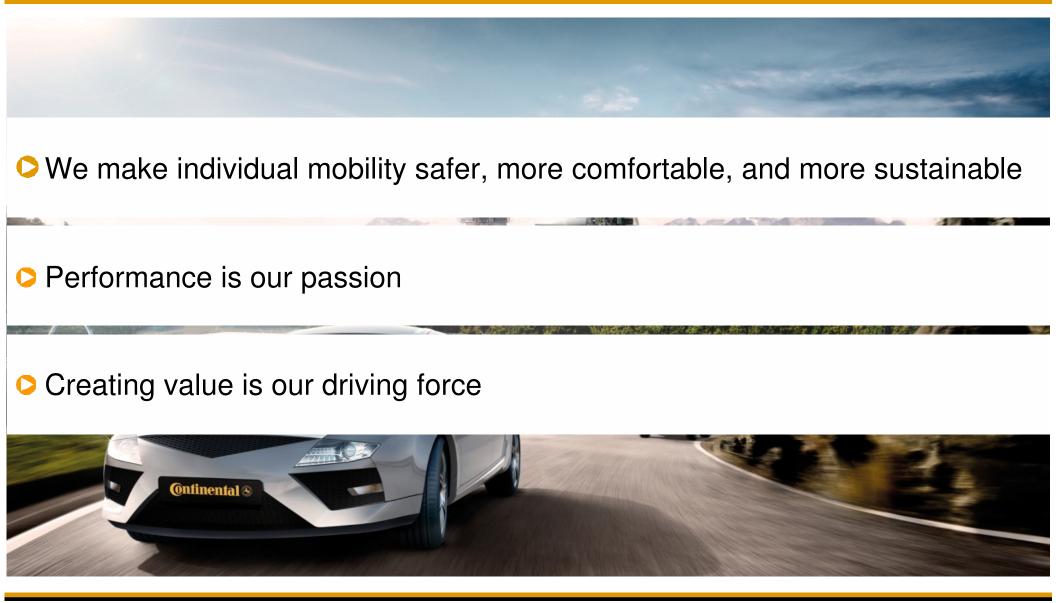


#### **Managing Security as an Innovation Driver**

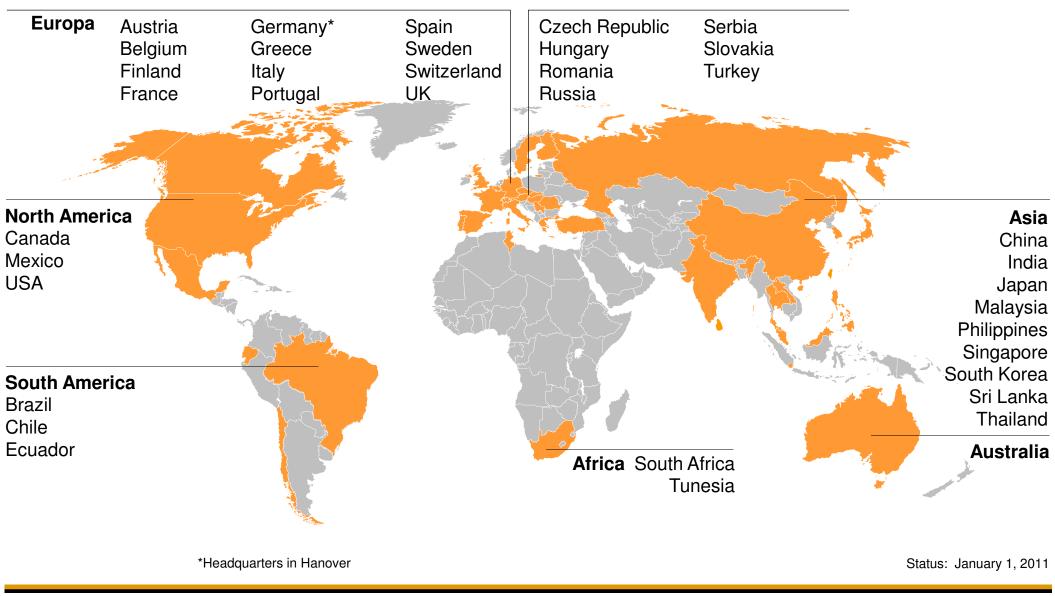


Bernhard Thomas (CTO), Thomas Ullrich (CSO)





### Continental Corporation 193 Production and R&D Locations in 37 Countries





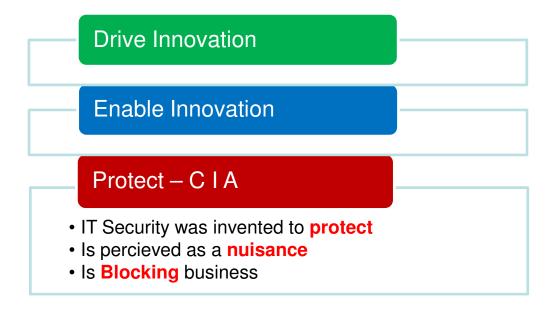
## Managing Security as an Innovation Driver – Overview

- 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



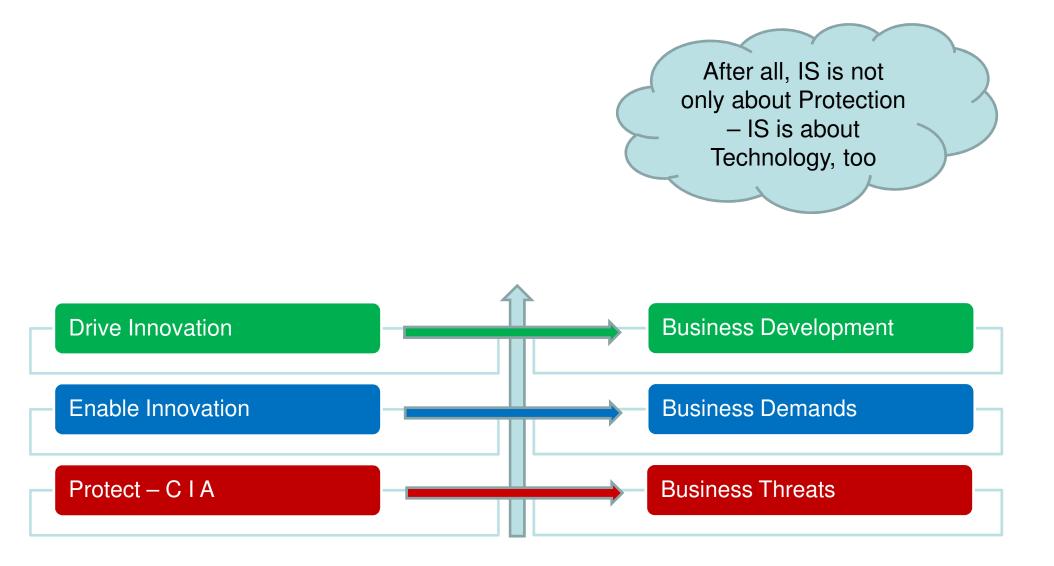
### What Do you Mean - Innovation Driver?

- IT Security was invented to protect CIA (C Confidentiality, I Integrity, A Availability)
- IT Security is highly valued, in principle, but percieved 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





#### **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





## 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

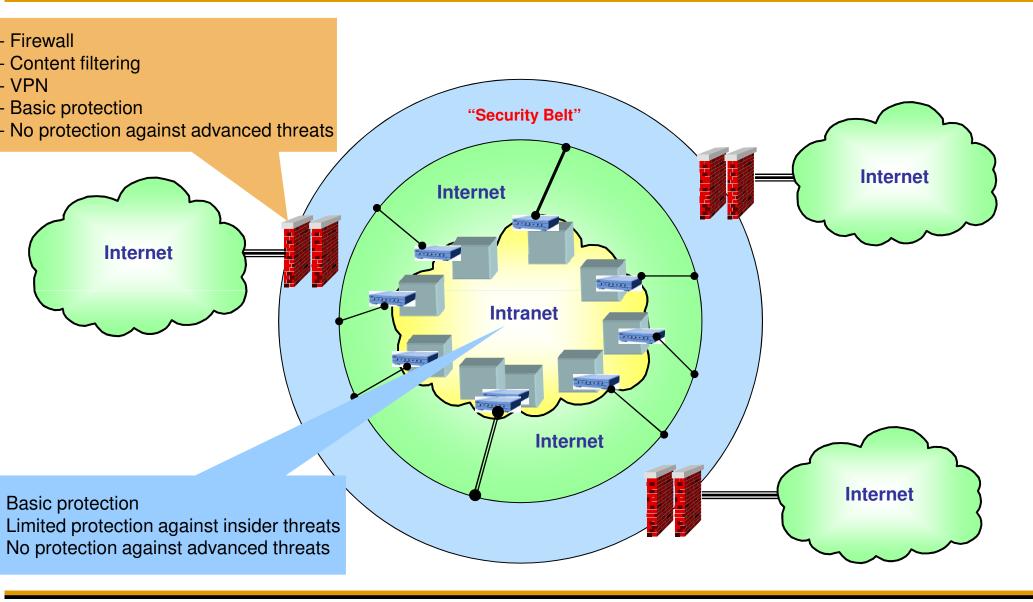








## **IS - The world we know (Perimeters in the CIAS Model)**



Corporate IT Infrastructure & Security Strategy



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

- Firewall
- Content filtering
- . VPN
- Basic protection

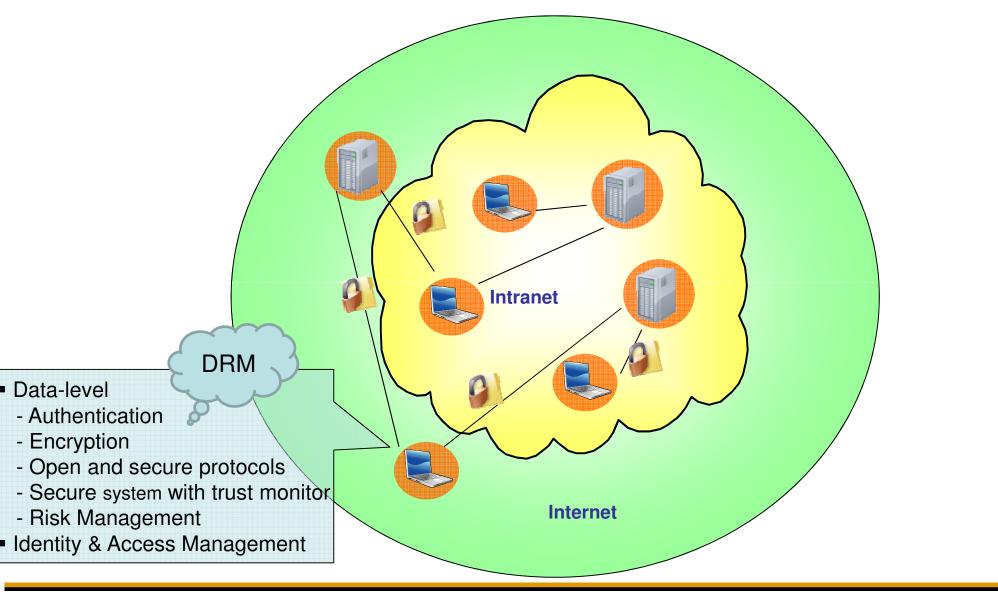
- No protection against advanced threats
  - Traditionally, our information assets and compute resources are "fenced in" around the outer perimeter of our network
    - There are "inner perimeters" and fences as well (shell model of security)
  - Today's business requirements for the flow of data between customers, suppliers, roadwarriors and business partners, is leading to the erosion of the (classical) network perimeter concept
  - Advanced attacks are already tunneled through the network perimeter

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



Corporate IT Infrastructure & Security Strategy

#### 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
    - **I**ntrane
  - Right where they reside and where they are used
  - Decrease the "surface" of threat exposure
- Data-level
  - Authentication
  - Encryption
  - Open and secure protocol
  - Secure system with trust monitor
  - Risk Management
- Identity & Access Management

Internet

Corporate IT Infrastructure & Security Strategy



#### **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 comprimising security



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

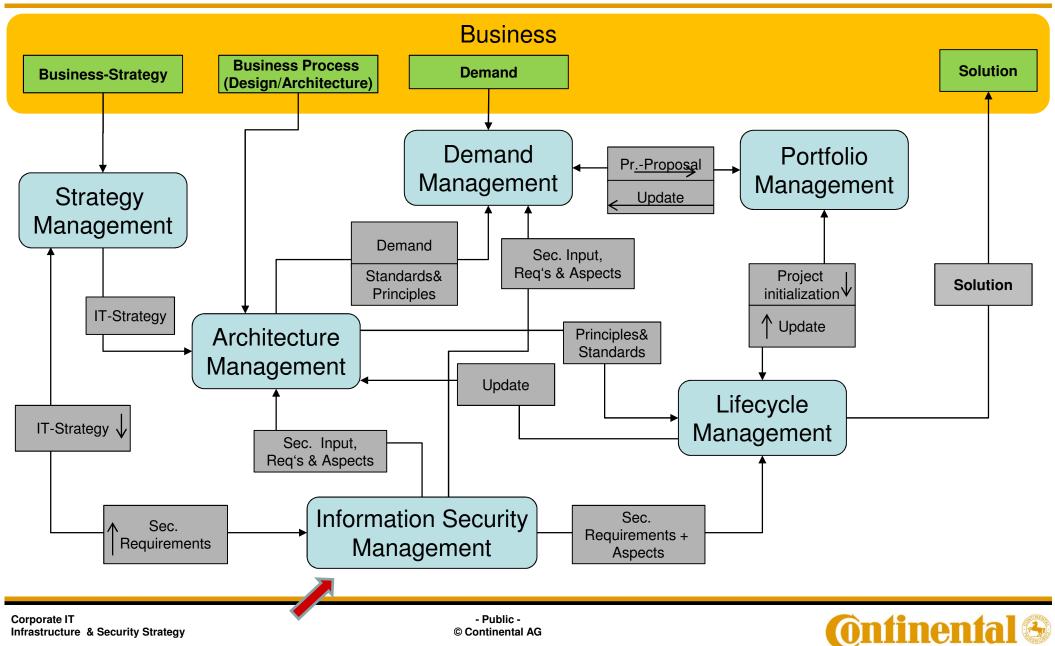
- IS built-in into top level IT Processes
- □ IS embedded in Service Architecture
- IS integrated into Service Life Cycle

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

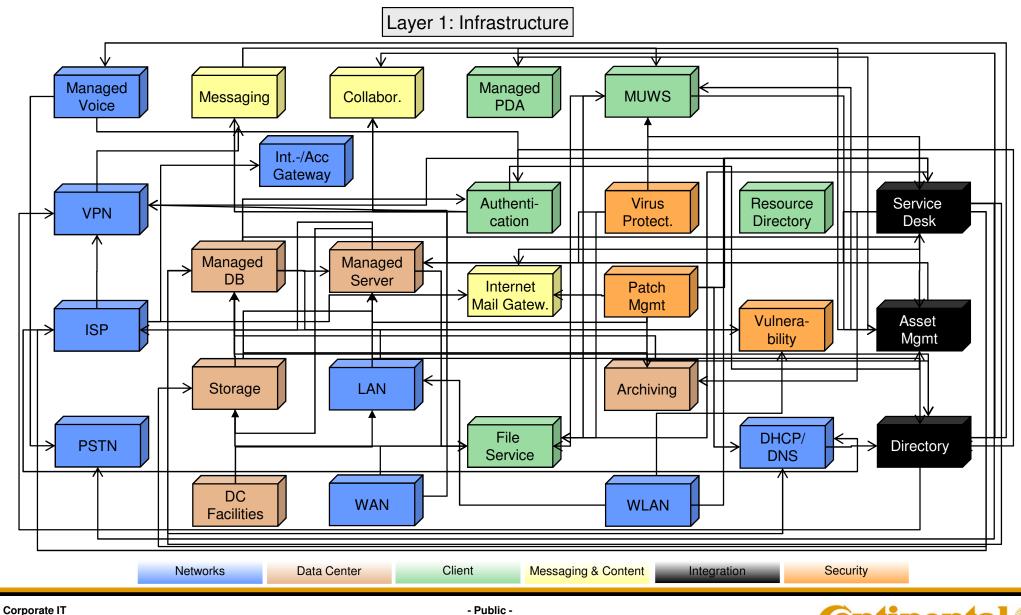
Corporate IT Infrastructure & Security Strategy



### **IS Management – Part of IT Processes Integrated Framework**



#### **Infrastructure Services at Continental IT**





© Continental AG



## **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: "Ma	anaged DB - MSSQL - SC	EE" - Windows Inter	net Explorer						_	. 8 ×
😋 💽 👻 🙋 http://eam.conti.c	de/EAM/ServiceDescriptions	_Details.iws?sp5=8&sb	fpgo=8&sbfpgn=&sbfid=1	:0:9&KeyAttribute=°	%7BBE876743-56B1-4CA0-82CB-718	8763FF7554%7D&PrimaryIr 💌 😽	X Live Search			P -
	tion: "Managed DB - MSSQL	- sc					🏠 • 🗟 • 🖶	🔹 🔂 Se	įte 👻 🎯 Ex <u>t</u> ra	as 🔹 💙
→ Upward Interfaces → Supported Services	Attended Operation	Time		5 × 10					窗	
→ Downward Interfaces	On call			7 x 24	follow the sun				<b>a</b>	
Required Services	Operation Time			7 x 24	excl. maintenance win	dows			窗	
→ Derived from → Service Parameters	Support			7 x 24					<b>a</b>	
→ Costs								2		
→ Processes → Roles	Service Level / H	(PI (3 Service El	ements)							
→ Required Skills	Name	Value								
→ All Documents	Availability	99.99	SLA Servicehours	Availability pe	er month max. Downtime			ø	窗	
Software			7 x 24	99,99%	2h					
→ Org. Units / Locations										
Actions										
_ Edit Service			Av in % = (Hrs-Ma	ain-Out)/(Hrs-N	1ain)*100					
Description			Hrs : = number of I	hours operation ti	me per month (7x24)					
Delete Service     Description	Main := number of hours agreed maintenance time per month Out := number of hours unscheduled downtime per month									
			Av : = Service av							
Compare Service										
<ul> <li>Show Roles / Staffs</li> <li>Mark as Target</li> </ul>	Response time	2h							窗	
<ul> <li>Mark as Target</li> <li>Service</li> </ul>	Time to fix	xx	Max duration [b]	Duiouitus Turana					1	
• Implement Role	<u>Inne to nx</u>	~~	Max. duration [h]	S Top	side / organization affected			•	ш	
New Service Element			4	A High	department affected					
• New Sourcing Constraint			16		n group / unit affected					
Constraint     New Cost Element			40	C Low	1 person affected					
New Process										
Require Document	Security Metrics	(6 Service Eleme	ents)			Detebase				
New Document     New Security	Name Value					Database				
Screening		Security Item: Da Type: Coverage	tabase Backup			Backup		ø	窗	
• New ISD from GSD		Units of Measure:	Percentage of System	IS						
New ISD from GSD     New ISD from ISD		Target Value: 98% Description: the p		s that are backed	up on a regular basis in accor	dance with the policy (at least fi	ull database			
New GSD from GSD			remental daily if not otl se backups divided by			ecurity requirements). The num	ber of databases			
New Generic Service					cies are being enforced.					
<ul> <li>New Application</li> <li>Service</li> </ul>		Source: Monitoring	by database script and	d analysis by Rep	orting Services	Public Accou	nt			
			asurement: monthly ffice: Marianne Tromb	ke			111			
Add Comment			blic Account Security	$\leftarrow$		Security			窗	
Create Favorite		Type: Coverage Units of Measure:	Percentage of System	IS		,				
		Target Value: 100		wing the GUEST a	account disabled (except temp	db) divided by the number of to	tal databases			
		Objective: to ensu			nt unauthorized access to infor					
		Formula: Source: Monitoring	by database script and	d analysis by Rep	orting Services	Critical Ev				
		Frequency of mea	asurement: monthly ffice: Marianne Tromb			Critical Fu				
	Coverage 2%	Security Item: Cri	itical Function Privilege			Privileo	jes	1	1 1	
	-	Type: Coverage					<u></u>			_
Fertig						j j j j Ver	rtrauenswürdige Sites		100%	- /

## SI Integrated Into Service Life Cycle

<b>U</b>				,				
Request o deeper Ana IT C	alysis Order received	Final IT Concept d approved ITG40	IT Design approved ITG60	Suppo approv ITC	ed succes		ted Use en	
Consolidation	Portfolio / Service Evaluation	Service Concept Refinement	Service Development	Rollout Preparation	Service Piloting	Service Rollout	Service Operation	Service Decommission
<ul> <li>Nervice Requirements, incl. Security and Quality requirements</li> <li>Service Requirements, incl. Security and Quality requirements</li> <li>German: Lastenheft)</li> <li>Service Operation Docu.: Service Level Agreement – [in work]</li> <li>Supplier Mgt. Docu.: Service Level Agreement – [in work]</li> <li>Supplier Mgt. Docu.: Service Level Agreement – [in work]</li> <li>Publice Design: Technology options, Solution Proposal – [in work]</li> <li>PM Docu.: Competence Center (CC), Expectation of Benefit by customer and of Funding, Cost Estimation by Demand Manager, Decision for 'Deeper Analysis' with named resources (IT Experts), Gate Release</li> </ul>	<ul> <li>GSD and TSG, incl: System &amp; Service Architecture – [in work]</li> <li>Incl: Service Specification, incl. Security and Quality Concept (German: Pflichtenheft) – [in work]</li> <li>Incl: Service Design: Solution Proposal</li> <li>Incl: Service Operation Docu:: Service Portfolio Catalogue – updated</li> <li>PM Docu:: Scope, Risks, Resources, Cost &amp; Benefit estimations, IT Project Class, Gate Release</li> <li>Customer Order AND IT Approval, IT Project Portfolio – updated</li> </ul>	<ul> <li>ISD, incl: Service Specification: Target definitions of service Impl. Service Description available (SDP), ), Quality Criteria and KPIs – [released]</li> <li>incl: System &amp; Service Architecture: Structure &amp; Interfaces – [released]</li> <li>incl: Service Operation Docu.: Service Security Plan, Service Level Agreement – [released]</li> <li>Supplier Mgt. Docu.: Sourcing Plan, Supplier Contracts prepared</li> <li>PM Docu.: Concept Workshop Result, IT Project Plan, Gate Release</li> <li>Capital Request (eCR) – [released]</li> </ul>	<ul> <li>Supplier Mgt. Docu.: Contracts with IT Suppliers signed – [released]</li> <li>Service Design: Functional Solution, Service Validation Plan – [released]</li> <li>Service Security Validation Plan, Quality Assurance - [released]</li> <li>PM Docu.: Regular project documents monitored &amp; updated, Gate Release</li> </ul>	<ul> <li>Service Operation Docu.: Support for Service available, Service documentation, Service Introduction Training material</li> <li>PM Docu.: Service Piloting Plan, Service Rollout Plan, Gate Release</li> <li>Pilot Support Commitment from affected location &amp; customer</li> </ul>	<ul> <li>Service Operation Docu.: Service Introduction Training Feedback</li> <li>Service: Service Validation Report, ISD review - [updated], Quality effect analysis, Release from customer – [released]</li> <li>PM Docu.: Security Screening - [released], Service Rollout Plan – updated, Gate Release</li> </ul>	<ul> <li>Service Operation Docu.: Users are successfully trained, Service</li> <li>Portfolio Catalogue – updated</li> <li>Service, Quality Management Process defined &amp; impl. – [released]</li> <li>PM Docu.: Project Portfolio – updated, Lessons Learned, IT Project Status Report (final - including target comparison), Handover to Service Responsible</li> </ul>	<ul> <li>Service Operation Docu.: Service Life-Cycle History, Regularly KPIs and Security Metrics of Service (e.g. Cost &amp; Benefit, Customer satisfaction), Improvement Plan, License Contract (updated according to usage), regular review &amp; update ISD, Gate Release</li> <li>Service Termination Notice</li> </ul>	<ul> <li>Service Decommission Agreement from all affected customers / locations</li> <li>Data Scrap Agreement from all affected customers / locations</li> <li>Service &amp; Data archived - [obsolete]</li> <li>Service &amp; Data archived - [obsolete]</li> <li>Service Operation Docu.: Maintenance Contract Cancellation, Service Portfolio Catalogue - updated, License &amp; Payments Cancellation, Gate Release</li> <li>Final Cancellation Notification to users</li> </ul>
Demand Mg	gr. Portfolio SC	Project SC	Project SC	Project SC	Project S	C Project SC	C Service R	esp. Service Resp.
Corporate IT			- Pi	ublic -				

Corporate IT Infrastructure & Security Strategy



# Innovation Ahead! Drive safely!

# Thank you

Corporate IT Infrastructure & Security Strategy

