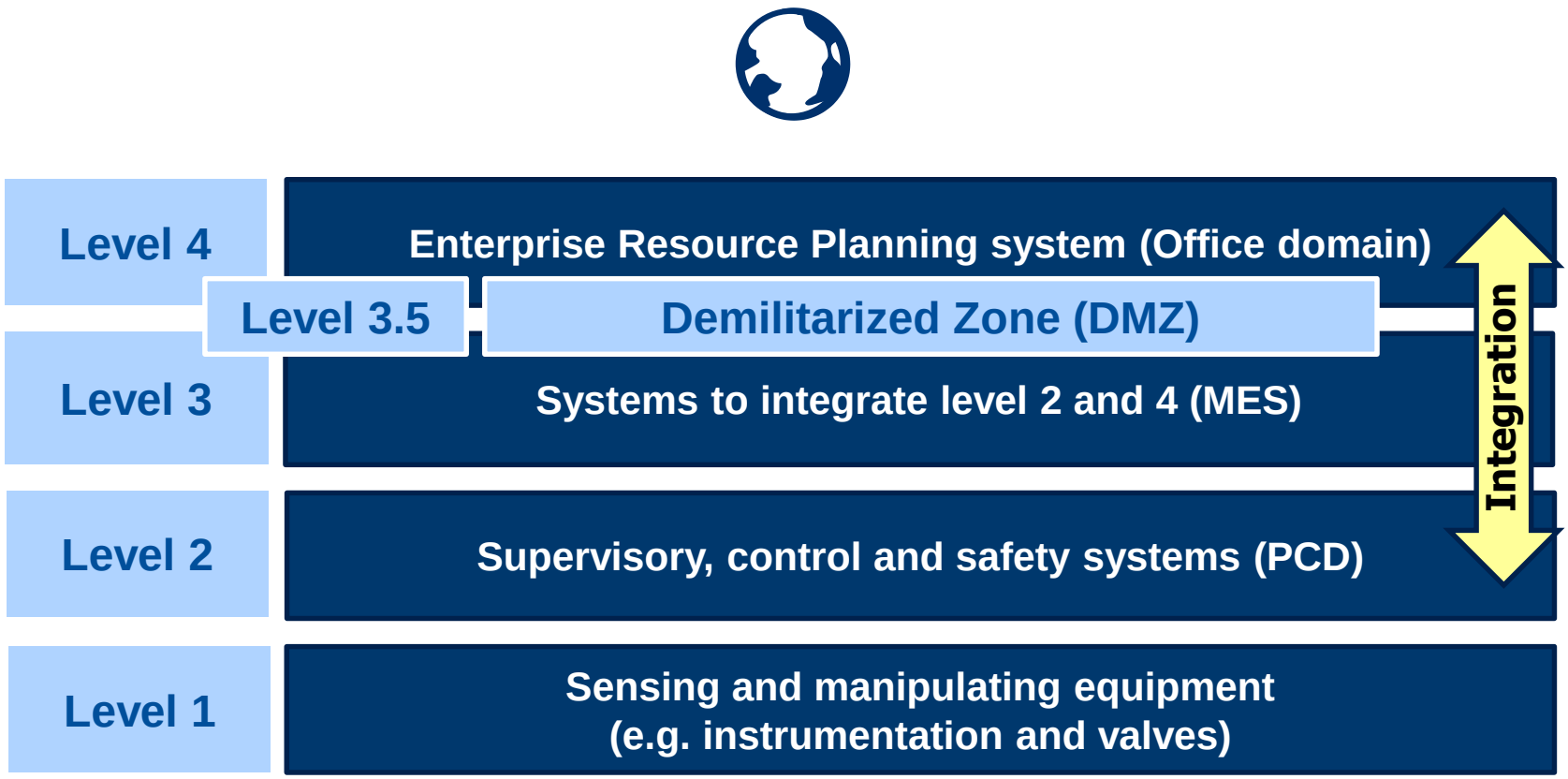


BARRIER MANAGEMENT

Even a bigger challenge

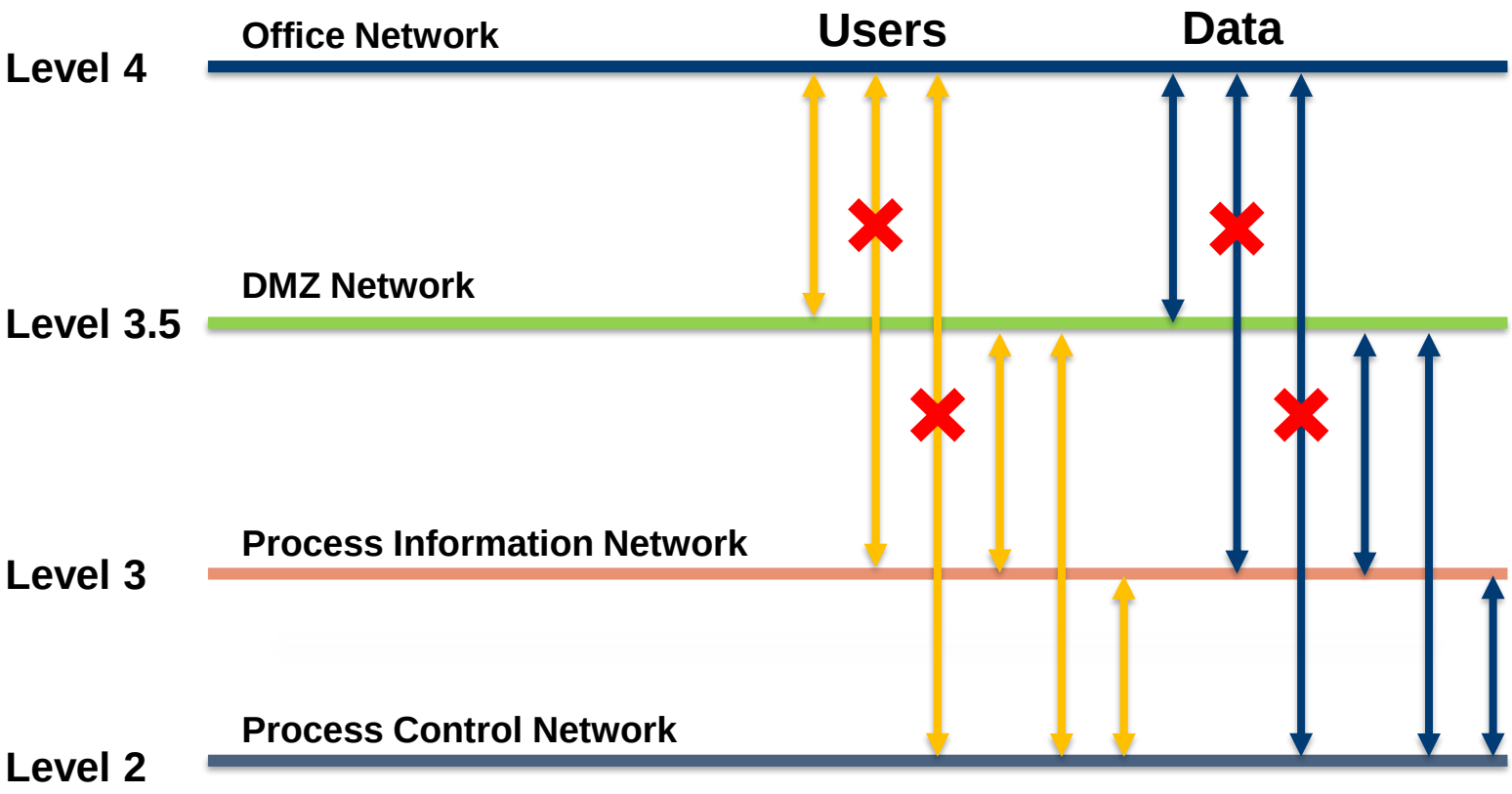
Introduction

The different domains



The objectives of ISA-95 are to provide consistent terminology that is a foundation for supplier and manufacturer communications, provide consistent information models, and to provide consistent operations models which is a foundation for clarifying application functionality and how information is to be used.

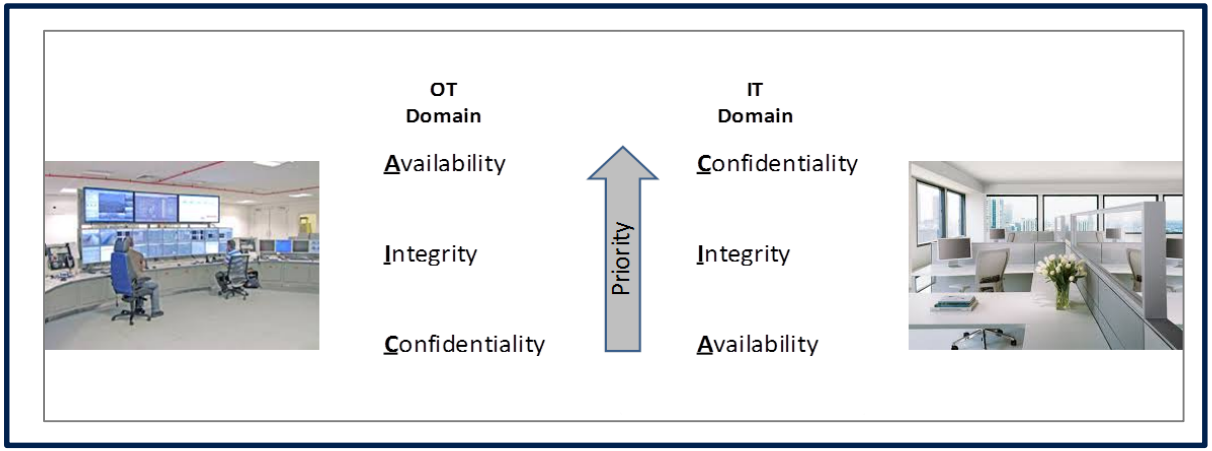
User and Information streams



The way information is exchanged between the different layers significantly determines the Cyber Security Infrastructure

Cyber Security for the different domains

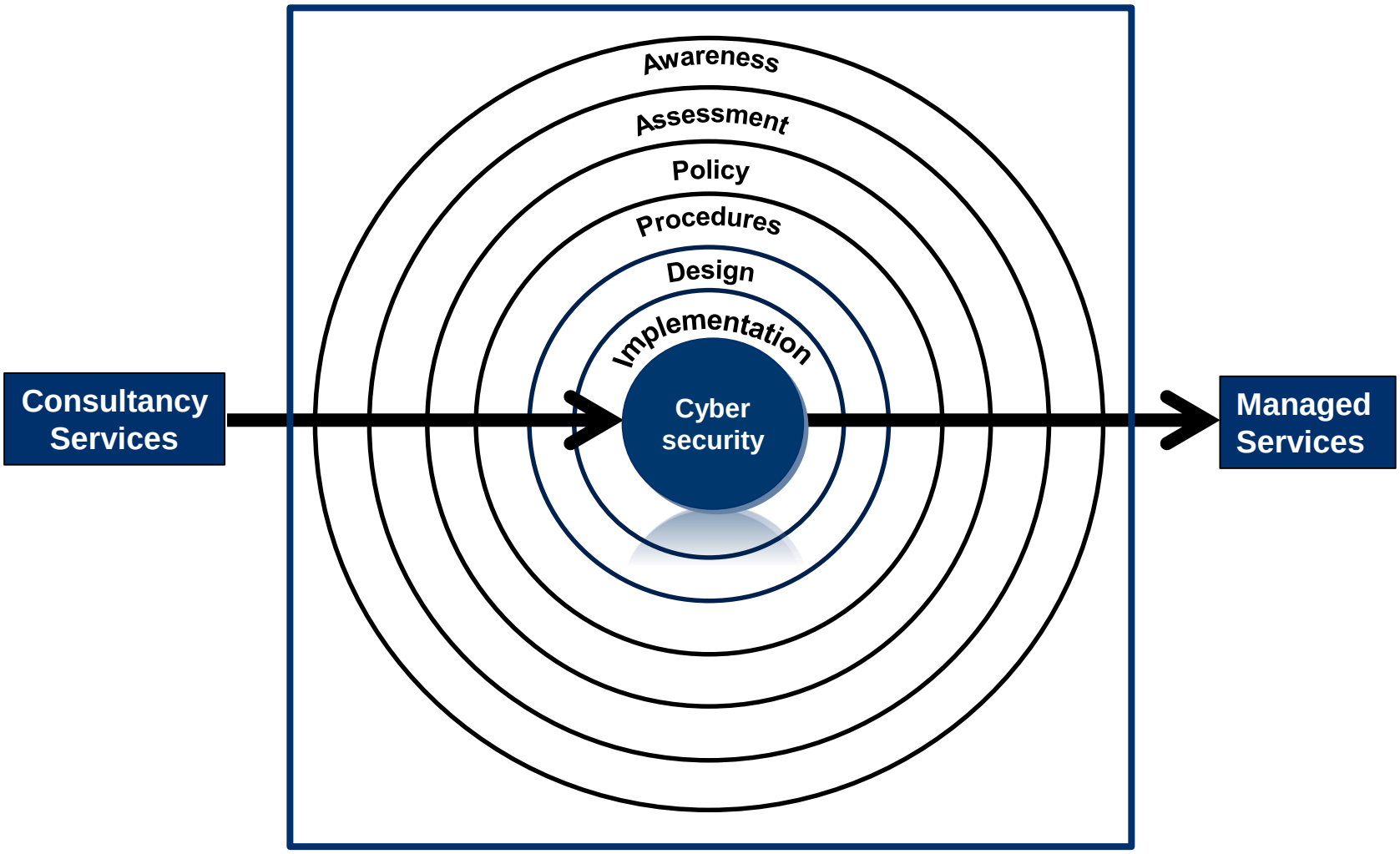
- **Today integration between different domain is crucial for plant operation**
- **Remote services is direct related to Cyber security and nowadays critical part of operation**
- **Cyber security in the control & production domain L2 and L3 is different from Cyber security in the office domain L4**



Why is the OT domain so different

- Business as usual for many years
- Many different suppliers
- No owner or multiple owners for Cyber security
- Limited knowledge of OT Cyber security
- Limited awareness for integrity and confidentiality
- Not one unified platform (Windows XP, Windows 7, Windows 10)
- Different levels of cyber security maturity among the suppliers
- OT System performance impacts availability and/or safety
- System updates by others may impact warranty or maintenance
- Often no proper asset inventory

Yokogawa Plant Security Program



Risk Management Framework

Certified company and consultants

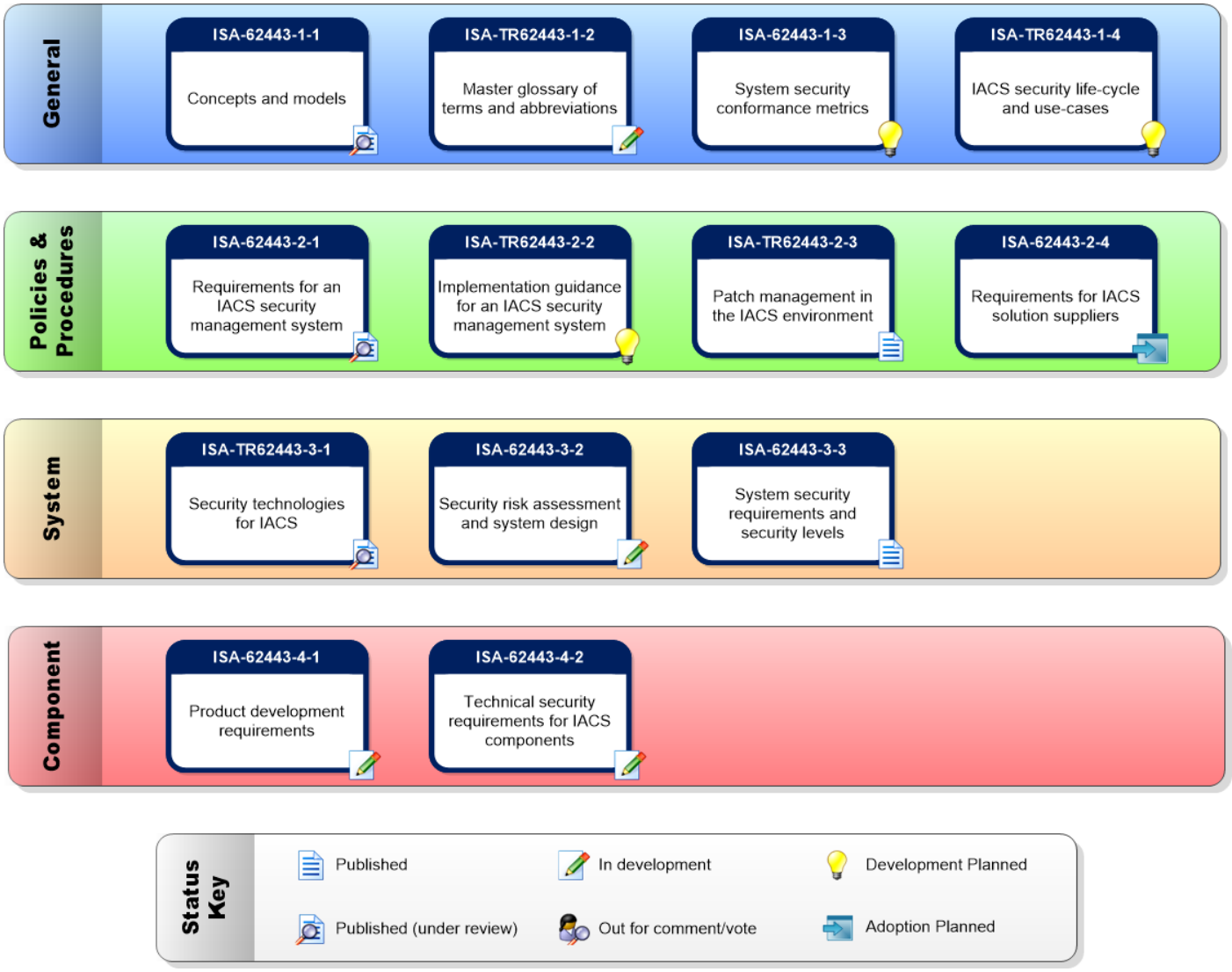
- **Global Industrial Cyber Security Professional (GICSP) applies for all our OT security consultants**

- **Certified Information Systems Security Professional (CISSP)**

- **Statement on Standards for Attestation Engagements (SSAE) No. 16 (from October 2015)**

- **ISO27001: Information security management**

The ISA-62443/IEC 62443 Series



Typical security level (IEC 62443)

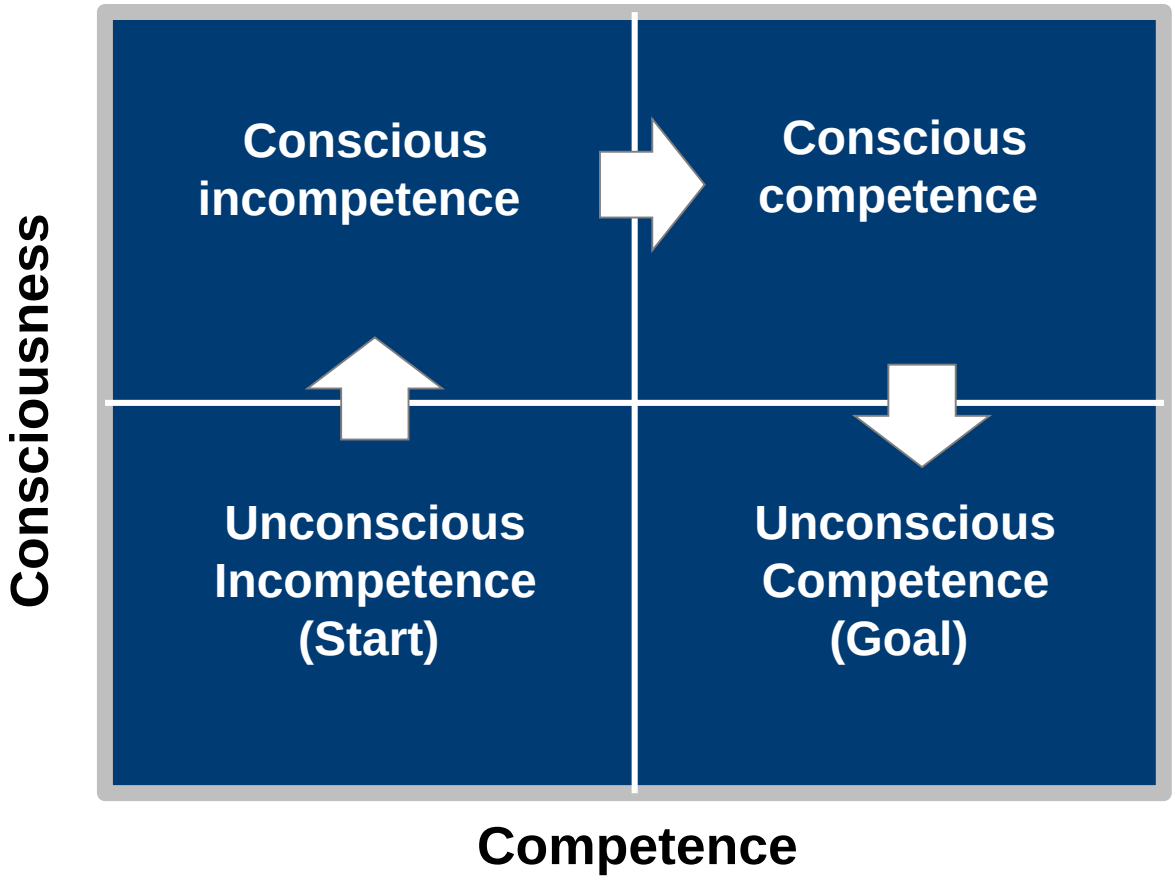
		Skills	Motivation	Means	Resources
SL4	Nation-state	ICS Specific	High	Sophisti-cated (Campaign)	Extended (multi-disciplinary teams)
SL3	Hacktivist, Terrorist	ICS specific	Moderate	Sophisti-cated (Attack)	Moderate (groups of hackers)
SL2	Cyber crime, Hacker	Generic	Low	Simple	Low (Isolated individuals)
SL1	Careless employee, contractor	No attack skills	Mistakes	Non-intentional	Employee, contractor

Maturity Indicator Levels

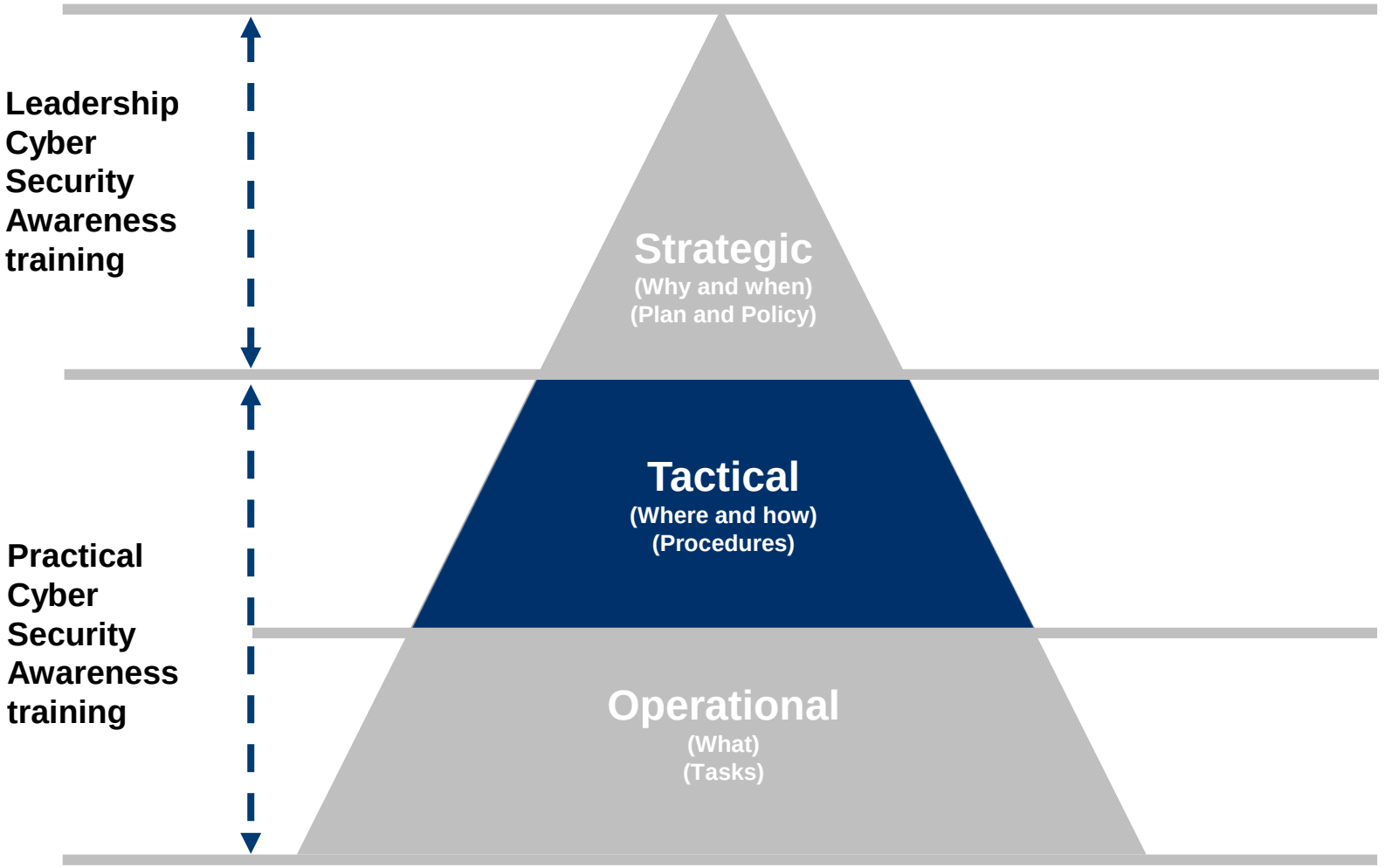
MIL4	Practices have been further institutionalized and are now being managed. Policies exist, the organization is fully risk aware and periodic audits and reviews of all activities are in place to improve and anticipate on new threats.
MIL3	Practices are no longer performed irregular or ad hoc, performance of the practices is sustained over time and are well documented. Overall performance is measured and documented.
MIL2	Initial formal practices exist but may be performed in an ad hoc manner. however they must be performed.
MIL1	No formal practices exist.

Awareness

Awareness



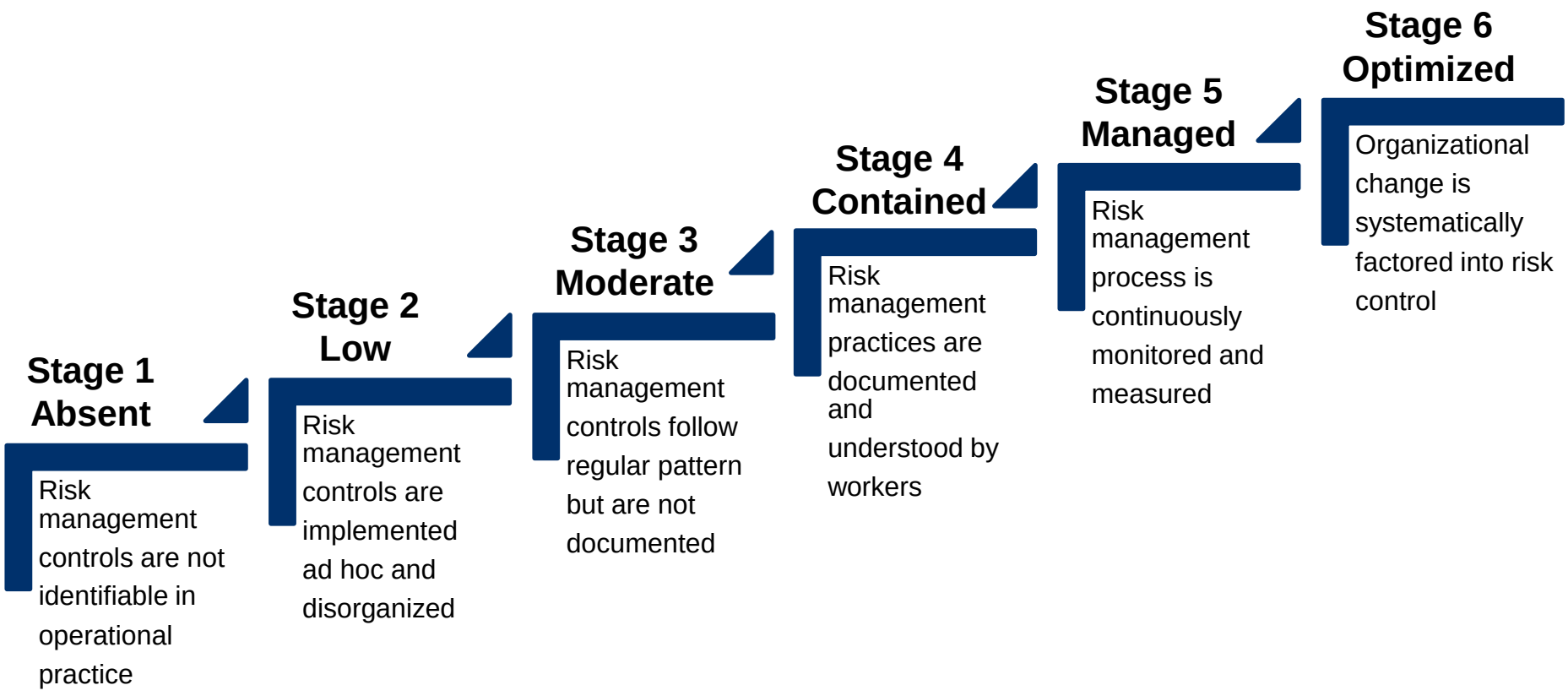
Awareness training



Risk Assessments

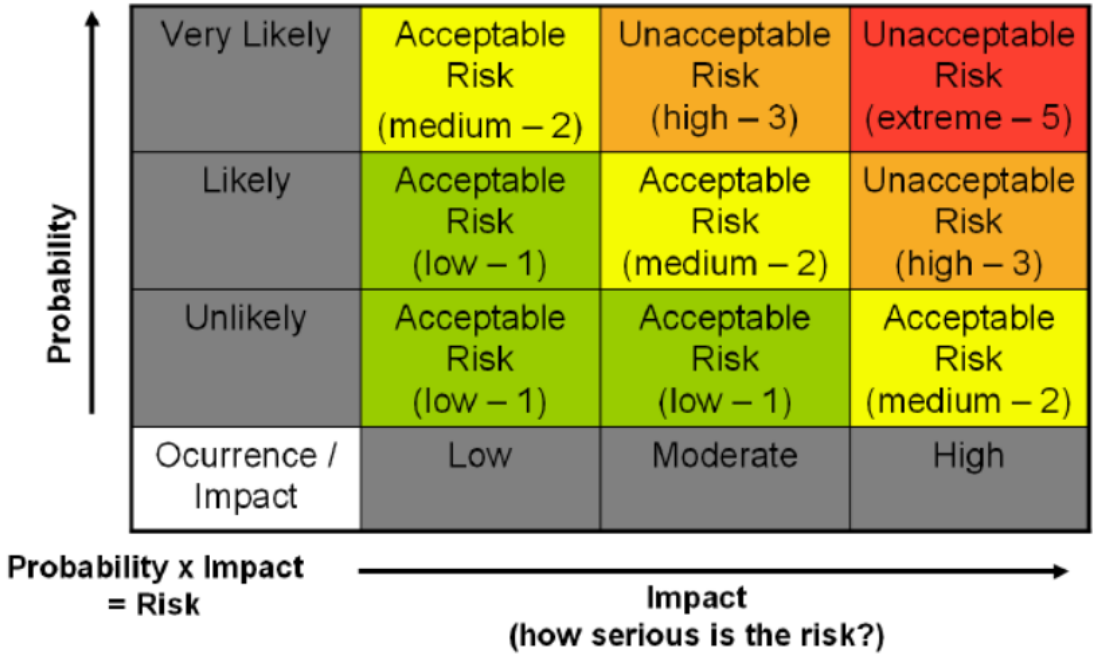
Stages of maturity scale

- **The practical Risk Management Framework process is executed in six phases, the first two of which involve the establishment of a formal security framework that is based on the setting of the boundaries of control and the definition of a security control set.**



Vulnerabilities versus Risk

- Risk = Likelihood * Impact
- Risk = Threat * Vulnerability * Asset
- Risk = ((Vulnerability * Threat)/CounterMeasure) * AssetValueatRisk



Types of risk assessment

Asset Risk Assessment

- Goal is detect the vulnerabilities related to the assets (e.g. end point security, user access, network security etc.) and determine the OT security base line. The assessment is focused on technology.
- It is a benchmark of the types and size of potential vulnerabilities, which could have a significant impact on asset and organization.
- It must be emphasized that the baseline is an initial risk assessment that focuses on a broad overview in order to determine the risk profile to be used in subsequent risk assessments and/or next step of the OT security program.
- The outcome is a risk profile with a clear description of the identified risks

Operational Risk Assessment

- Goal is to assess the operational effectiveness of identifying, analyzing and respond to risk in the OT domain. The assessment is focused on organization and processes.
- Similar to the Asset Risk Assessment, initially it is a benchmark to determine the base line.
- The outcome is a risk profile with a clear description of the identified risks

Infrastructure Readiness Assessment

- **Inventory (asset) management**
  - Nodes connected to the network
  - Installed software and versions
- **Physical Security assessment**
- **Network Security assessment**
  - Network Architecture
  - Firewalls
  - Routers & Switches
  - Remote Access
- **Host Based Security assessment**
  - Antivirus Management
  - Patch Management
  - System Hardening
- **Disaster Recovery assessment**

Physical Security

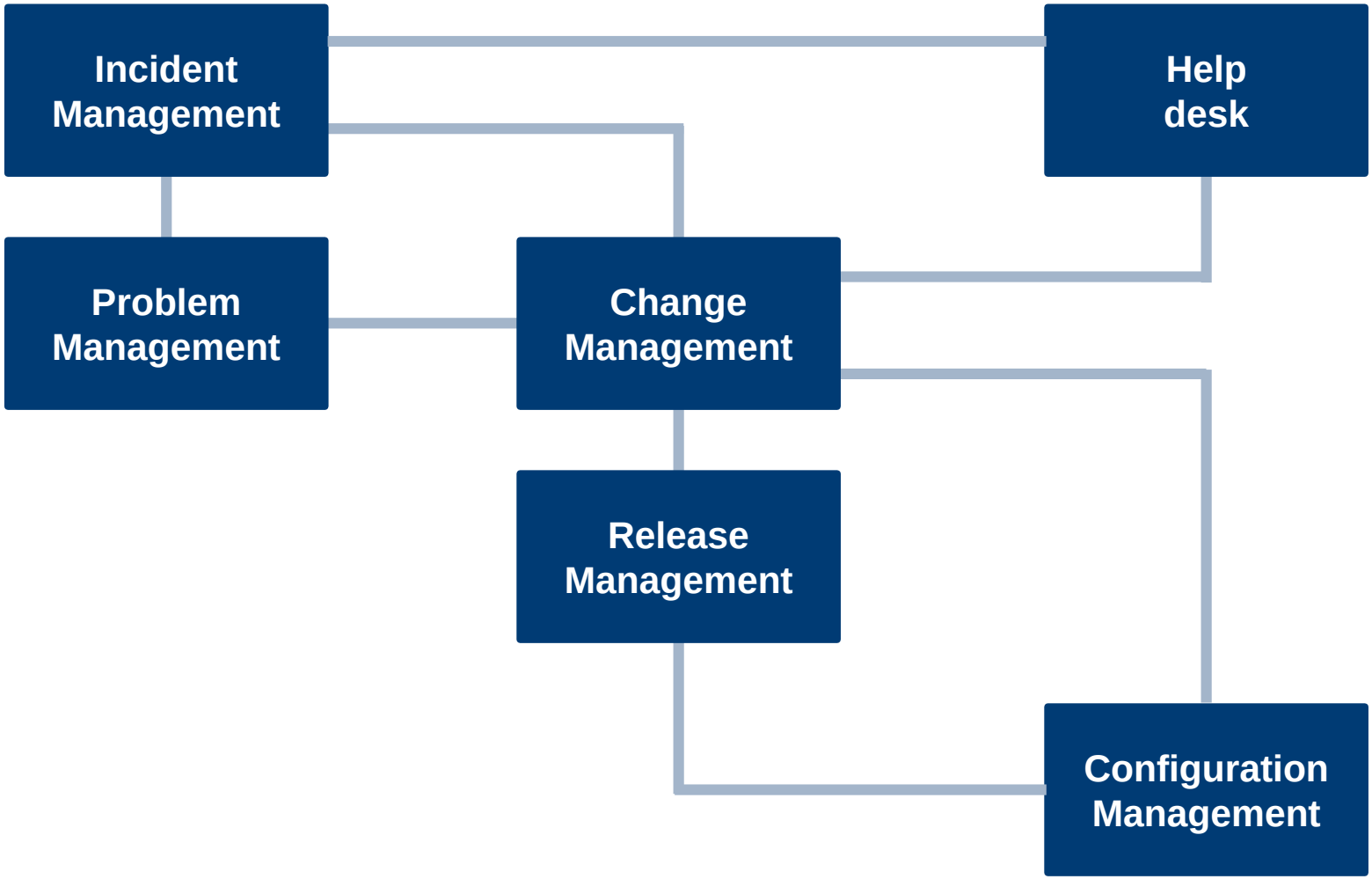
Network Security

Host Based Security

Application Based Security

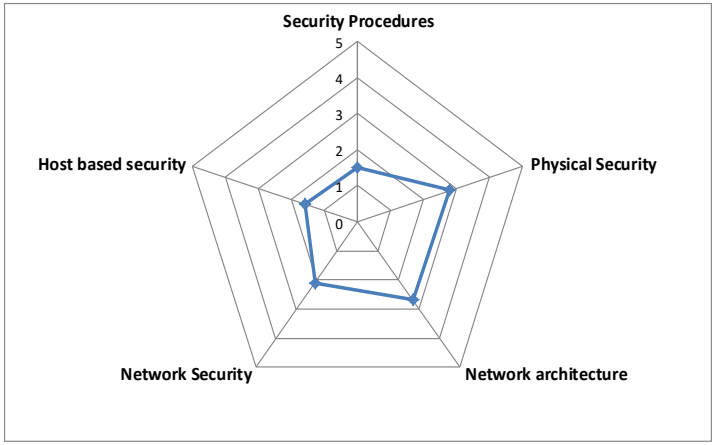
Disaster Recovery

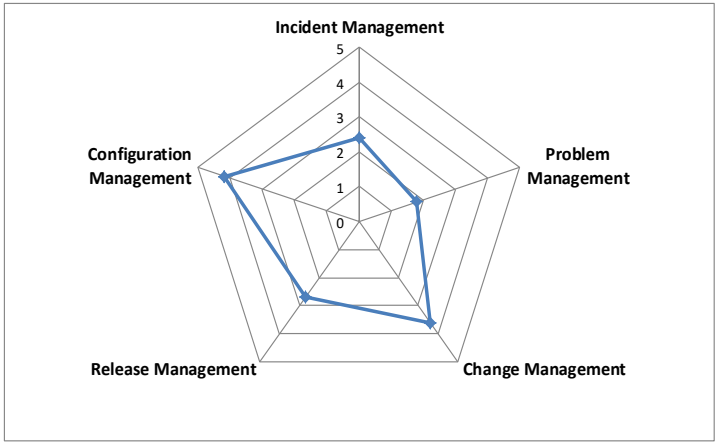
ITIL Process



Assessment report

Operations		1.5
Incident Management		
Problem Management		
Change Management		
Release Management		
Configuraiton Management		
Physical Security		2.8
Environment		
User Access Policy		
Network Architecture		2.7
Network levelling		
Network Zoning		
Network Security		2.1
Firewall		
Routers & Switches		
Legacy Devices		
Network Management		
Host Based Security		1.6
Antivirus Management	2.4	
Patch Management	1.0	
System Hardening	1.5	
Backup and Disaster Recovery	1.5	
`Remote access		





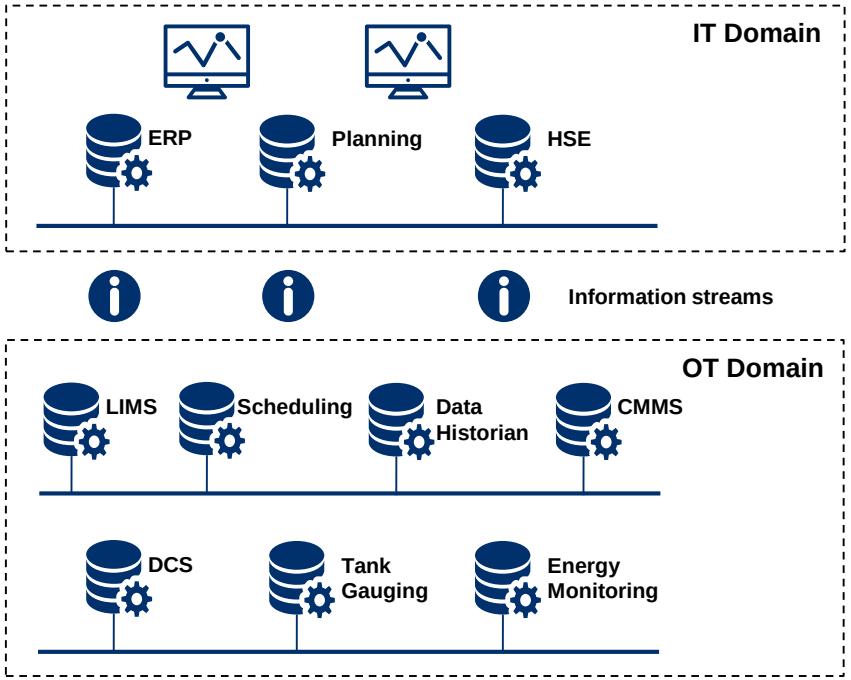
- **Deliverables:**
  - **Score card**
  - **Site report with findings and recommendations**

Types of risk assessment

Business Risk Assessment

- Goal is to identify risk with respect to information security between the IT domain and the OT domain.
- The main information streams between the IT and OT domain are analyzed in accordance with the three security objectives; Confidentiality, Integrity, and Availability
- The potential CIA impact values are determined by using the values low, moderate, high or not applicable.

Information stream	Security category			Comment
	C	I	A	
Accounting				
Environmental reporting				
Planning & Scheduling				
Logistics				



Security Objectives

- **CONFIDENTIALITY**
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
    - A loss of confidentiality is the unauthorized disclosure of information
- **INTEGRITY**
  - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
    - A loss of integrity is the unauthorized modification or destruction of information
- **AVAILABILITY**
  - Ensuring timely and reliable access to and use of information
    - A loss of availability is the disruption of access to or use of information or an information system

Potential impact on organization and business

- The potential impact is **LOW** if:
  - The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, assets, or individuals.
- The potential impact is **MODERATE** if:
  - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, assets, or individuals.
- The potential impact is **HIGH** if:
  - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.

Categorization of Information Types

- SC information **type** = {(confidentiality, impact), (integrity, impact), (availability, impact)}
  - where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE

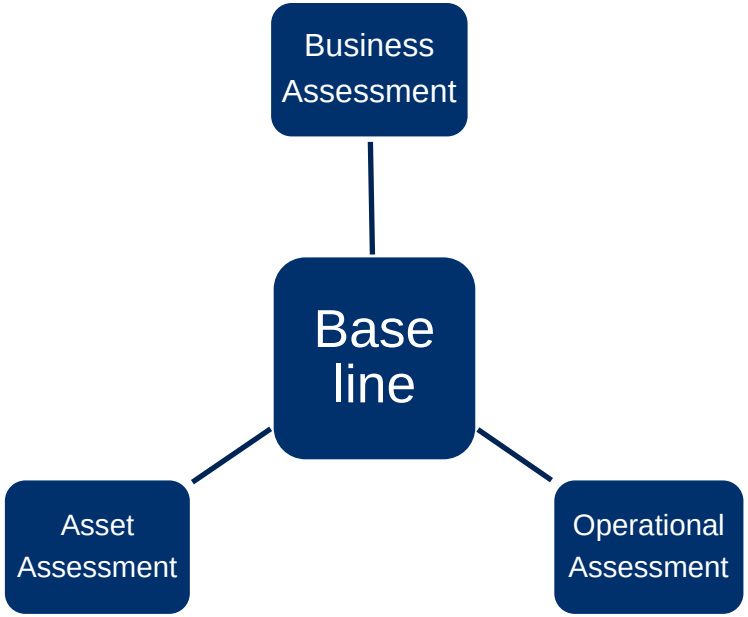
- SC information **system** = {(confidentiality, impact), (integrity, impact), (availability, impact)}
  - where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE

Examples:

- SC control system = {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}
- SC historian system = {(confidentiality, moderate), (integrity, HIGH), (availability, moderate)}

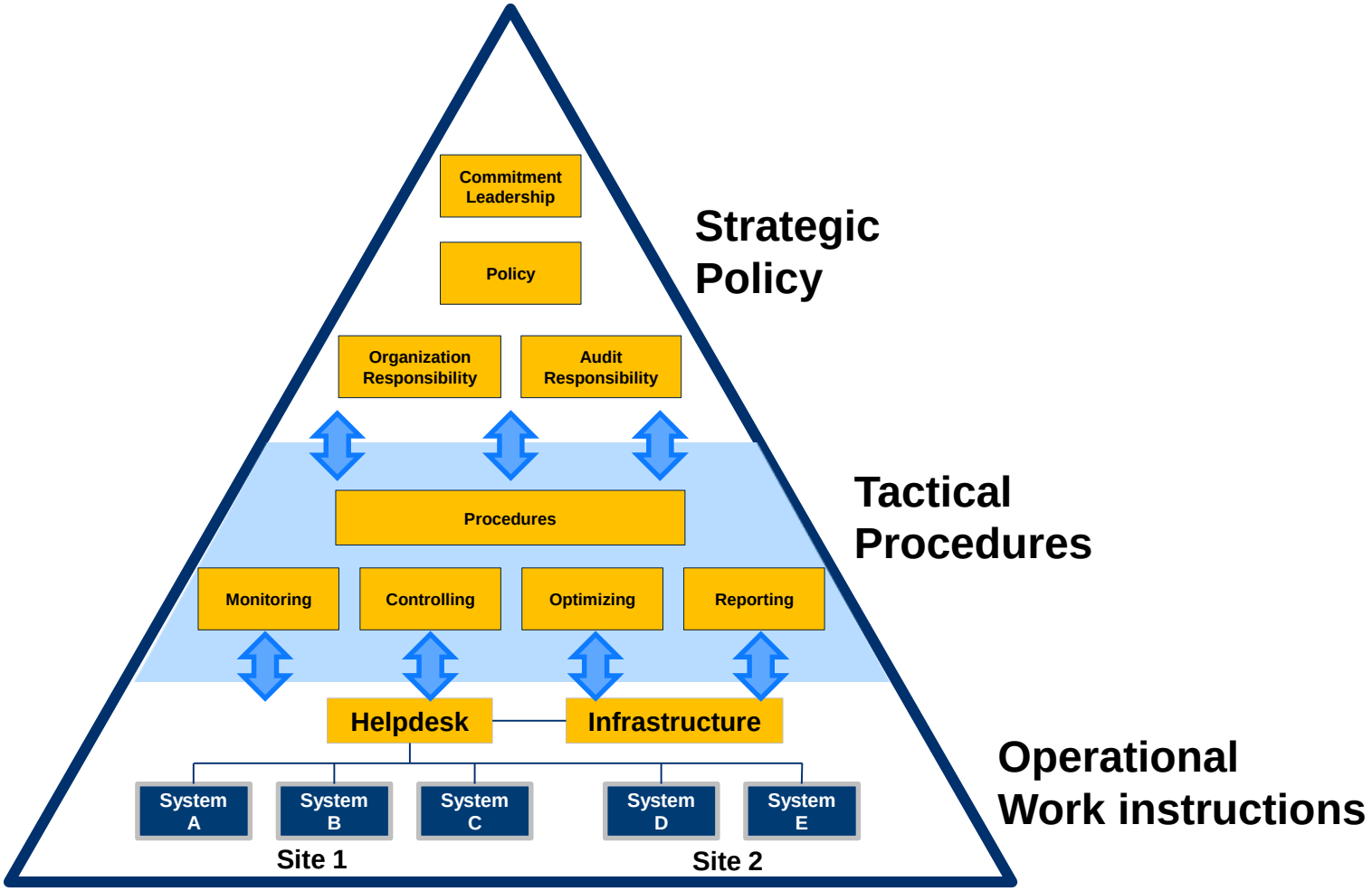
Baseline Risk Assessment

- The overall OT security baseline risk management provides the understanding of the actual and potential risks to asset, people and processes. This information is useful in determining the next step in the OT security program. Next step could be:
  - Determine and prioritize the policy statements
  - Determine and prioritize the security countermeasures
  - Input to the OT security business case



Policy, Procedures, Business Case and Design Principles

Management Structure



Policy

- [Wiki] A **policy** is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol. Policies are generally adopted by a governance body within an organization.

- Policies are clear, simple high level statements of how your organisation intends to conduct its services, actions or business.

Typical Cyber security policy content

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

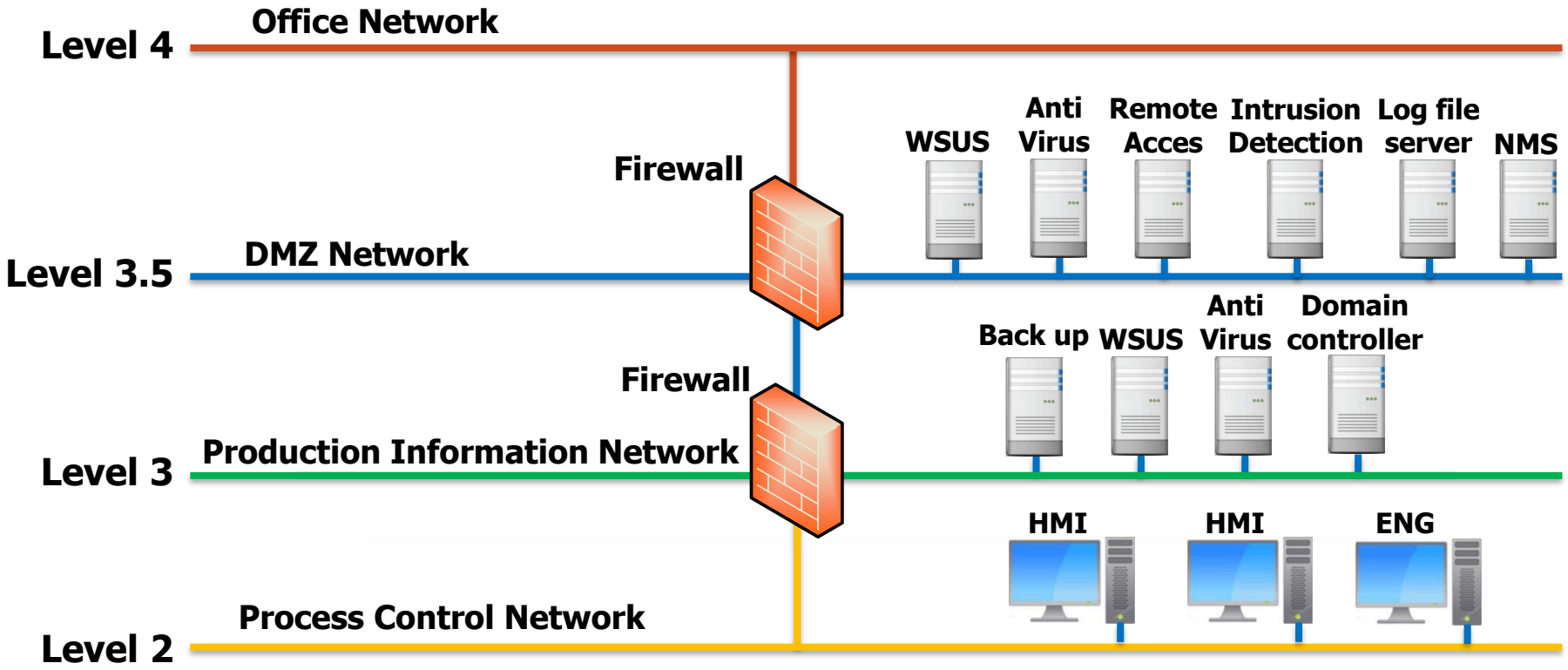
Procedures

- A Procedure is based and related to a Policy and its deliverables.

- [Wiki] A procedure is a document written to support a "policy directive". A procedure is designed to describe **Who, What, Where, When**, and **Why** by means of establishing corporate accountability in support of the implementation of a "policy".

Design Principles

- Design principles are sets of generally guidelines and design considerations, all of which reflect the accumulated policies and procedures. They serve as a starting point for detail design.



WSUS	: Windows Server Update Services	HMI	: Human Interface Station
NMS	: Network Monitoring Station	ENG	: Engineering Station

Business case for OT security

- **The business case is a translation of the risk assessment and policies into a proposal to senior management for budget to implement the total OT program**

- **Typical content for an OT security business case**
  - **Executive summary**
    - Summary for senior management
  - **Recommendations**
    - Provide a recommendation for solving the business and operational needs/problems
  - **Business and operational needs**
    - Analysis of the Business and operational needs in relation to the identified risks
  - **Solution Analysis**
    - Summary of the different OT security solutions including the CAPEX and OPEN costs
  - **Available Options**
    - Alternative solutions or example outsourcing of services

OT security program

Managed services

Managed Services

Requirement	Yokogawa Managed Service
Asset Inventory	Automated asset discovery and asset inventory
O.S. Security patching	Automated distribution of validated Microsoft updates
Anti-Virus Management & Updates	Automated distribution of validated signature updates
Intrusion detection and prevention	In-line deep packet inspection of inbound and outbound network traffic
Remote Access	Unified secured remote access, with 2 factor authentication
Log file collection	Automated log file collection to central log server
Traffic monitoring	Active alerting and proactive blocking of unauthorized communication
Security majority reporting	Automated report of the status of the applied security measures
Proactive system monitoring	CPU, Memory load, Disk usage, system and software failures
24x7x365 supported	Helpdesk and managed services
Incident response	Global security incident response team

Co-innovating tomorrow™