OMV Aktiengesellschaft

Challenges for
Information Security

Hansjörg Kalcher (CISO)

FH St. Pölten, Jänner 2013

Sec_rity is not complete without U !

PETROM
Member of OMV Group

Move & More. OMV

AGENDA

OMV GROUP, ORGANIZATION

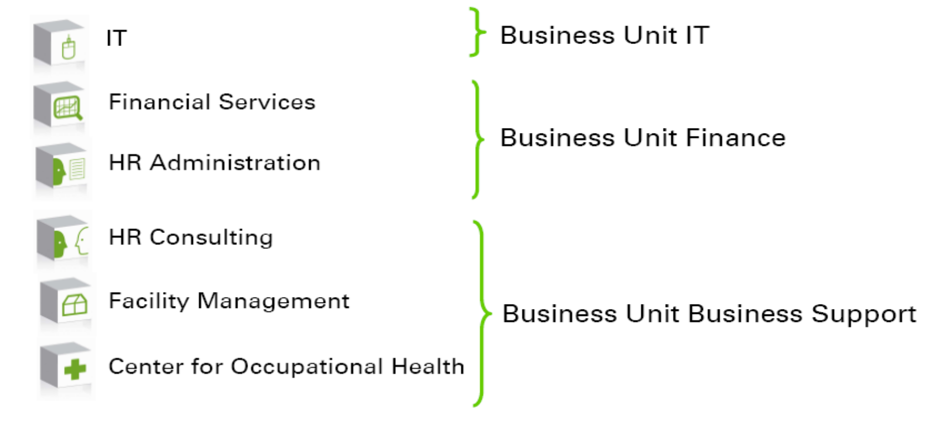
Business areas within OMV Group

Refining & Marketing

Exploration & Production

Gas & Power

Global Solutions an integrated Competence Center within OMV



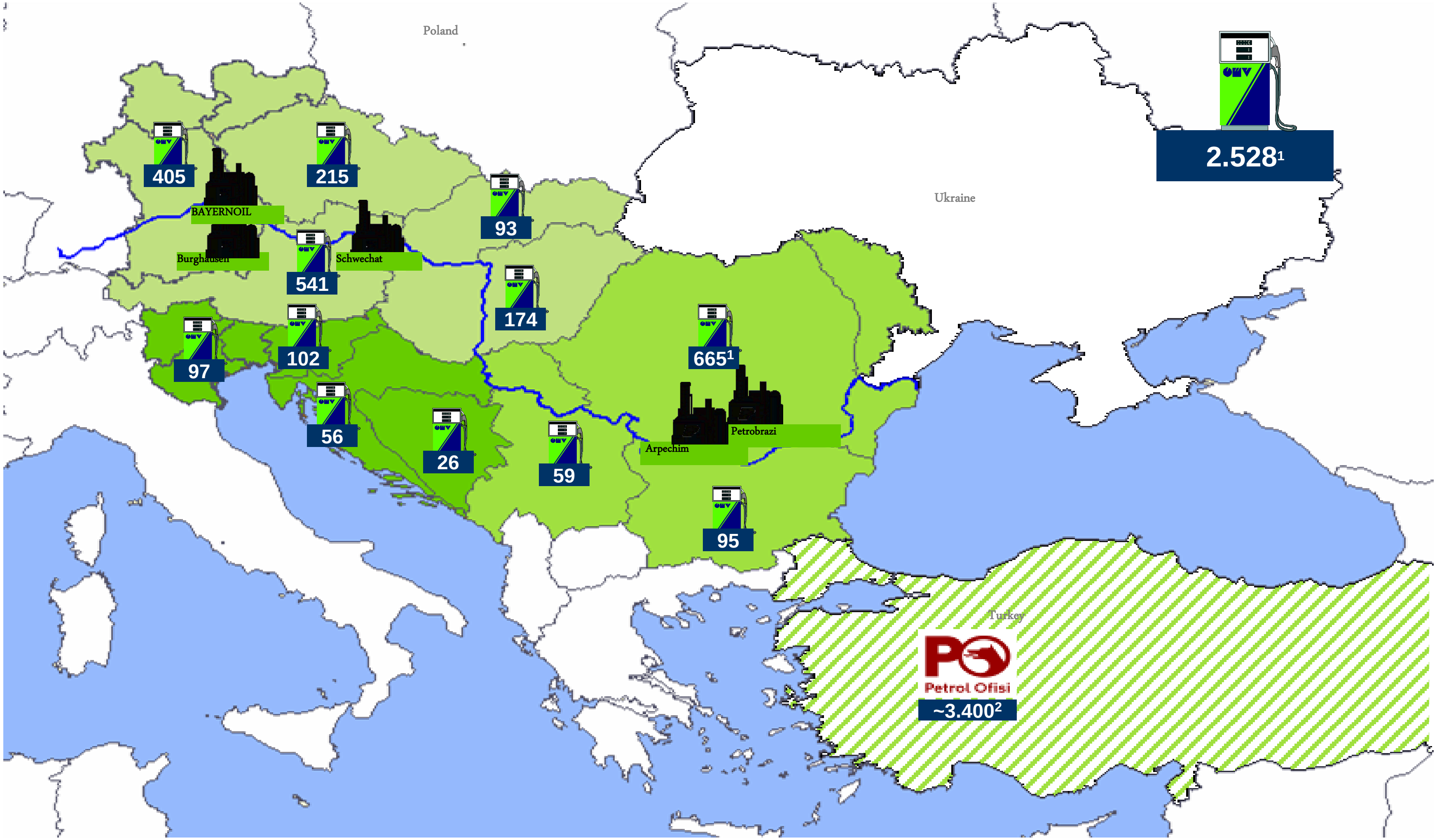
IT } Business Unit IT

Financial Services
HR Administration } Business Unit Finance

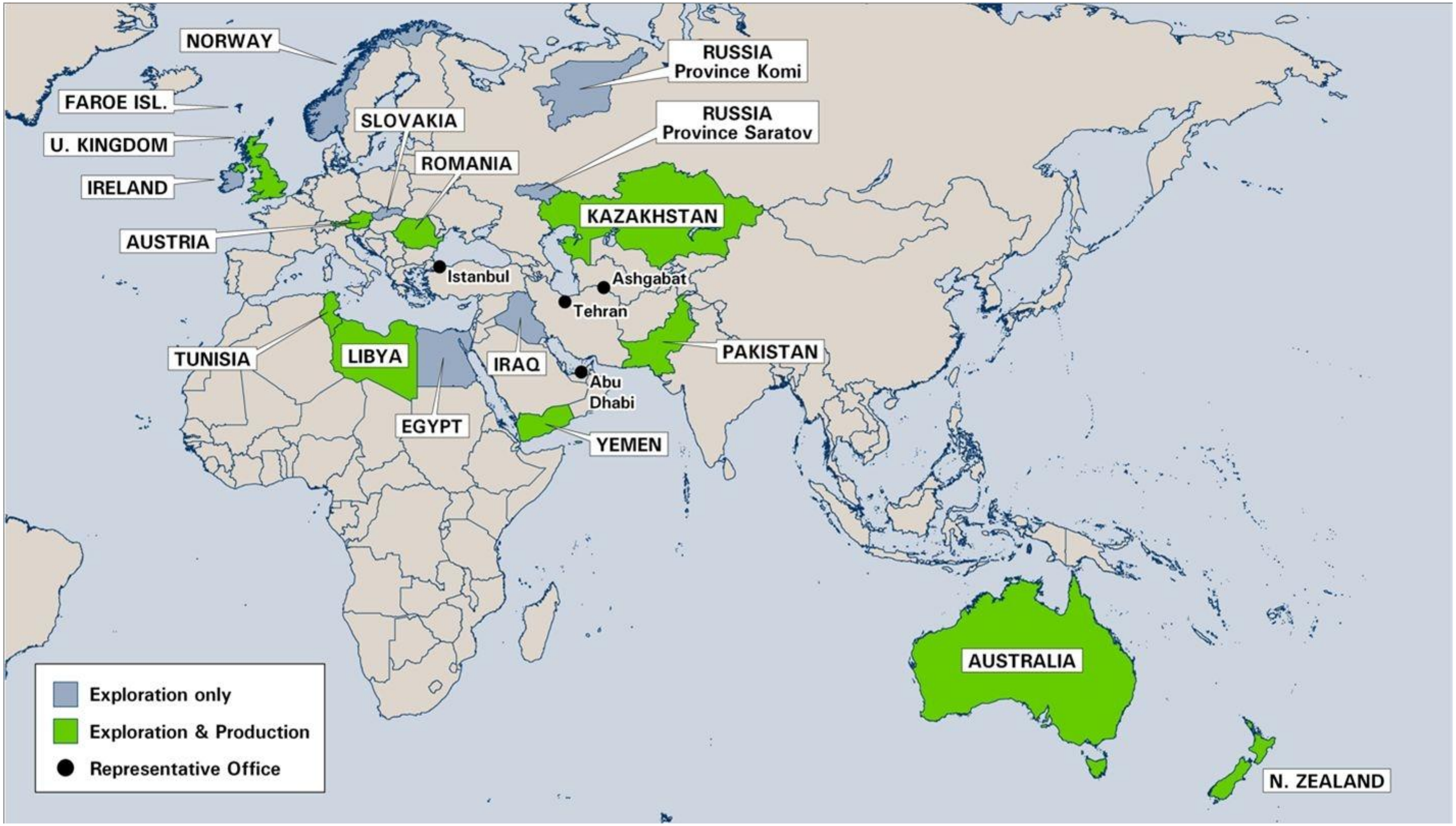
HR Consulting
Facility Management
Center for Occupational Health } Business Unit Business Support

~ 30 000 employees; ~ 2.100 server; ~ 18.000 clients

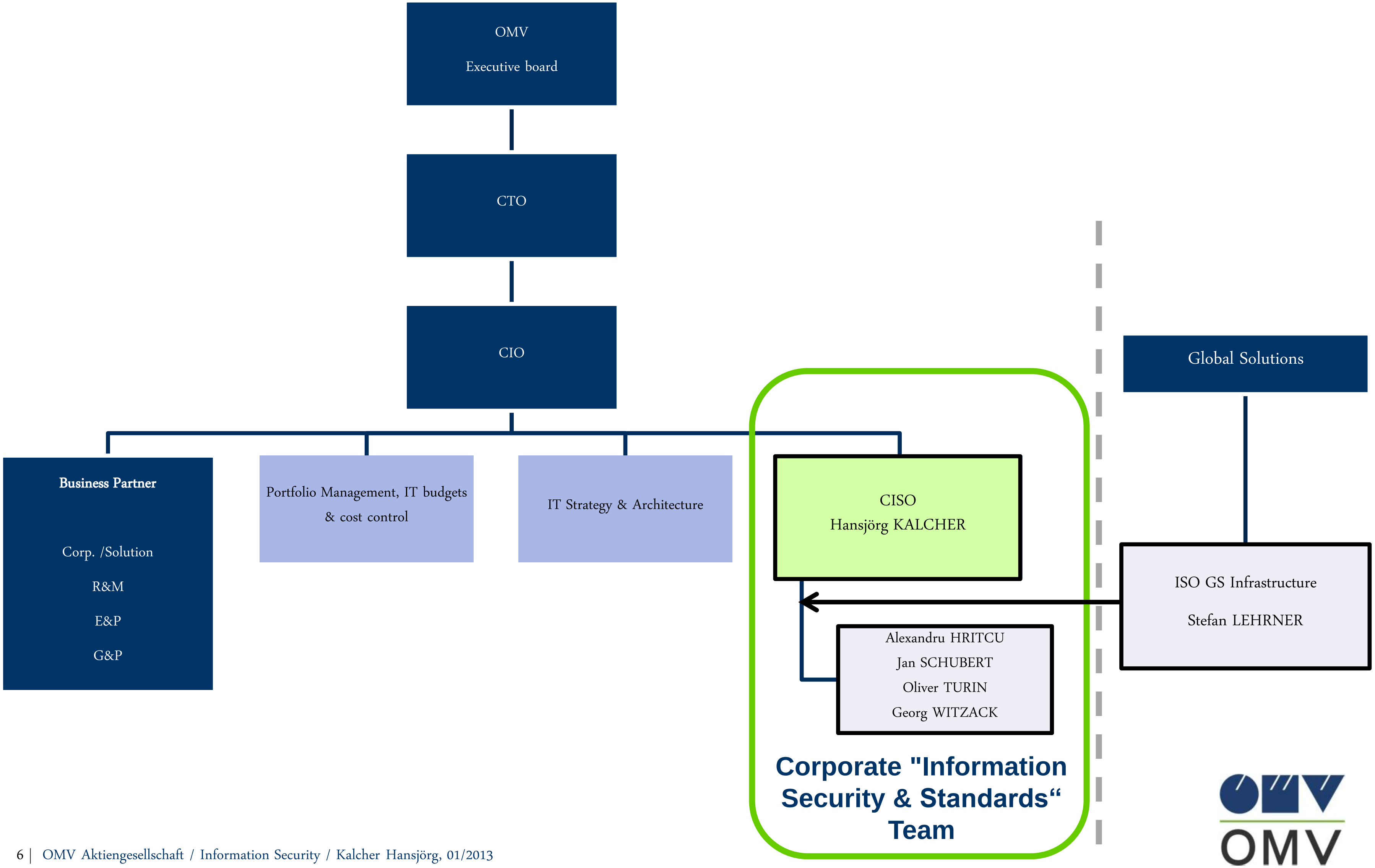
Refining & Marketing activities (R&M)



Exploration & Production activities (E&P)



Corporate Information Security…where are we?



OMV
Executive board

CTO

CIO

Business Partner

Corp. /Solution

R&M

E&P

G&P

Portfolio Management, IT budgets & cost control

IT Strategy & Architecture

CISO
Hansjörg KALCHER

Alexandru HRITCU
Jan SCHUBERT
Oliver TURIN
Georg WITZACK

Corporate "Information Security & Standards“ Team

Global Solutions

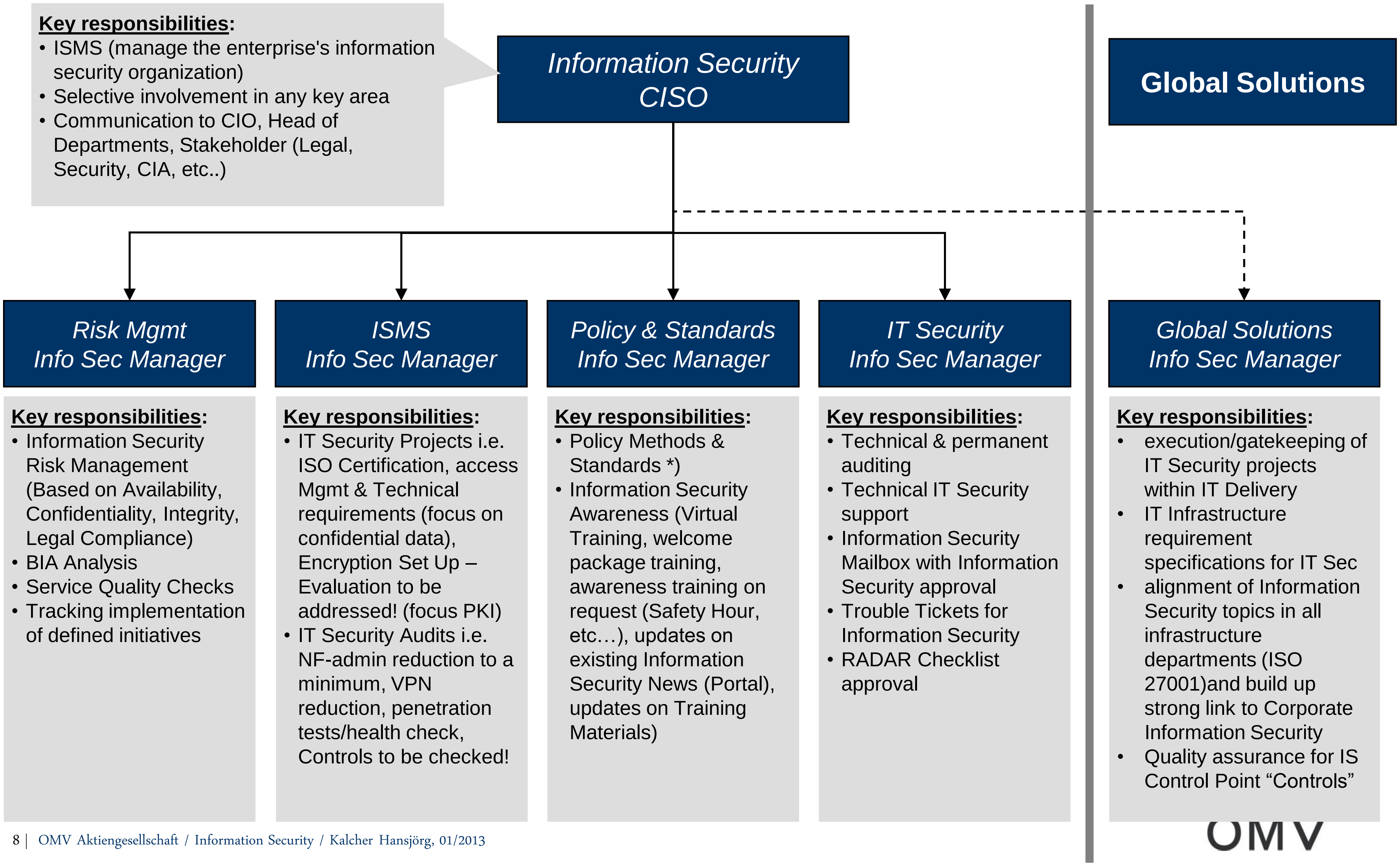
ISO GS Infrastructure

Stefan LEHRNER

AGENDA

- OMV GROUP, ORGANIZATION
- DISCIPLINES
- AWARENESS

Information Security - Department personnel and responsibilities



Key responsibilities:
- ISMS (manage the enterprise's information security organization)
- Selective involvement in any key area
- Communication to CIO, Head of Departments, Stakeholder (Legal, Security, CIA, etc..)

Information Security CISO

Global Solutions

Risk Mgmt Info Sec Manager

Key responsibilities:
- Information Security Risk Management (Based on Availability, Confidentiality, Integrity, Legal Compliance)
- BIA Analysis
- Service Quality Checks
- Tracking implementation of defined initiatives

ISMS Info Sec Manager

Key responsibilities:
- IT Security Projects i.e. ISO Certification, access Mgmt & Technical requirements (focus on confidential data), Encryption Set Up – Evaluation to be addressed! (focus PKI)
- IT Security Audits i.e. NF-admin reduction to a minimum, VPN reduction, penetration tests/health check, Controls to be checked!

Policy & Standards Info Sec Manager

Key responsibilities:
- Policy Methods & Standards *)
- Information Security Awareness (Virtual Training, welcome package training, awareness training on request (Safety Hour, etc…), updates on existing Information Security News (Portal), updates on Training Materials)

IT Security Info Sec Manager

Key responsibilities:
- Technical & permanent auditing
- Technical IT Security support
- Information Security Mailbox with Information Security approval
- Trouble Tickets for Information Security
- RADAR Checklist approval

Global Solutions Info Sec Manager

Key responsibilities:
- execution/gatekeeping of IT Security projects within IT Delivery
- IT Infrastructure requirement specifications for IT Sec
- alignment of Information Security topics in all infrastructure departments (ISO 27001)and build up strong link to Corporate Information Security
- Quality assurance for IS Control Point “Controls”

Information Security – Way forward…

…making sure the information keeps

- confidential
- upright and
- available

“Doing the right things”:

- Approach “Information Risk Management”: Reducing the risks based on business needs

Ensure Information Security Risk Management

Safeguarding information according to its protection requirements

2012 | 2013 | 2014

RISK MANAGEMENT

MANAGEMENT SYSTEM

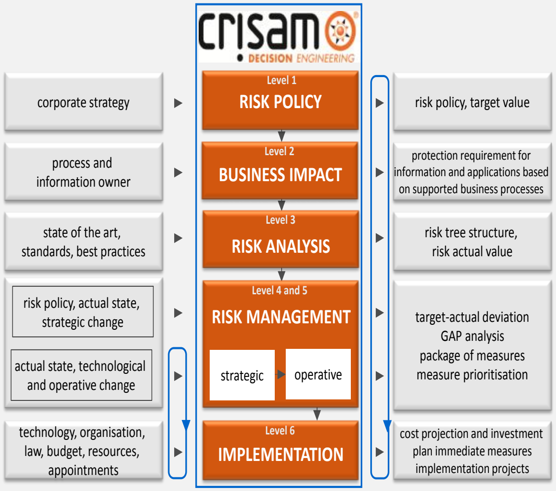
POLICY & STANDARDS

TECHNICAL INFO SEC

- ***Facts & Figures 2012:***
  7000 IT technical audits done;
  45 Risk Assessments for critical IT Services done
  600 measures addressed
  150 BIA awareness sessions top management done;
  160 detailed BIA interviews done

Risk Management Focus 2013 (central computing)

- **Business Impact Analysis**
- **Risk Analysis**
- **Risk Management**
- **Measure Implementation**



crisam DECISION ENGINEERING

corporate strategy → Level 1 RISK POLICY → risk policy, target value

process and information owner → Level 2 BUSINESS IMPACT → protection requirement for information and applications based on supported business processes

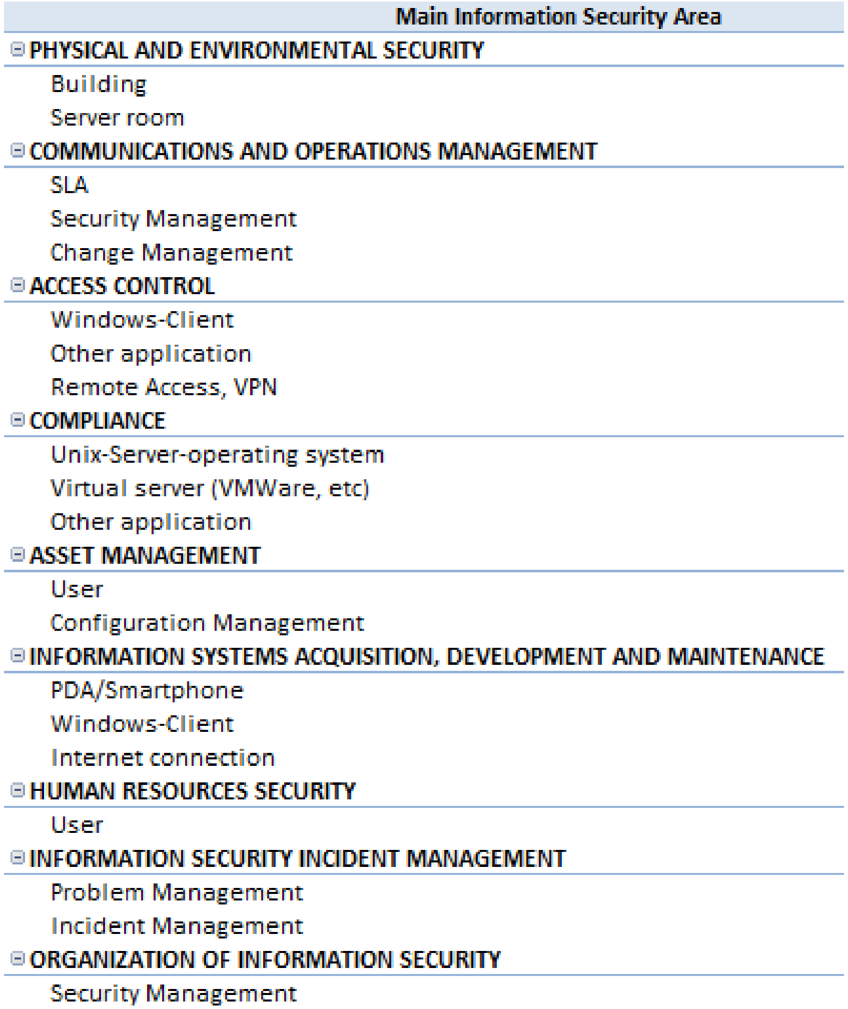
state of the art, standards, best practices → Level 3 RISK ANALYSIS → risk tree structure, risk actual value

risk policy, actual state, strategic change → Level 4 and 5 RISK MANAGEMENT → target-actual deviation GAP analysis package of measures measure prioritisation

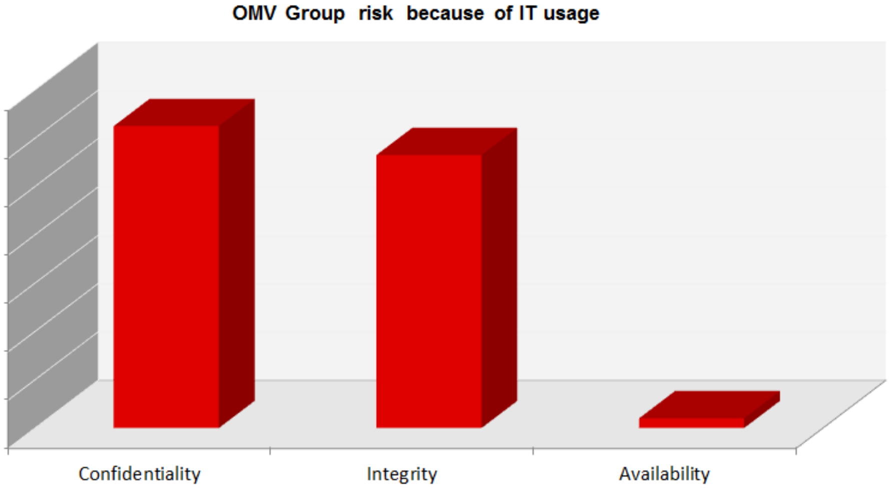
actual state, technological and operative change → strategic → operative

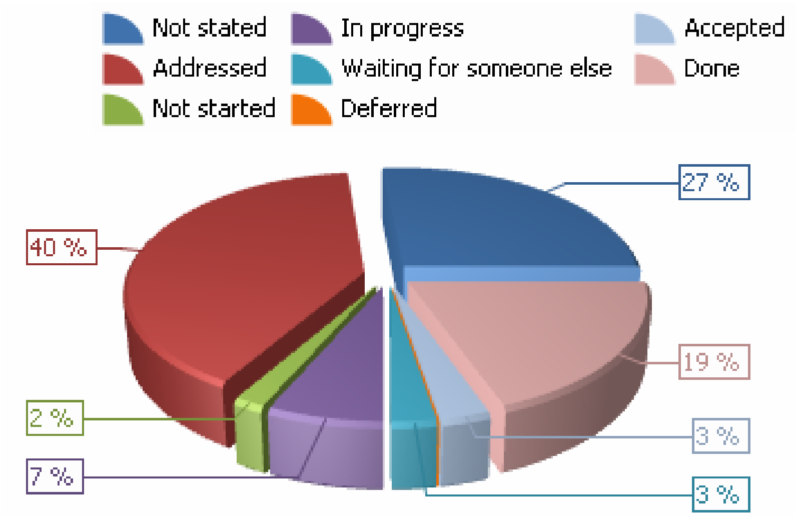
technology, organisation, law, budget, resources, appointments → Level 6 IMPLEMENTATION → cost projection and investment plan immediate measures implementation projects

Examples of areas with highest risk



Main Information Security Area
⊟ PHYSICAL AND ENVIRONMENTAL SECURITY
Building
Server room
⊟ COMMUNICATIONS AND OPERATIONS MANAGEMENT
SLA
Security Management
Change Management
⊟ ACCESS CONTROL
Windows-Client
Other application
Remote Access, VPN
⊟ COMPLIANCE
Unix-Server-operating system
Virtual server (VMWare, etc)
Other application
⊟ ASSET MANAGEMENT
User
Configuration Management
⊟ INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
PDA/Smartphone
Windows-Client
Internet connection
⊟ HUMAN RESOURCES SECURITY
User
⊟ INFORMATION SECURITY INCIDENT MANAGEMENT
Problem Management
Incident Management
⊟ ORGANIZATION OF INFORMATION SECURITY
Security Management





Ensure Information Security Management System

Safeguarding information according to its protection requirements

2012 | 2013 | 2014

RISK MANAGEMENT

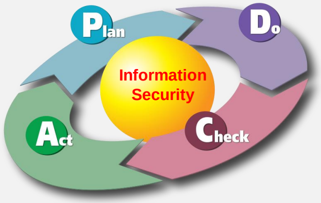
MANAGEMENT SYSTEM

POLICY & STANDARDS

TECHNICAL INFO SEC

Management System Focus 2013 (central computing)

- **Plan Do Check Act** steering and quality assurance
- **ISO 27001** annual certification support
- **Awareness increase**
  - Portal
  - Trainings
  - Info Screens
  - Newsletter
  - Promotion virtual training
  - „Exhibition booth“ (high level topics, Live Demos, non-technical focus, private focus, etc..)
- **Networking** with security relevant organisations (BKA, CERT, AkSiGo, Sec Researchers, Engergy Sector Companies



Ensure Information Security Policy Methods & Standards

Safeguarding information according to its protection requirements

2012 | 2013 | 2014

RISK MANAGEMENT

MANAGEMENT SYSTEM

POLICY & STANDARDS

TECHNICAL INFO SEC

Policy Methods & Standards Focus 2013 (central computing)

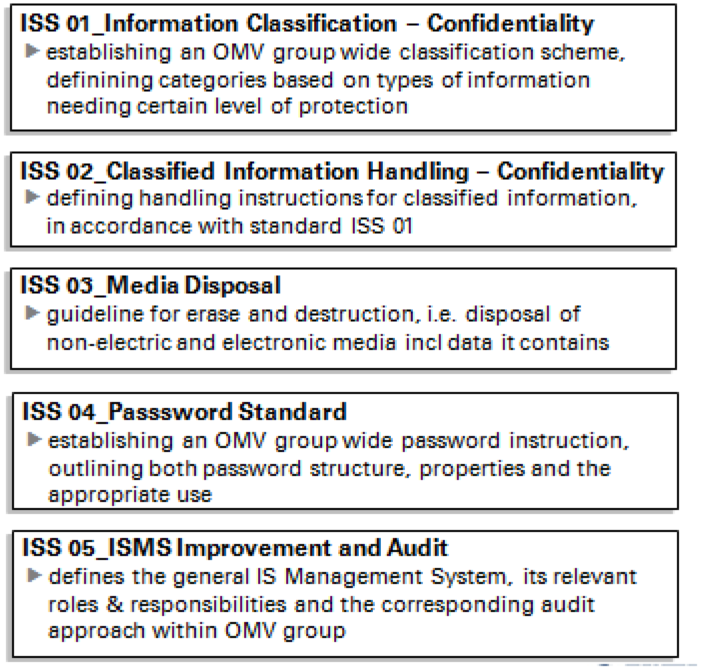
- **Standards:**
  Revamping and consolidation of existing IT and security standards in functional alignment with new IT strategy (at present 47 standards to be revised);
- **PCI Assessment:**
  Ensuring successful Payment Card Industry Data Security Standard (PCI DSS)
- **IS Training:**
  Enhancing the Virtual Training Platform regarding both function and content
- **AD-Hoch measures:**
  Responding to short-term emerging legal or business requirements by releasing corresponding regulatory documents (i.e. work instructions)

Ensure Information Security Policy Methods & Standards

Examples

Defining group wide, high level Standards for Information Security

Standards
(Examples)



ISS 01_Information Classification – Confidentiality
- establishing an OMV group wide classification scheme, definining categories based on types of information needing certain level of protection

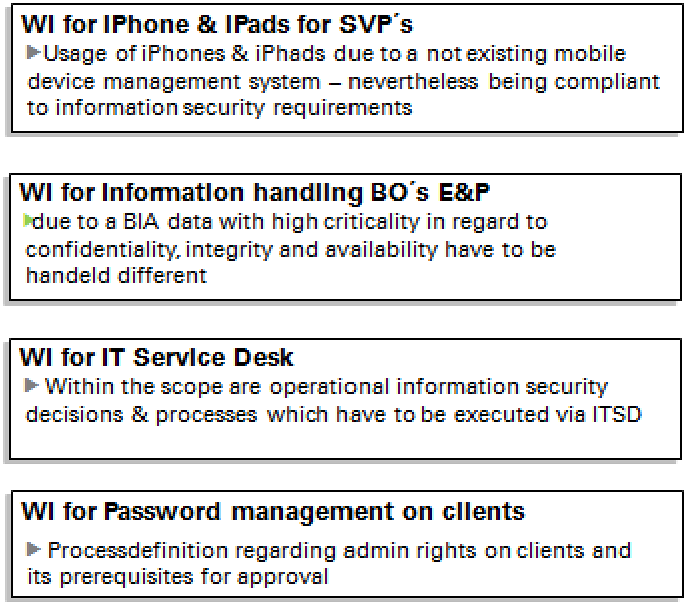
ISS 02_Classified Information Handling – Confidentiality
- defining handling instructions for classified information, in accordance with standard ISS 01

ISS 03_Media Disposal
- guideline for erase and destruction, i.e. disposal of non-electric and electronic media incl data it contains

ISS 04_Passsword Standard
- establishing an OMV group wide password instruction, outlining both password structure, properties and the appropriate use

ISS 05_ISMS Improvement and Audit
- defines the general IS Management System, its relevant roles & responsibilities and the corresponding audit approach within OMV group

Working instructions
(Examples)



WI for IPhone & IPads for SVP´s
- Usage of iPhones & iPhads due to a not existing mobile device management system – nevertheless being compliant to information security requirements

WI for Information handling BO´s E&P
- due to a BIA data with high criticality in regard to confidentiality, integrity and availability have to be handeld different

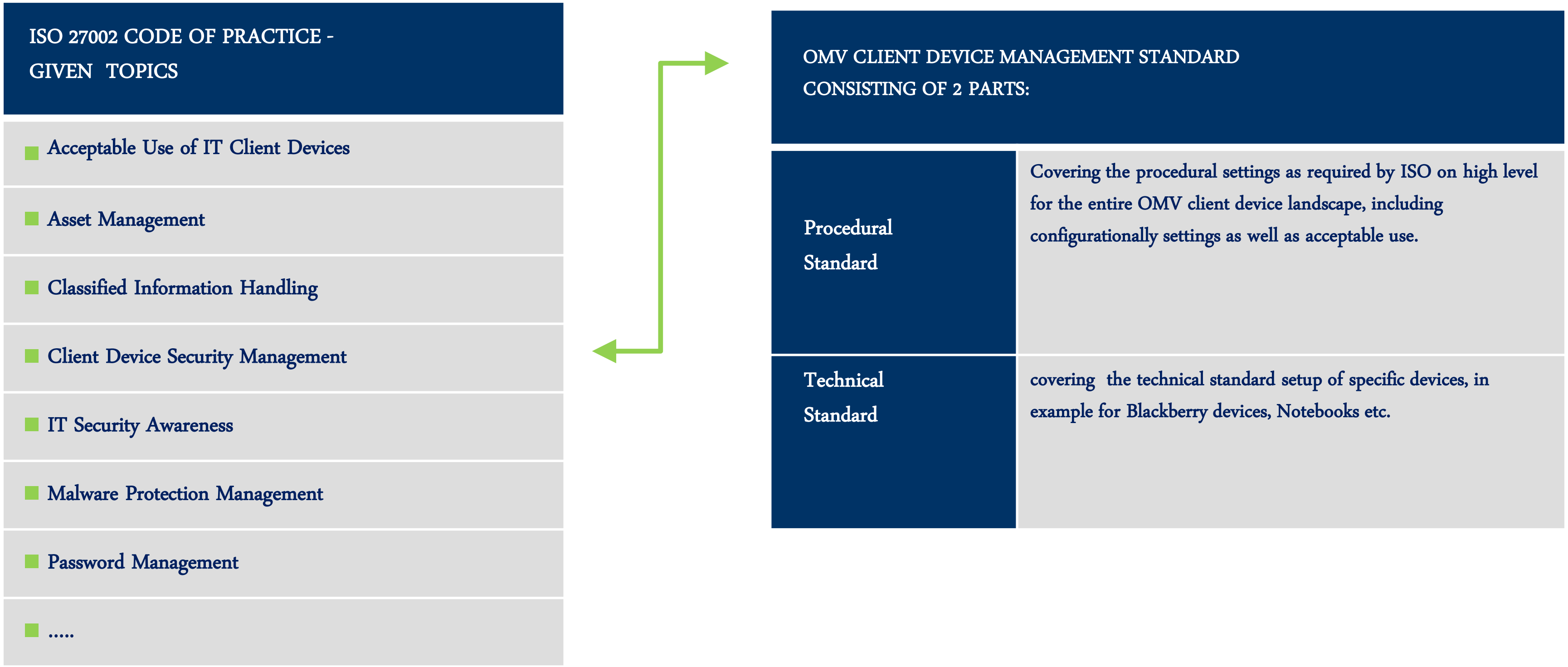
WI for IT Service Desk
- Within the scope are operational information security decisions & processes which have to be executed via ITSD

WI for Password management on clients
- Processdefinition regarding admin rights on clients and its prerequisites for approval

Ensure Information Security Policy Methods & Standards

Best practise

Transferring the code of practice from ISO 27k into standardisational guidelines based on a feasible approach by considering business needs and general workability aspects



ISO 27002 CODE OF PRACTICE -
GIVEN TOPICS

- Acceptable Use of IT Client Devices
- Asset Management
- Classified Information Handling
- Client Device Security Management
- IT Security Awareness
- Malware Protection Management
- Password Management
- .....

OMV CLIENT DEVICE MANAGEMENT STANDARD
CONSISTING OF 2 PARTS:

Procedural Standard	Covering the procedural settings as required by ISO on high level for the entire OMV client device landscape, including configurationally settings as well as acceptable use.
Technical Standard	covering the technical standard setup of specific devices, in example for Blackberry devices, Notebooks etc.

Ensure Technical Information Security

Safeguarding information according to its protection requirements

2011 | 2012 | 2013

RISK MANAGEMENT

MANAGEMENT SYSTEM

POLICY & STANDARDS

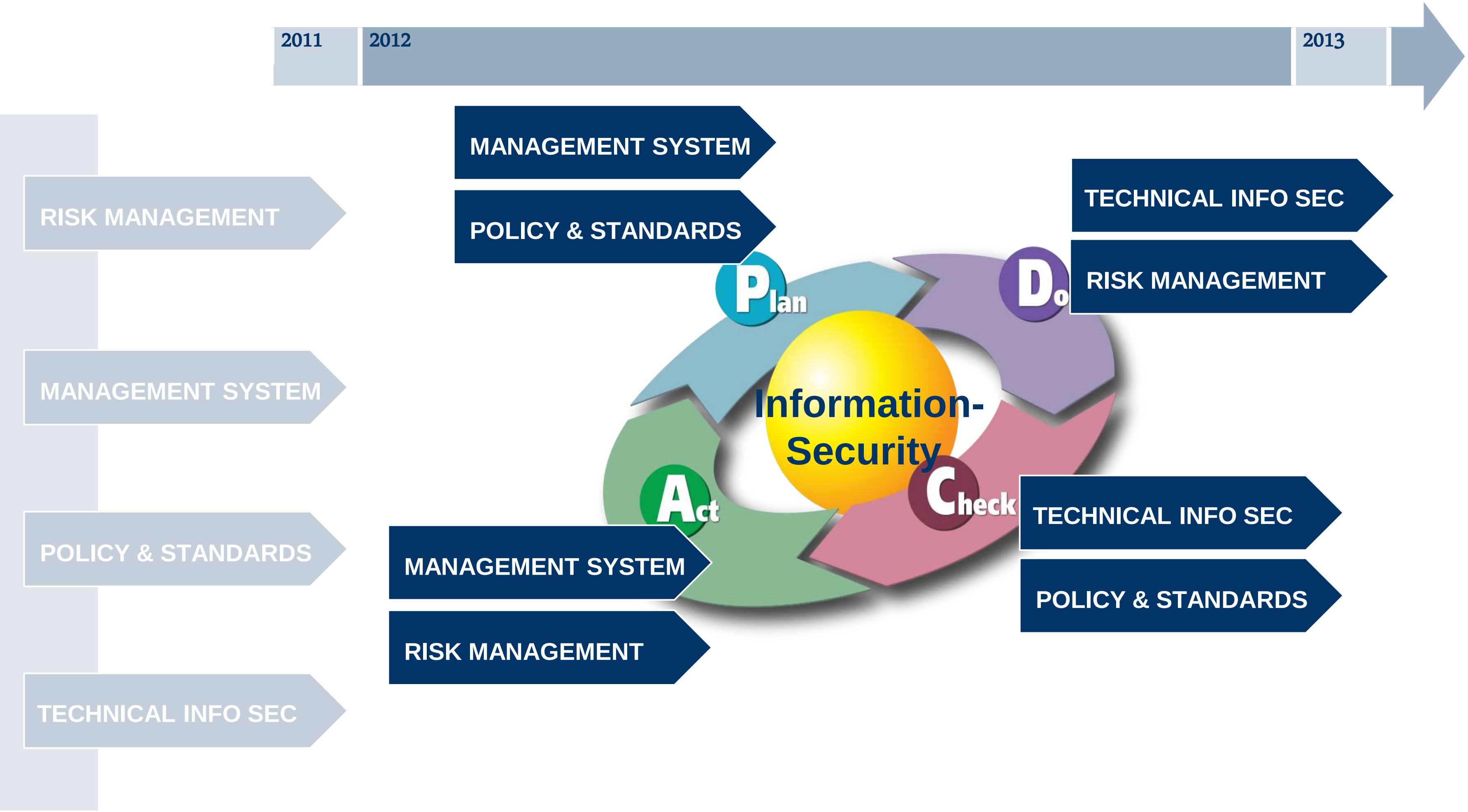
TECHNICAL INFO SEC

Technical Information Security Focus 2013 (central computing)

- **Project support and implementation e.g.:**
  - Mobile Device Management
  - Win7 Bit Locker
  - Unified Access Gateway
  - Identity & Access Management System
  - Web Application Firewall
  - MS Direct Access
  - Global Vulnerability Management-
- **Reporting and auditing mechanism**
- **Organisational interaction** with OGS to be enhanced

Ensure Information Security by the PDCA cycle

Safeguarding information according to its protection requirements



RISK MANAGEMENT

MANAGEMENT SYSTEM

POLICY & STANDARDS

TECHNICAL INFO SEC

MANAGEMENT SYSTEM

POLICY & STANDARDS

TECHNICAL INFO SEC

RISK MANAGEMENT

TECHNICAL INFO SEC

POLICY & STANDARDS

MANAGEMENT SYSTEM

RISK MANAGEMENT

AGENDA

- OMV GROUP, ORGANIZATION
- DISCIPLINES
- AWARENESS

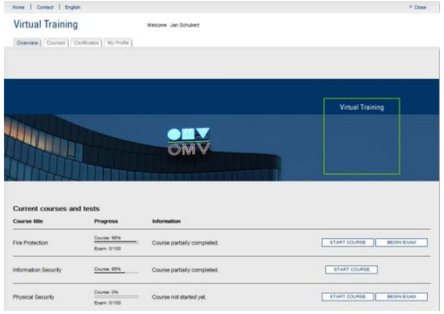
Awareness within OMV Group

Awareness with a virtual training

Creating Awareness by empowering the Virtual Training Platform

http://vtc.omv.com

- Interactive course about Information Security, available in the Intranet
- Possibility to get a certificate
- Intended to integrate the virtual training mandatorily in the personal performance and development cycle (PDS)



Virtual Training

Welcome Jan Schubert

Virtual Training

Current courses and tests

Course title	Progress	Information	
Fire Protection	Course: 95% Exam: 0/100	Course partially completed.	START COURSE BEGIN EXAM
Information Security	Course: 60%	Course partially completed.	START COURSE
Physical Security	Course: 0% Exam: 0/100	Course not started yet.	START COURSE BEGIN EXAM

Handling
Security Incidents
Entrance area

Danger Spot
Telephone and Fax
Data Backup

Information Security is more than just IT Security

Information Security Day 2012

Ensure Information Security

Safeguarding information according to its protection requiremen

IT and non-IT

There was a story about 4 people named Everybody, Somebody, Anybody and Nobody.

There was an important job to be done and Everybody was sure that Somebody would do it.

Anybody could have done it, but Nobody did it.

Now when Somebody got angry about that, because it was Everybody's job, Everybody thought Anybody could do it, but Nobody realized that Everybody would not do it.

It ended up that Everybody blamed Somebody when Nobody did what Anybody could have done!

Sec_rity is not complete without U!

Finally

THANK YOU FOR YOUR ATTENTION!

OR IN THE WORDS OF A MAGPIE:

Questions?