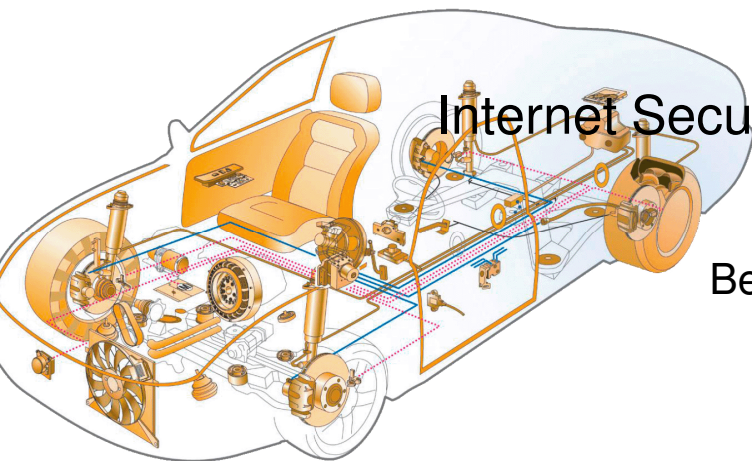




Managing Security as an Innovation Driver



Internet Security Days 2011 – Brühl 13.-15. Sept 2011

Bernhard Thomas (CTO), Thomas Ullrich (CSO)

Continental Corporation

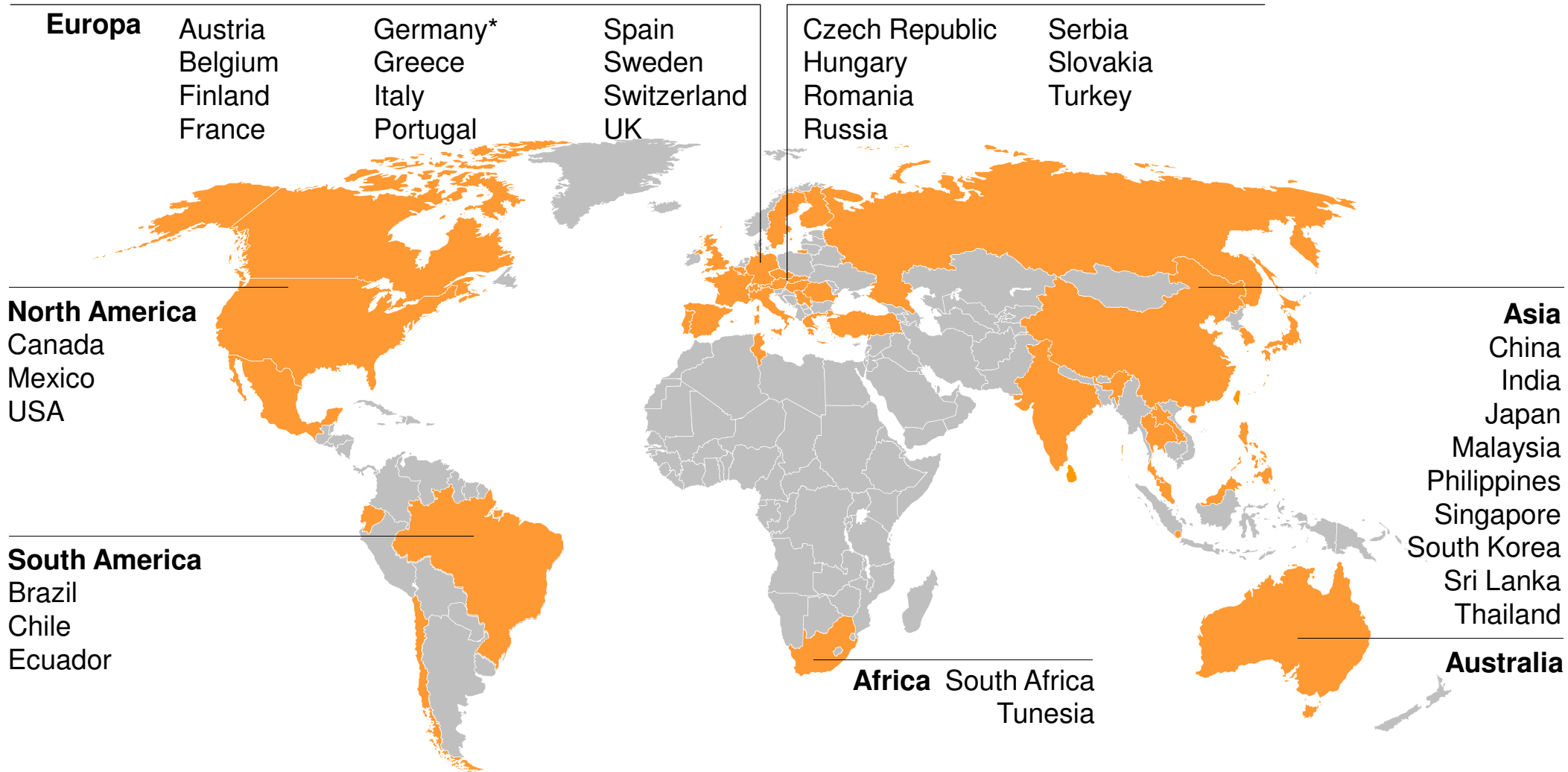
Our Vision

- ▶ We make individual mobility safer, more comfortable, and more sustainable
- ▶ Performance is our passion
- ▶ Creating value is our driving force



Continental Corporation

193 Production and R&D Locations in 37 Countries



*Headquarters in Hanover

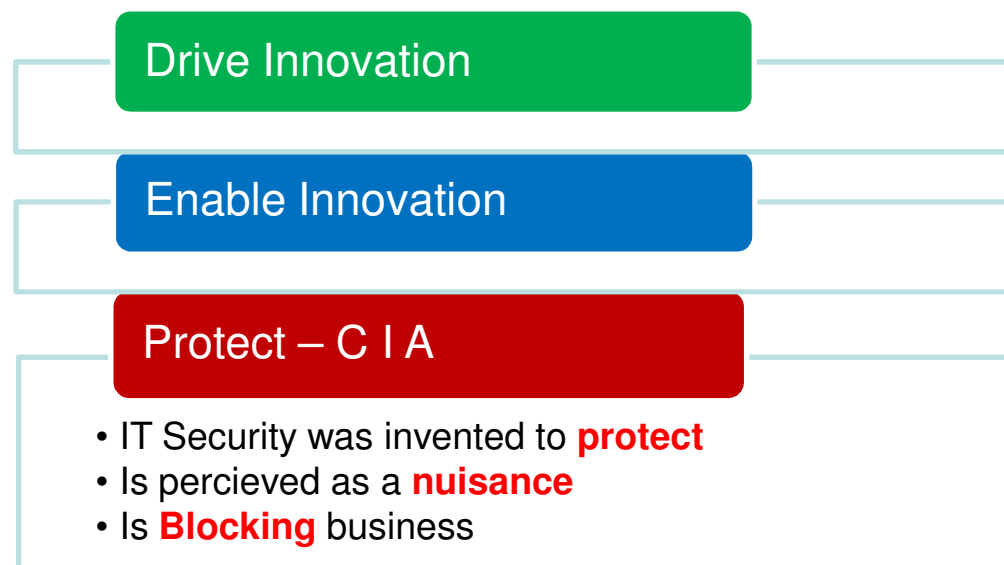
Status: January 1, 2011

Managing Security as an Innovation Driver – Overview

- Continental – we make individual mobility safer, more comfortable, and more sustainable
- “What do you mean – Innovation Driver?”: Positioning IT Security
- A change of perspective: From Threat view to Business view
- Discussion of examples from past to future
- How to make Security effective as Innovator / Enabler

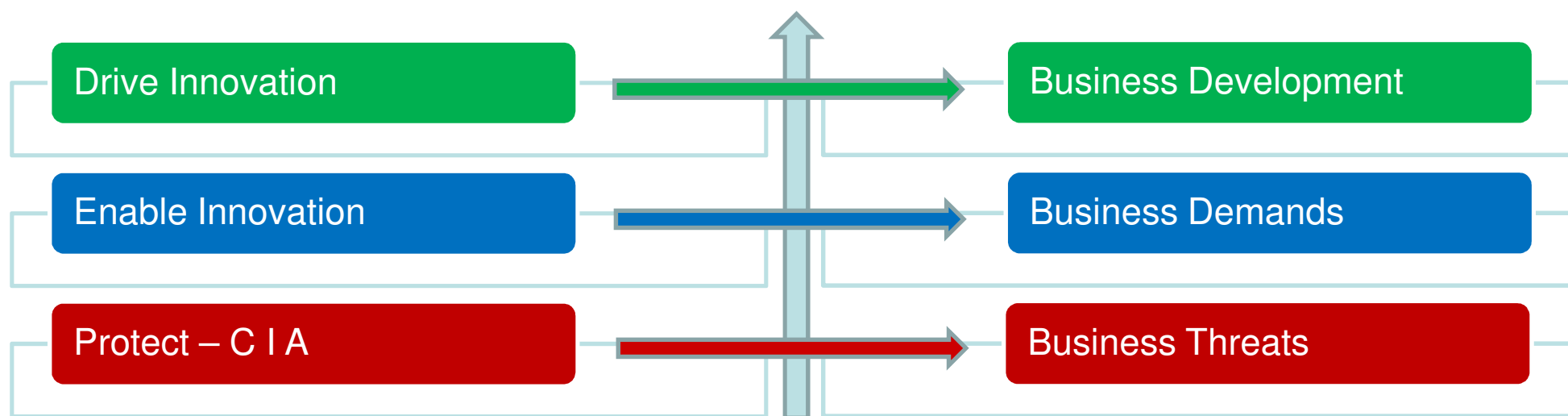
What Do you Mean - Innovation Driver?

- IT Security was invented to **protect** – CIA (C – Confidentiality, I – Integrity, A – Availability)
 - IT Security is highly valued, in principle, but perceived as **nuisance** when the user is exposed to protection measures
 - Careful protection is more often than not experienced as **blocking** the dynamic business
- How can IT Security be an **Innovation Driver**?



How Can IS be an Innovation Driver? - A Change of Perspective

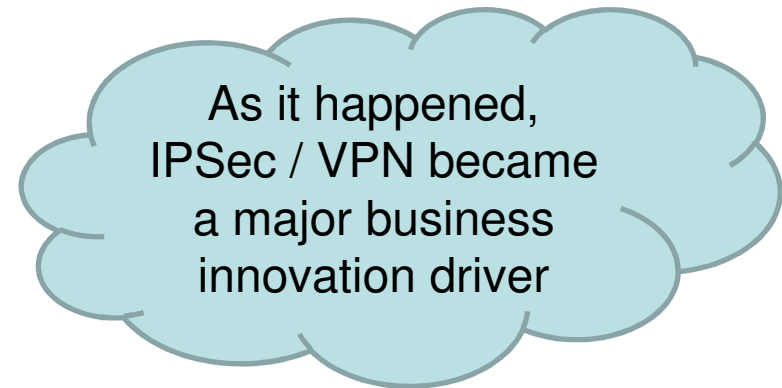
After all, IS is not only about Protection
– IS is about Technology, too



Pretty Abstract – What About Examples?

An example from the past (the 90's): **IPSec / VPN**

- **Protection Technology:** VPN techniques were developed in IT Security to protect data streams on their way through public, unencrypted networks
- **Use:** VPN created a burst in home office and mobile use
- **Business Impact:** VPN created an attractive alternative to join (new) company locations to the company network, or partners, customers to company resources



As it happened,
IPSec / VPN became
a major business
innovation driver

IS Innovation Driver – More Examples, Even from the Future

Digital Identity

- Protection Technology: PKI, Digital Signature, Secure Authentication.....
- Use: **One**, officially granted, ID rather than many spread over devices and sources
- Business Impact: Business over Internet, Cloud Service consumption, Community access



Private use / Business use

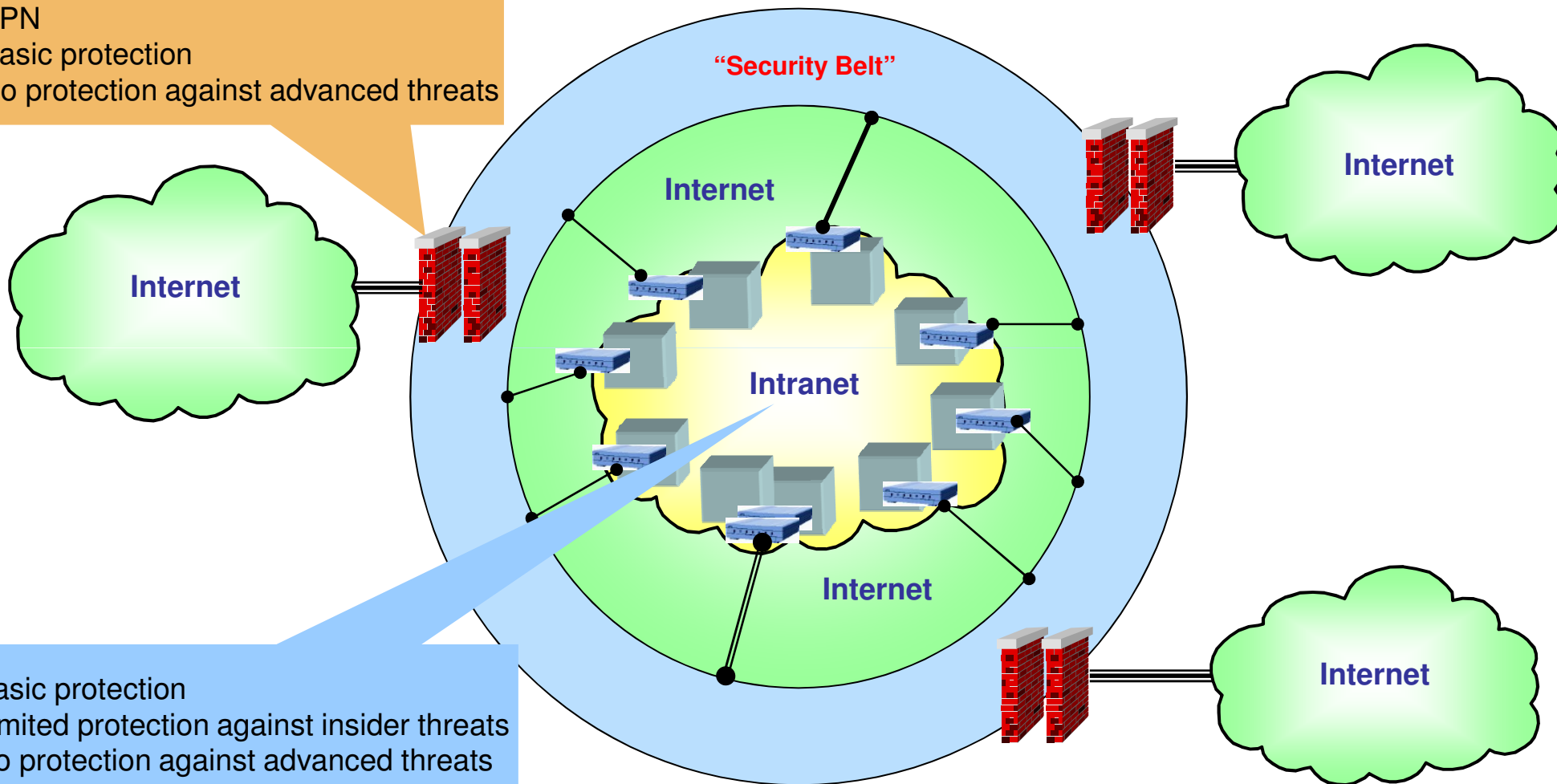
- Protection Technology: Encryption, Device Management (e.g. uniform security settings), Client Virtualization, Sandboxing...
- Use: Use same device, or any device, for private **and** for business application
- Business Impact: Business-Life-Balance integration, Business mobilization



Next stop:
De-perimetrization ?

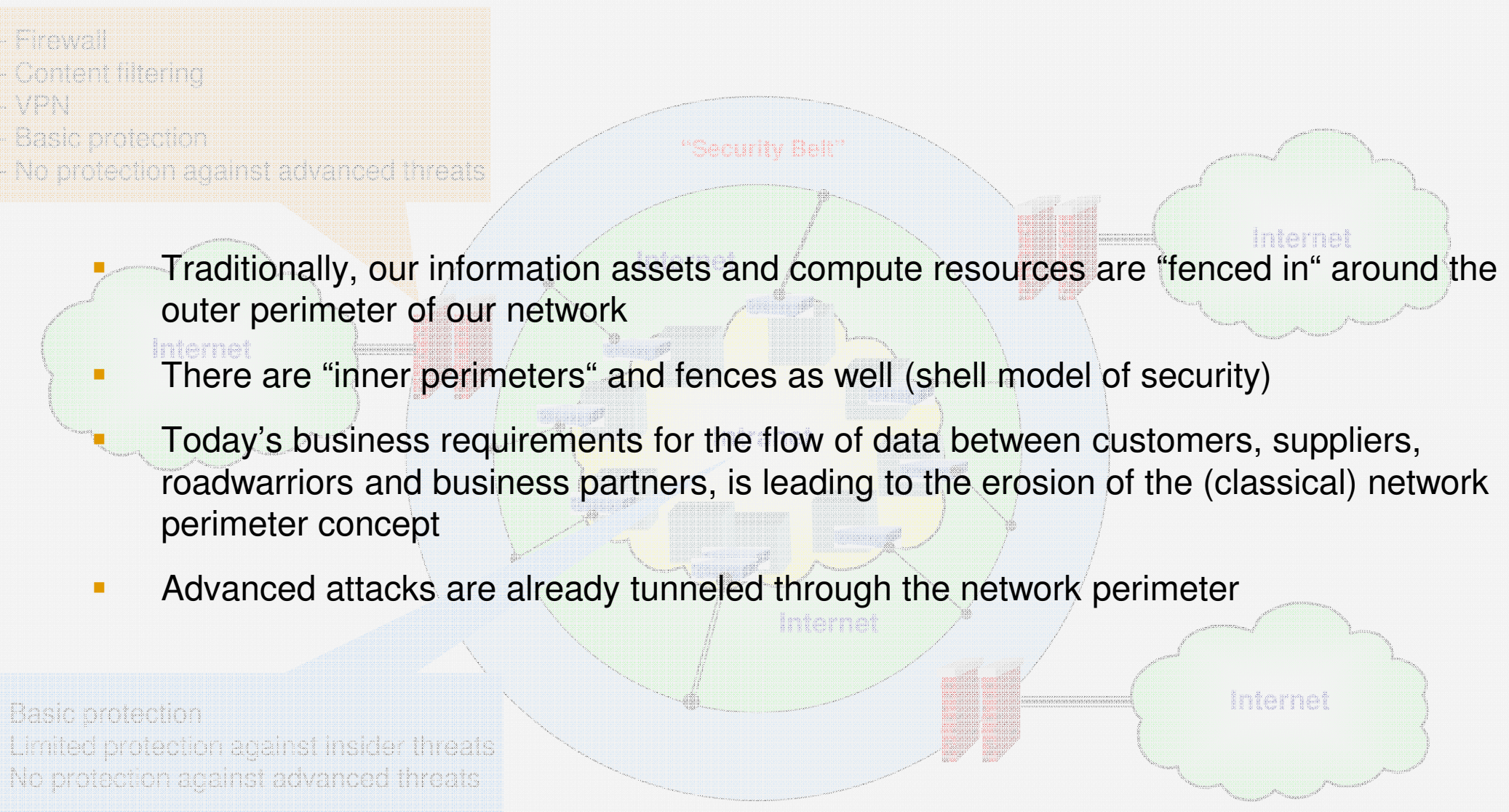
IS - The world we know (Perimeters in the CIAS Model)

- Firewall
- Content filtering
- VPN
- Basic protection
- No protection against advanced threats

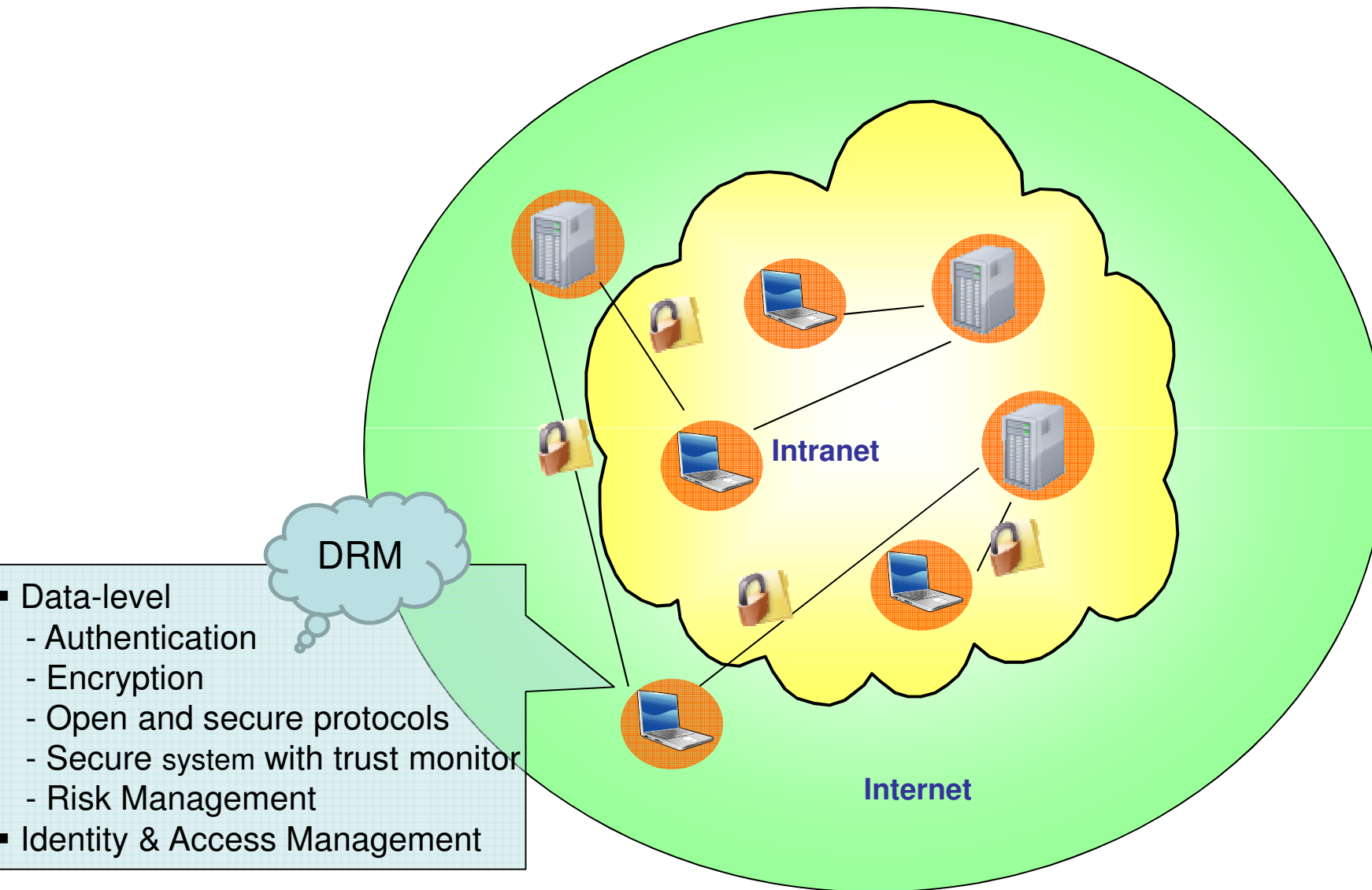


Basic protection
Limited protection against insider threats
No protection against advanced threats

IS - The world we know (Perimeters in the CIAS Model)



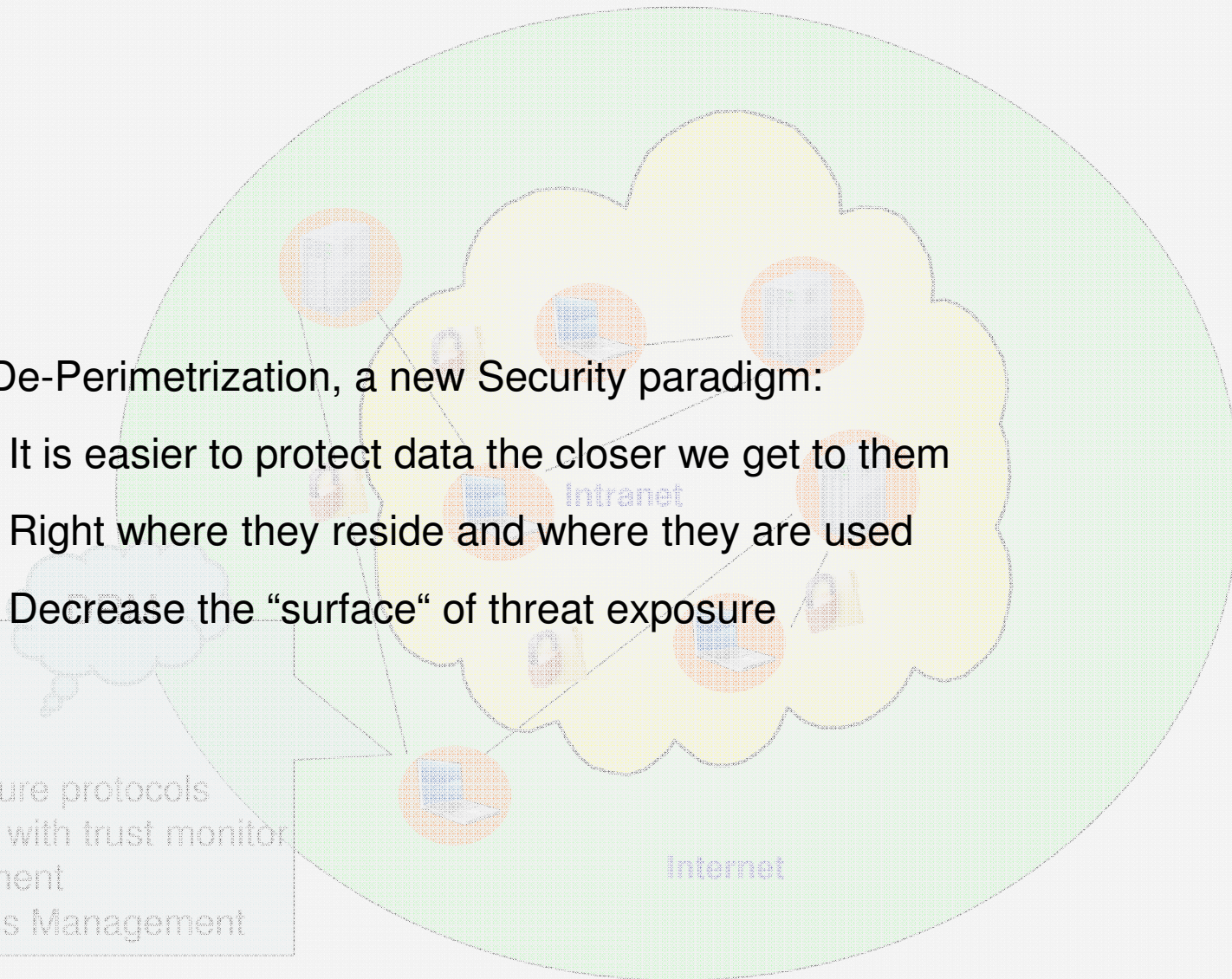
So ... Tear Down the Walls? – The De-perimeterized Network



So ... Tear Down the Walls? – The De-perimeterized Network

- De-Perimetrization, a new Security paradigm:
 - It is easier to protect data the closer we get to them
 - Right where they reside and where they are used
 - Decrease the “surface“ of threat exposure

- Data-level
 - Authentication
 - Encryption
 - Open and secure protocols
 - Secure system with trust monitor
 - Risk Management
- Identity & Access Management



De-Perimetrization - An Innovation Driver?

- Imagine a world with a de-perimeterized collaboration oriented architecture, where
 - Carve-in/carve-out-activities are no longer excessive projects
 - Joint ventures are not held back by IT integration and Security issues
 - Business partner integration is not a big project anymore
 - Makes a Collaboration Oriented Business Architecture much easier to implement

- And at the same time lets the CSO sleep well, i.e., WITHOUT compromising security

How to Make Security an Effective Enabler / Innovator

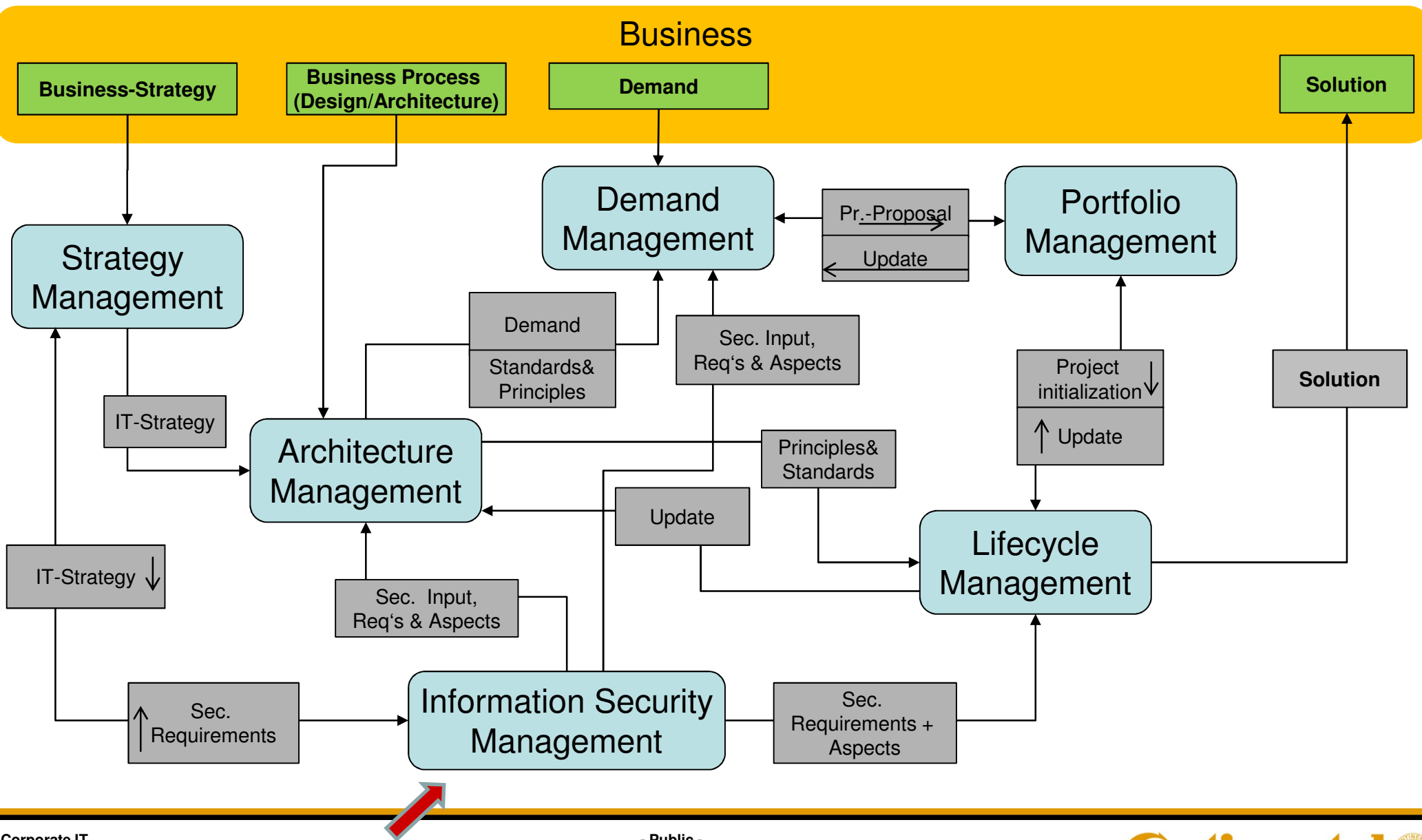
Three roads to manage IS as an effective Business Enabler / Innovator – at a glance

- ❑ IS built-in into top level IT Processes
- ❑ IS embedded in Service Architecture
- ❑ IS integrated into Service Life Cycle

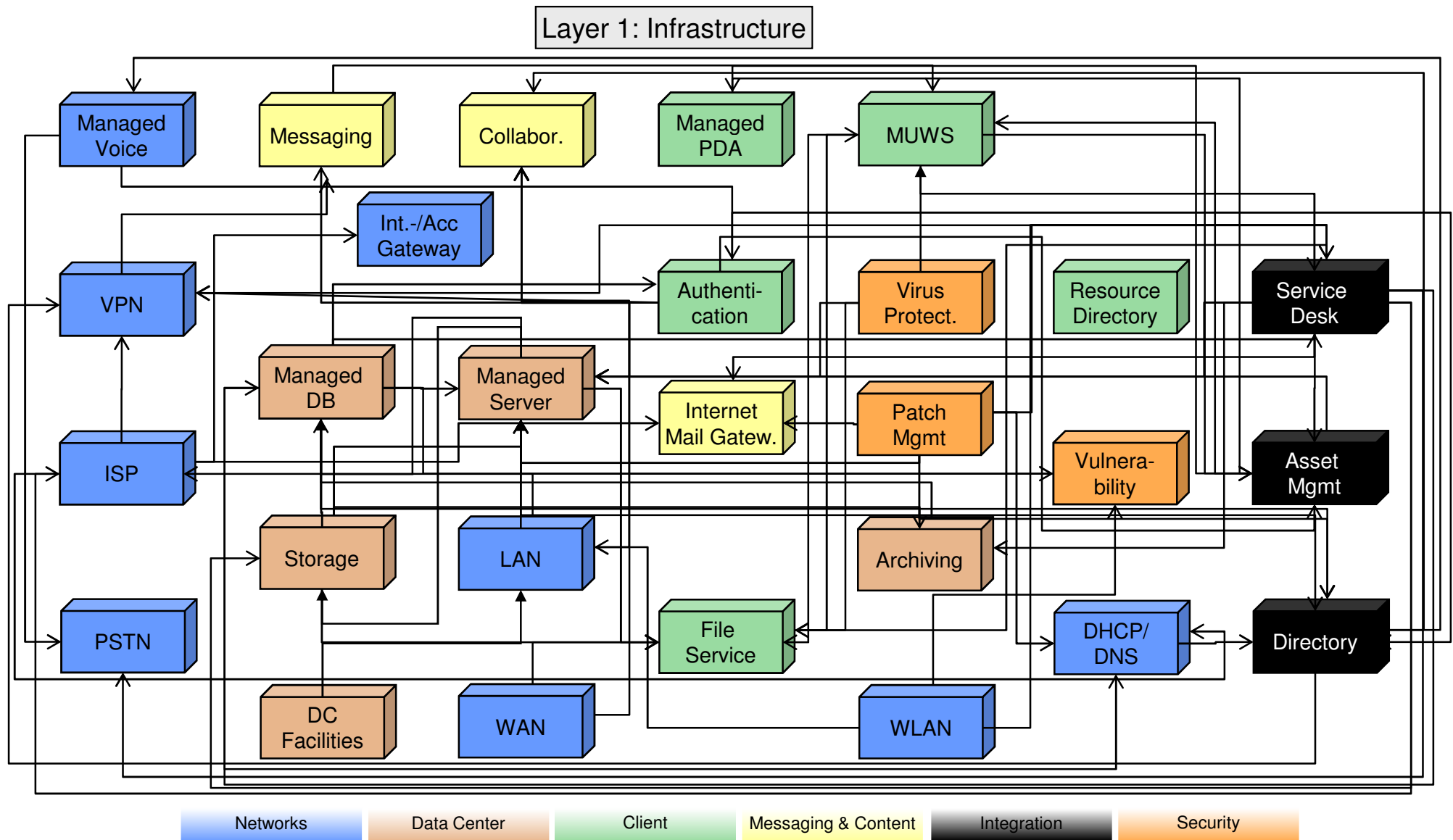


Remember, IS is not only about Protection & Policies – IS is about Technology, too

IS Management – Part of IT Processes Integrated Framework



Infrastructure Services at Continental IT



IS Embedded in Service Architecture

- Operational security defined as (Infrastructure) Services
 - Part of Service Architecture, hence have “Consumers“
 - Subject to Service Life Cycle Management
 - Security technology part of / turned into Service
- Security Management embedded in other Services
 - Security technologies as part of the employed technology
 - Security metrics defined and measured, similar to SLs / KPIs, per Service
 - Subject to Service Life Cycle Management
 - Service specific security screening for Risk Management

Excerpt From Service Description: Sec Metrics in Managed DB - MSSQL

EAM - Service Description: "Managed DB - MSSQL - SCEE" - Windows Internet Explorer

http://eam.conti.de/EAM/ServiceDescriptions_Details.iws?sp5=8&sfpgo=8&sfpgn=8&sfid=1:0:9&KeyAttribute=%7BBE876743-56B1-4CA0-82CB-718763FF7554%7D&PrimaryIr

EAM - Service Description: "Managed DB - MSSQL - SC..."

- Upward Interfaces
- Supported Services
- Downward Interfaces
- Required Services
- Derived from
- Service Parameters
- Costs
- Processes
- Roles
- Required Skills
- All Documents
- Software
- Org. Units / Locations

Actions

- Edit Service Description
- Delete Service Description
- Compare Service
- Show Roles / Staffs
- Mark as Target Service
- Implement Role
- New Service Element
- New Sourcing
- Constraint
- New Cost Element
- New Process
- Require Document
- New Document
- New Security Screening
- New ISD from GSD
- New ISD from ISD
- New GSD from GSD
- New Generic Service
- New Application Service
- Add Comment
- Create Favorite

Attended Operation Time	Value			
Attended Operation Time	5 x 10			
On call	7 x 24	follow the sun		
Operation Time	7 x 24	excl. maintenance windows		
Support	7 x 24			

Service Level / KPI (3 Service Elements)

Name	Value			
Availability	99.99	SLA Servicehours Availability per month max. Downtime		
		7 x 24	99,99%	2h

Av in % = (Hrs-Main-Out)/(Hrs-Main)*100

Hrs : = number of hours operation time per month (7x24)
Main : = number of hours agreed maintenance time per month
Out : = number of hours unscheduled downtime per month
Av : = Service availability, available uptime

Response time	Value			
Response time	2h			
Time to fix	xx	Max. duration [h]	Priority	Impact
		1	S	Top side / organization affected
		4	A	High department affected
		16	B	Medium group / unit affected
		40	C	Low 1 person affected

Security Metrics (6 Service Elements)

Name	Value			
Coverage	98%	Security Item: Database Backup		
		Type: Coverage		
		Units of Measure: Percentage of Systems		
		Target Value: 98%		
		Description: the percentage of databases that are backed up on a regular basis in accordance with the policy (at least full database backup weekly, incremental daily if not otherwise defined for the database due to other security requirements). The number of databases with regular database backups divided by the total number of databases.		
		Objective: to measure the extent to which the backup policies are being enforced.		
		Formula:		
		Source: Monitoring by database script and analysis by Reporting Services		
		Frequency of measurement: monthly		
		Owner Security Office: Marianne Trombke		
Coverage	100%	Security Item: Public Account Security		
		Type: Coverage		
		Units of Measure: Percentage of Systems		
		Target Value: 100%		
		Description: the number of databases having the GUEST account disabled (except tempdb) divided by the number of total databases		
		Objective: to ensure authorized user access and to prevent unauthorized access to information systems		
		Formula:		
		Source: Monitoring by database script and analysis by Reporting Services		
		Frequency of measurement: monthly		
		Owner Security Office: Marianne Trombke		
Coverage	2%	Security Item: Critical Function Privileges		
		Type: Coverage		

Database Backup

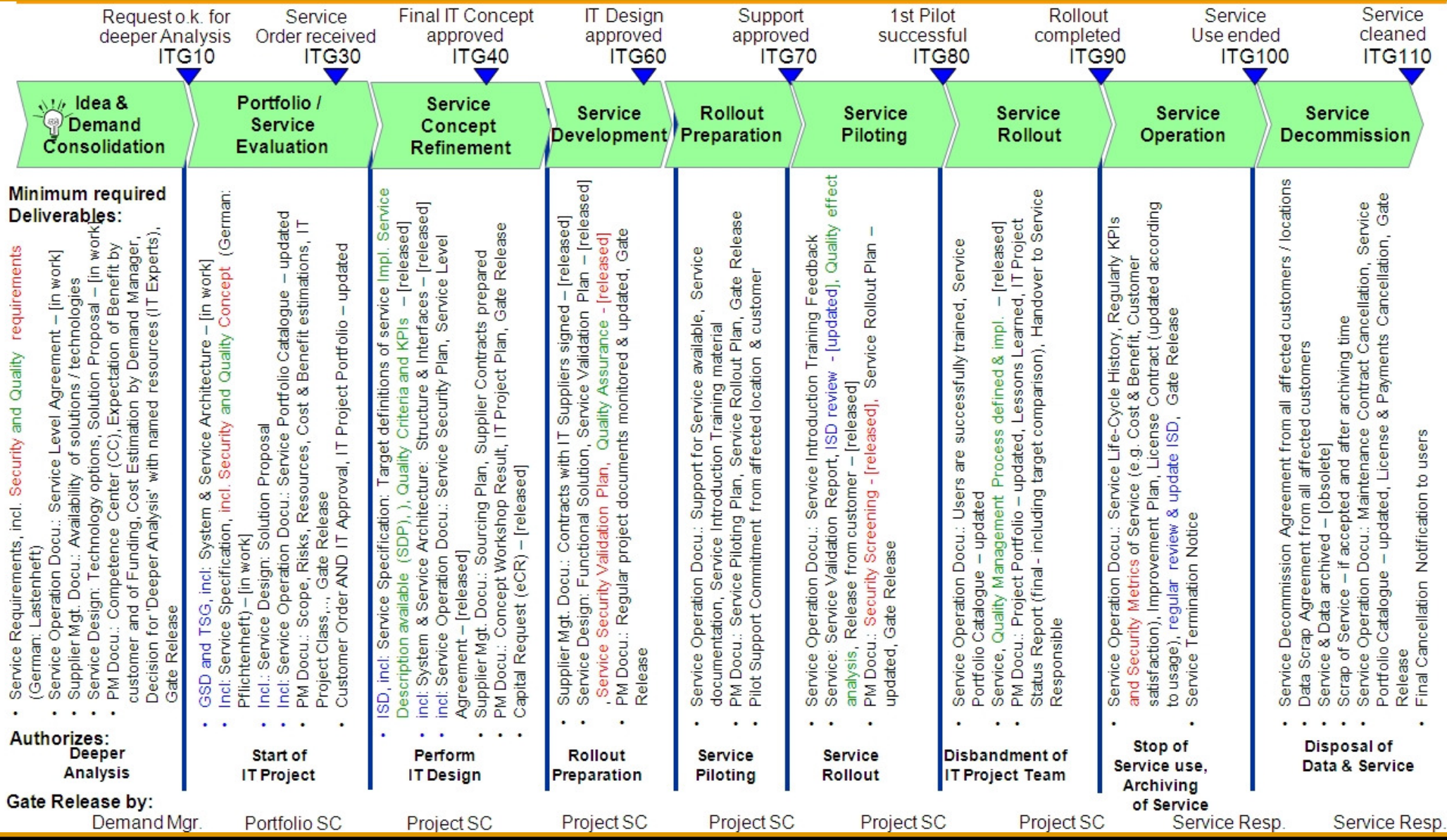
Public Account Security

Critical Function Privileges

Fertig

Vertrauenswürdige Sites 100%

SI Integrated Into Service Life Cycle



Innovation Ahead! Drive safely!

Thank you