



RiskMap

Process for determining the IT risk landscape

ISACA RoundTable

October 2012

Kay Behnke

Agenda

NXP

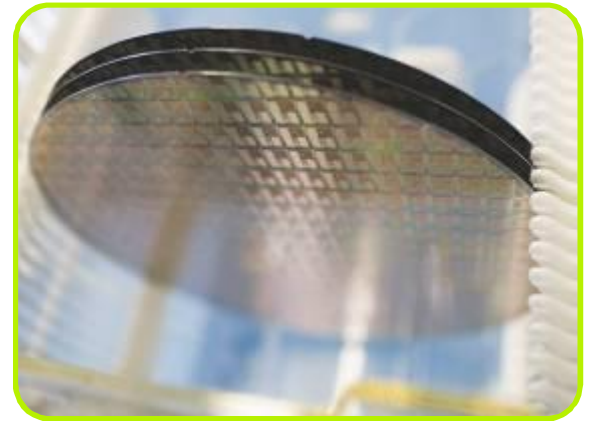
RiskMap

Next Steps

NXP Semiconductors

NXP Semiconductors N.V. (Nasdaq: NXPI) provides High Performance Mixed Signal and Standard Product solutions that leverage its leading RF, Analog, Power Management, Interface, Security and Digital Processing expertise.

- **Headquarters:** Eindhoven, The Netherlands
- **Employee base:** approximately 25,000 employees working in more than 25 countries with research and development activities in Asia, Europe and the United States, and manufacturing facilities in Asia and Europe
- **Net sales:** \$4.2 billion in 2011, over 62% of our sales are derived from the Asia Pacific region (incl. Japan)
- **Customers:** Leading OEMs worldwide



Key macro growth drivers in electronics



Energy Efficiency

- Efficient power conversion and low stand-by power
- Energy-saving lighting and back-lighting
- Energy conservation through demand side management
- Electric/lighter vehicles, intelligent traffic management



Connected Mobile Devices

- Proliferation of mobile data usage, wireless infra build-out
- Smart mobile devices: always-on, multimedia, location-based
- Connected car, many broadcast & connectivity standards
- New user interfaces (e.g., touch, joystick)



Security

- Secure mobile transactions and secure identity
- Authentication, tagging and tracking
- Car and home access, security & remote diagnostics
- Radar and (body) scanning installations

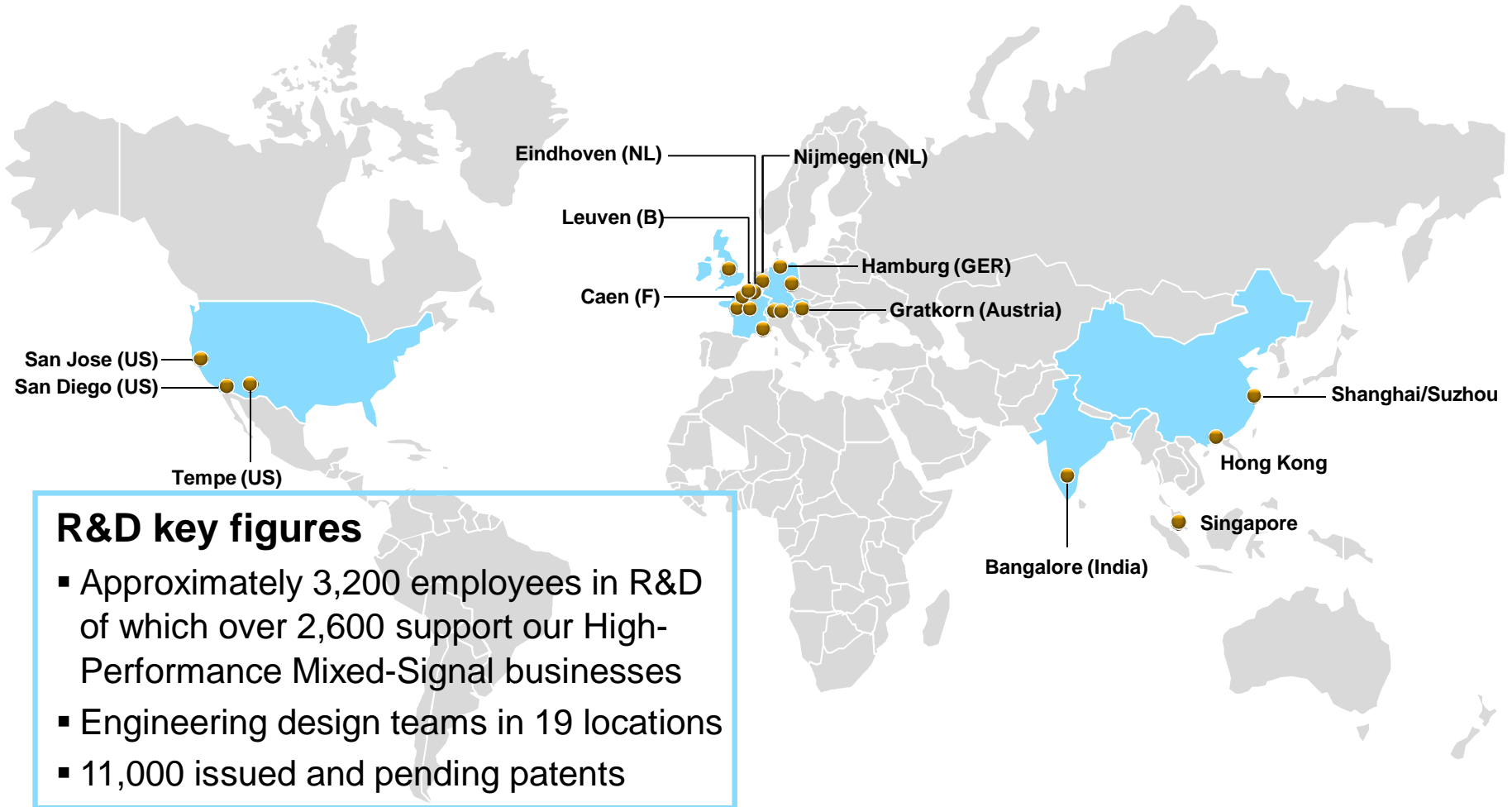


Health

- Personal healthcare and portable emergency devices
- Connected hearing aids and implantable devices
- Car safety & comfort
- Electronic diagnostics

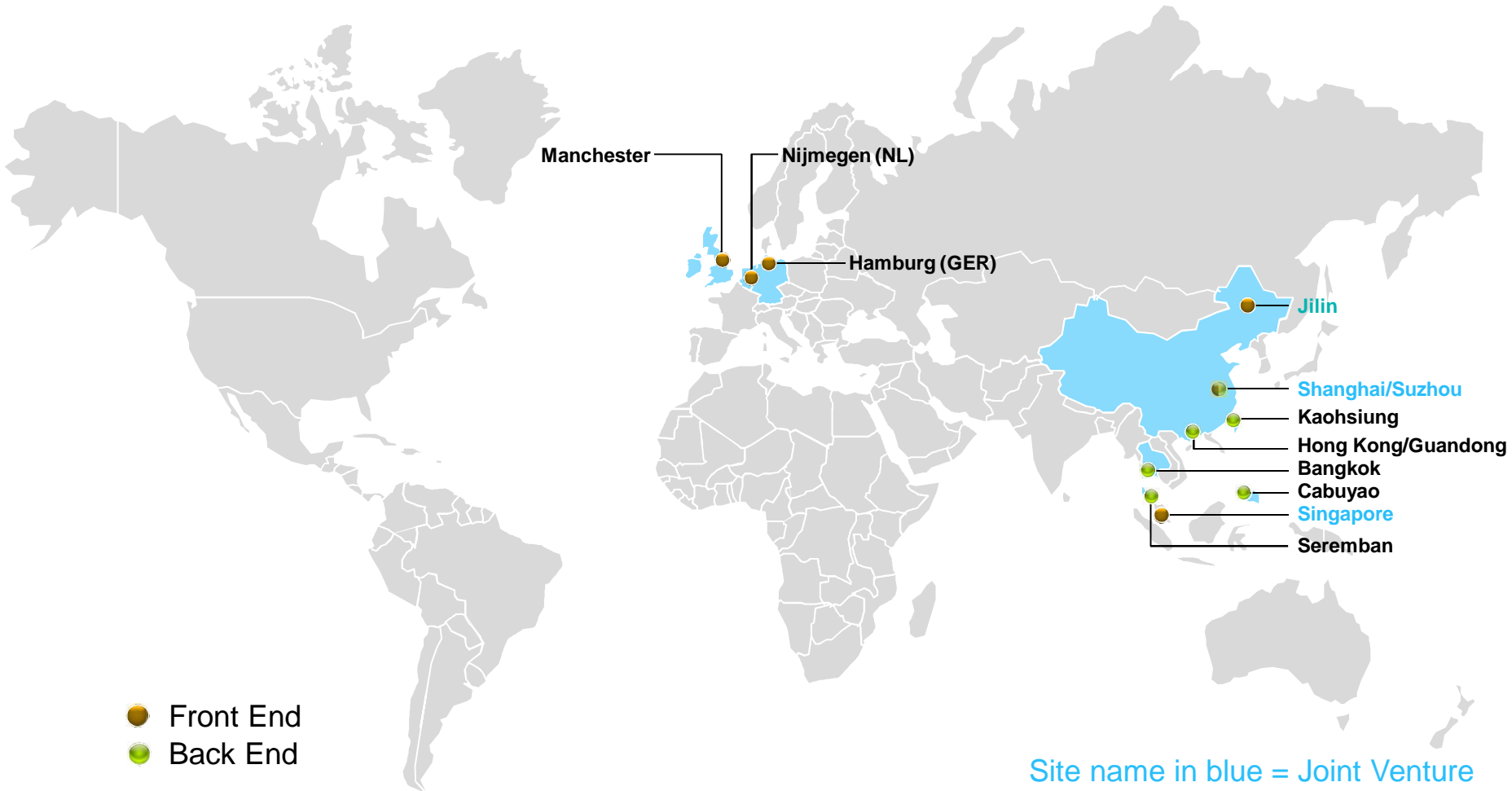
Strong innovation track record dating 50+ years

Focused investment of over \$550 million per year in R&D



World class manufacturing capabilities

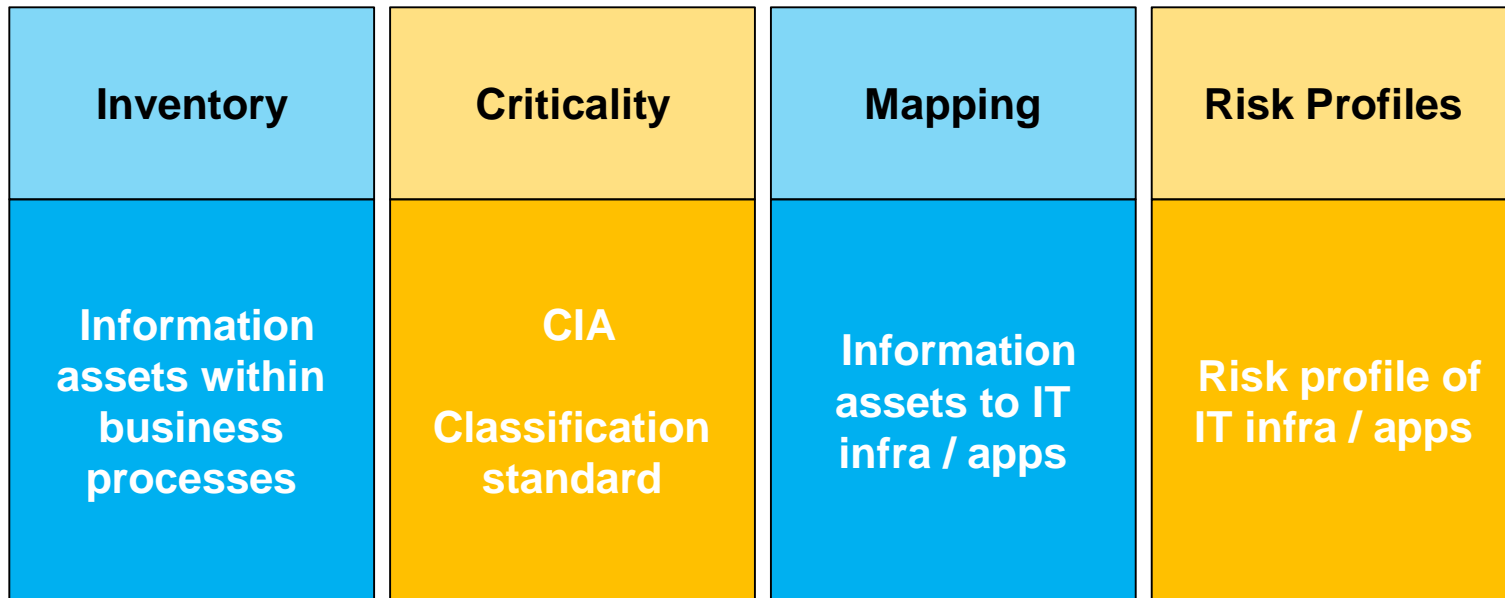
Differentiated process technologies and competitive manufacturing



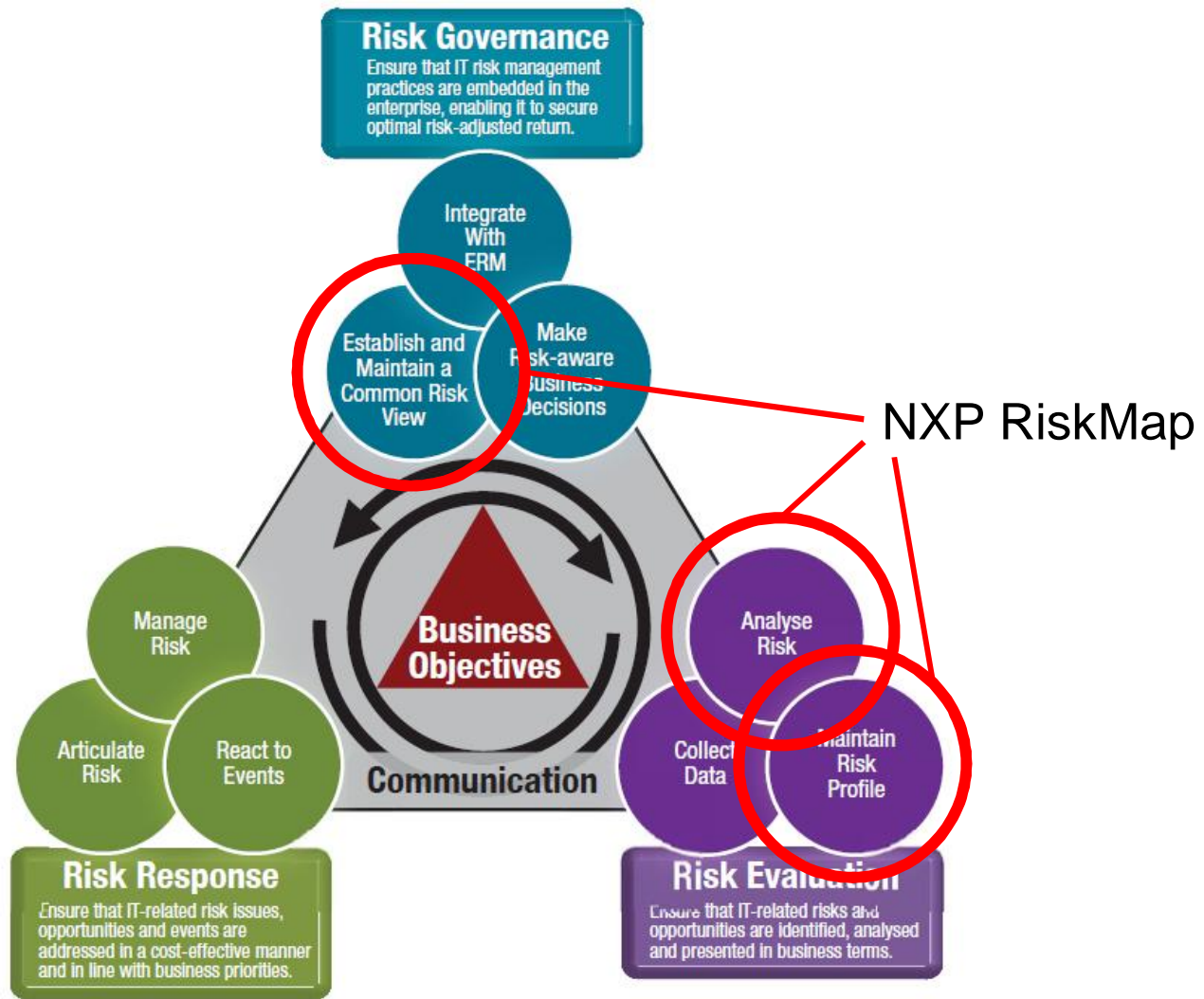


For more information about NXP: www.nxp.com

Objectives



RiskIT Framework (ISACA)



Process steps (RiskMap 1.0)



Add-Ons (RiskMap 2.0)



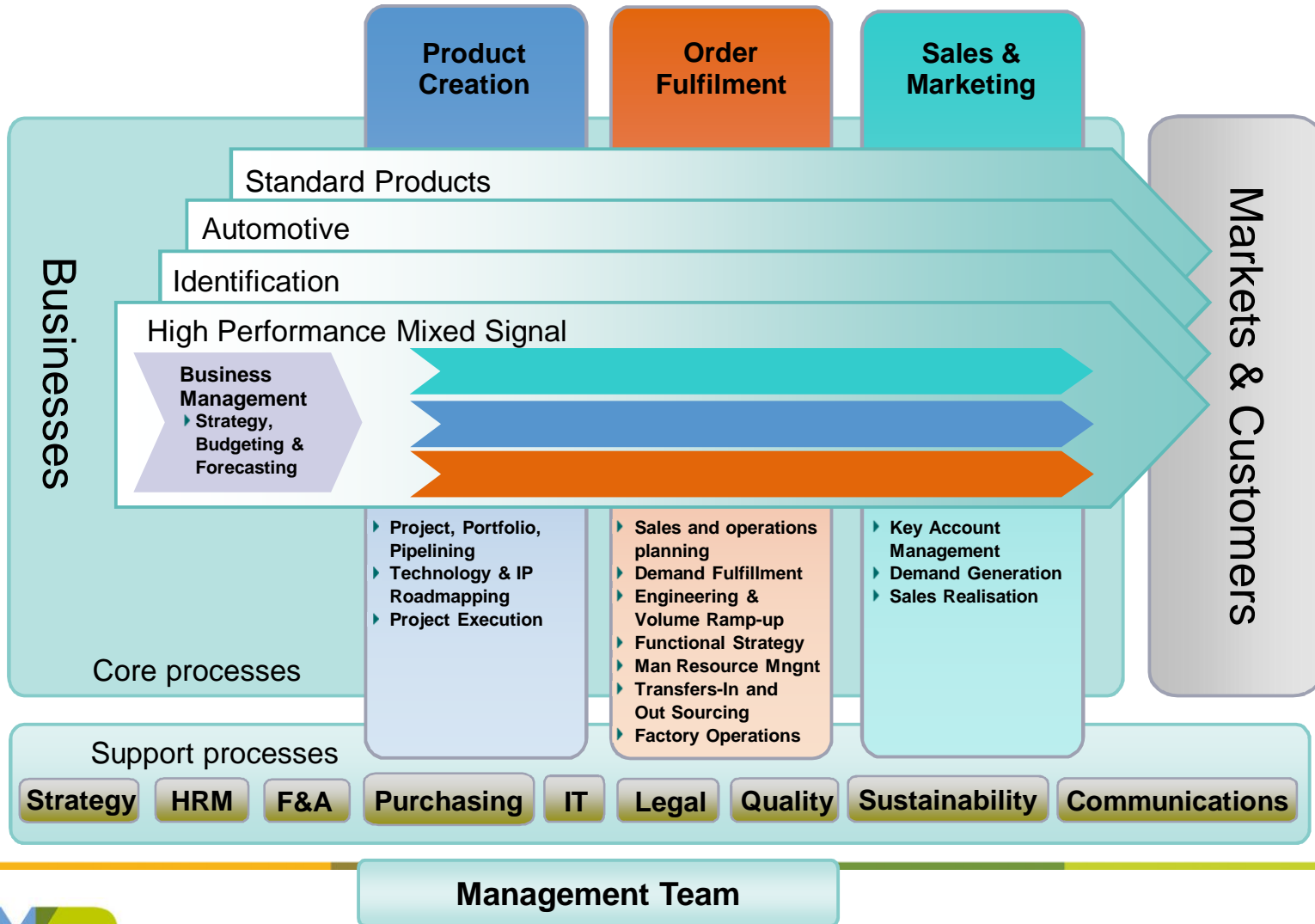
Process step

Preparation

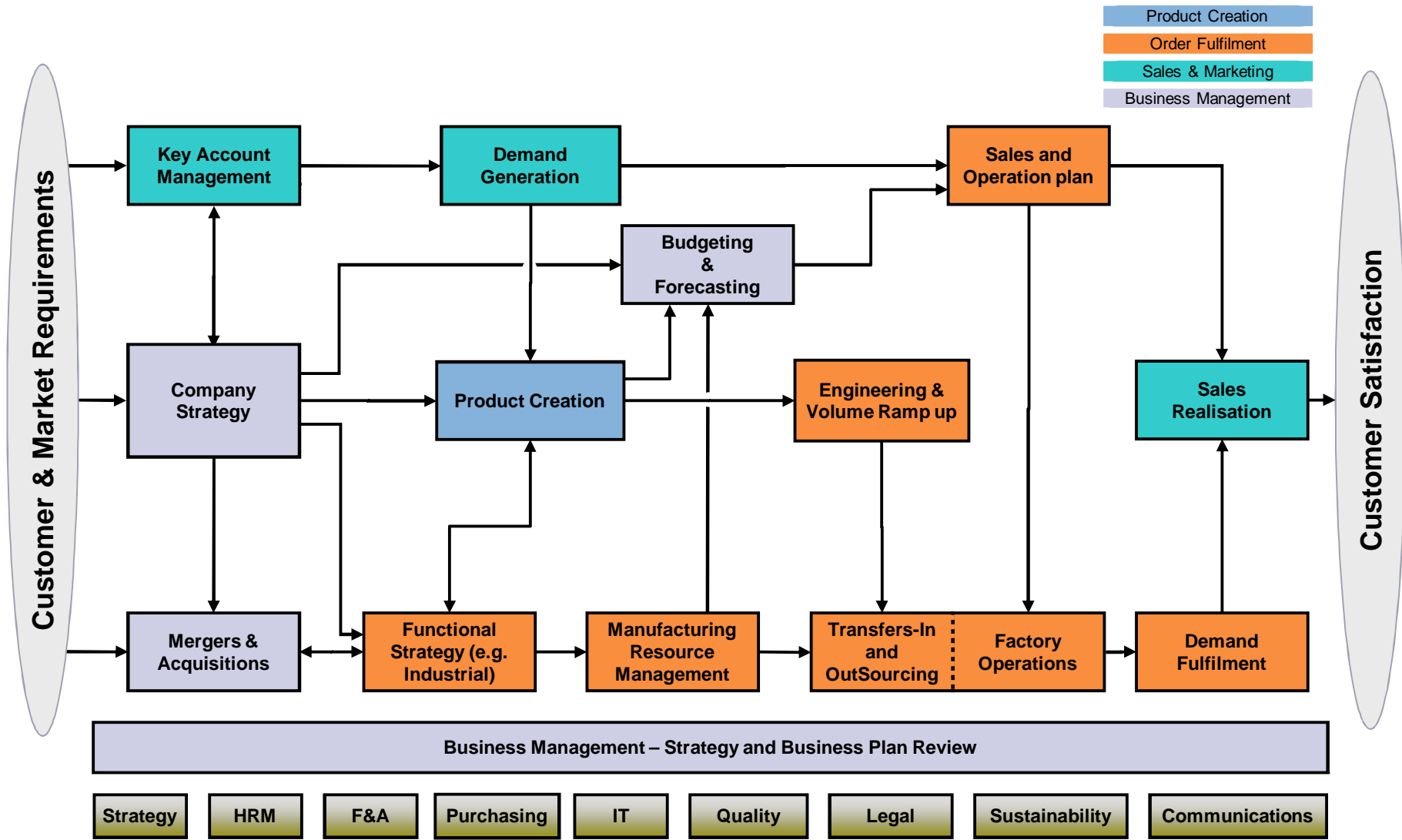
Buy-in from
business
process
owners

Severity
rating criteria

Business processes



NXP Processes and Main Linkages



Expressing impact in business terms

CobIT Information Criteria	Balanced Scorecard (BSC)	COSO ERM	FAIR	ISF
Effectiveness Efficiency Confidentiality Integrity Availability Compliance Reliability	Financial Customer Internal Growth	Strategic Operations Reporting Compliance	Productivity Response Replacement Competitive advantage Legal Reputation	Finance Operations Customer Employee

Expressing impact in business terms

CobIT Information Criteria	Balanced Scorecard (BSC)	COSO ERM	FAIR	ISF
Effectiveness Efficiency Confidentiality Integrity Availability Compliance Reliability	Financial Customer Internal Growth	Strategic Operations Reporting Compliance	Productivity Response Replacement Competitive advantage Legal Reputation	Finance Operations Customer Employee

Severity rating criteria

Property of information		Business impact type	Severity rating				
Ref.	Impact		A-Very high, B-High, C-Medium, D-Low, E-Very low				
Financial			A Very high	B High	C Medium	D Low	E Very low
F1	Loss of sales, orders or contracts	Financial impact	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%
F2	Loss of tangible assets (e.g. fraud, theft of money, lost interest)	Financial impact	\$30m+	\$1m to \$30m	\$100K to \$1m	\$10K to \$100K	Less than \$10K
F3	Penalties/legal liabilities (e.g. breach of legal, regulatory or contractual obligations)	Financial impact	\$30m+	\$1m to \$30m	\$100K to \$1m	\$10K to \$100K	Less than \$10K
F4	Unforeseen costs (e.g. recovery costs)	Financial impact	\$30m+	\$1m to \$30m	\$100K to \$1m	\$10K to \$100K	Less than \$10K
F5	Depressed share price (e.g. sudden loss of share value)	Loss of share value	25% +	11% to 25%	6% to 10%	1% to 5%	Less than 1%

Process step

Execution

Information
Asset
selection

Information
Asset rating
(C, I, A)

Information
Asset
mapping

Rating of information assets (1)

Key Business process	Business process	Information Type	Information is <i>disclosed</i> without authorization	Information is <i>modified</i> without authorization	Information is <i>unavailable</i> for 1 hour	Information is <i>unavailable</i> for 1 day
Sales & Marketing	Key Account Management	Customer Ranking				
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements				
Sales & Marketing	Demand Generation	Pricing & Quoting				
Sales & Marketing	Demand Generation	Customer Forecast				
Sales & Marketing	Sales Realization	Customer Contracts				
Sales & Marketing	Sales Realization	Design Win				

Rating of information assets (2)

Key Business process	Business process	Information Type	Information is <i>disclosed</i> without authorization	Information is <i>modified</i> without authorization	Information is <i>unavailable</i> for 1 hour	Information is <i>unavailable</i> for 1 day
Sales & Marketing	Key Account Management	Customer Ranking	Medium	Low	Low	Low
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements	High	Medium	Low	Low
Sales & Marketing	Demand Generation	Pricing & Quoting	Very High	Very High	Low	High
Sales & Marketing	Demand Generation	Customer Forecast	High	High	Low	Low
Sales & Marketing	Sales Realization	Customer Contracts	High	High	Low	Low
Sales & Marketing	Sales Realization	Design Win	High	Low	Low	Low

Mapping of information assets to applications (1)

Key Business process	Business process	Information Type	Appl A (CLASS)	Appl B (i2)	Appl C (B2B)	Appl D (CRM)
Sales & Marketing	Key Account Management	Customer Ranking	X	X		
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements				X
Sales & Marketing	Demand Generation	Pricing & Quoting	X		X	
Sales & Marketing	Demand Generation	Customer Forecast		X	X	
Sales & Marketing	Sales Realization	Customer Contracts				X
Sales & Marketing	Sales Realization	Design Win			X	X

Mapping of information assets to applications (2)

Key Business process	Business process	Information Type	Appl A (CLASS)				Appl B (i2)				Appl C (B2B)				Appl D (CRM)			
			M	L	L	L	M	L	L	L								
Sales & Marketing	Key Account Management	Customer Ranking	M	L	L	L	M	L	L	L								
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements													H	M	L	L
Sales & Marketing	Demand Generation	Pricing & Quoting	VH	VH	L	H					VH	VH	L	H				
Sales & Marketing	Demand Generation	Customer Forecast					H	H	L	L	H	H	L	L				
Sales & Marketing	Sales Realization	Customer Contracts													H	H	L	L
Sales & Marketing	Sales Realization	Design Win									H	L	L	L	H	L	L	L



Mapping of information assets to applications (3)

Key Business process	Business process	Information Type	Appl A (CLASS)				Appl B (i2)				Appl C (B2B)				Appl D (CRM)			
			VH	VH	L	H	H	H	L	L	VH	VH	L	H	H	H	L	L
Sales & Marketing	Key Account Management	Customer Ranking	M	L	L	L	M	L	L	L								
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements													H	M	L	L
Sales & Marketing	Demand Generation	Pricing & Quoting	VH	VH	L	H					VH	VH	L	H				
Sales & Marketing	Demand Generation	Customer Forecast					H	H	L	L	H	H	L	L				
Sales & Marketing	Sales Realization	Customer Contracts													H	H	L	L
Sales & Marketing	Sales Realization	Design Win									H	L	L	L	H	L	L	L



Process step

Calibration

Information
Asset
calibration

Application
criticality
verification

Mapping of information assets to applications – after calibration

Key Business process	Business process	Information Type	Appl A (CLASS)				Appl B (i2)				Appl C (B2B)				Appl D (CRM)			
			VH	VH	L	H	H	H	L	L	VH	VH	L	H	H	H	L	L
Sales & Marketing	Key Account Management	Customer Ranking	M	L	L	L	M	L	L	L								
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements													H	M	L	L
Sales & Marketing	Demand Generation	Pricing & Quoting	VH	VH	L	H					VH	VH	L	H				
Sales & Marketing	Demand Generation	Customer Forecast					H	H	L	L	H	H	L	L				
Sales & Marketing	Sales Realization	Customer Contracts													H	H	L	L
Sales & Marketing	Sales Realization	Design Win									H	L	L	L	H	L	L	L



Mapping of information assets to applications – after calibration

Key Business process	Business process	Information Type	Appl A (CLASS)				Appl B (i2)				Appl C (B2B)				Appl D (CRM)			
			VH	VH	L	H	H	H	L	L	VH	M	L	H	H	H	L	L
Sales & Marketing	Key Account Management	Customer Ranking	M	L	L	L	M	L	L	L								
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements													H	M	L	L
Sales & Marketing	Demand Generation	Pricing & Quoting	VH	VH	L	H					VH	VH	L	H				
Sales & Marketing	Demand Generation	Customer Forecast					H	H	L	L	H	H	L	L				
Sales & Marketing	Sales Realization	Customer Contracts													H	H	L	L
Sales & Marketing	Sales Realization	Design Win									H	L	L	L	H	L	L	L



Process step



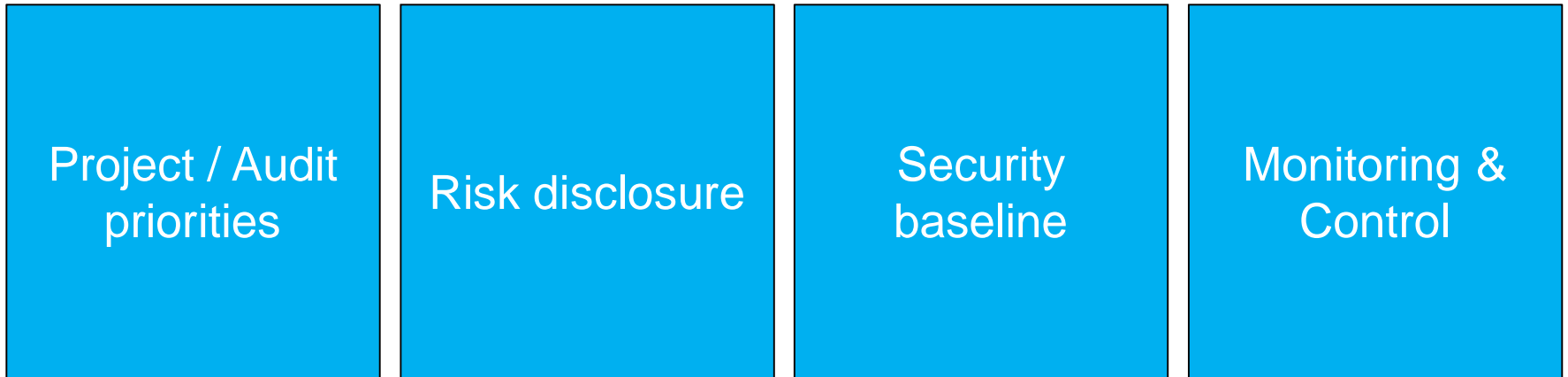
7 business
domains

14 business
processes

51 business
applications

56 information
assets

Usage



Add-On

Information
Classification

Information
Classification
Standard

Information
Asset
Inventory

Classification categories



Classification example

Process	Information	Classification			
		COMPANY PUBLIC	COMPANY INTERNAL	COMPANY CONFIDENTIAL	COMPANY SECRET
Holding					
	NXP legal entity/ reporting entity structure and changes to it		X		
	Debt/Equity before publication of financial results	X		X	
	Stock Based compensations			X	
	Earnings per share	X			X
	Group Equity	X			X
	Annual report/ Quarterly report related disclosures	X			X
	M & A transactions	X			X

Rating of information assets (1)

Key Business process	Business process	Information Type	Public	Internal	Confidential	Secret
Sales & Marketing	Key Account Management	Customer Ranking				
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements				
Sales & Marketing	Demand Generation	Pricing & Quoting				
Sales & Marketing	Demand Generation	Customer Forecast				
Sales & Marketing	Sales Realization	Customer Contracts				
Sales & Marketing	Sales Realization	Design Win				

Rating of information assets (2)

Key Business process	Business process	Information Type	Public	Internal	Confidential	Secret
Sales & Marketing	Key Account Management	Customer Ranking			X	
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements		X		
Sales & Marketing	Demand Generation	Pricing & Quoting			X	
Sales & Marketing	Demand Generation	Customer Forecast				X
Sales & Marketing	Sales Realization	Customer Contracts			X	
Sales & Marketing	Sales Realization	Design Win			X	

Mapping of information assets to applications (1)

Key Business process	Business process	Information Type	Appl A (CLASS)	Appl B (i2)	Appl C (B2B)	Appl D (CRM)
Sales & Marketing	Key Account Management	Customer Ranking	X	X		
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements				X
Sales & Marketing	Demand Generation	Pricing & Quoting	X		X	
Sales & Marketing	Demand Generation	Customer Forecast		X	X	
Sales & Marketing	Sales Realization	Customer Contracts				X
Sales & Marketing	Sales Realization	Design Win			X	X

Mapping of information assets to applications (2)

Key Business process	Business process	Information Type	Appl A (CLASS)	Appl B (i2)	Appl C (B2B)	Appl D (CRM)
Sales & Marketing	Key Account Management	Customer Ranking	Confidential	Confidential		
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements				Internal
Sales & Marketing	Demand Generation	Pricing & Quoting	Confidential		Confidential	
Sales & Marketing	Demand Generation	Customer Forecast		Secret	Secret	
Sales & Marketing	Sales Realization	Customer Contracts				Confidential
Sales & Marketing	Sales Realization	Design Win			Confidential	Confidential

Mapping of information assets to applications (3)

Key Business process	Business process	Information Type	Appl A (CLASS)	Appl B (i2)	Appl C (B2B)	Appl D (CRM)
			Confidential	Secret	Secret	Confidential
Sales & Marketing	Key Account Management	Customer Ranking	Confidential	Confidential		
Sales & Marketing	Demand Generation	Customer Opportunity / Requirements				Internal
Sales & Marketing	Demand Generation	Pricing & Quoting	Confidential		Confidential	
Sales & Marketing	Demand Generation	Customer Forecast		Secret	Secret	
Sales & Marketing	Sales Realization	Customer Contracts				Confidential
Sales & Marketing	Sales Realization	Design Win			Confidential	Confidential

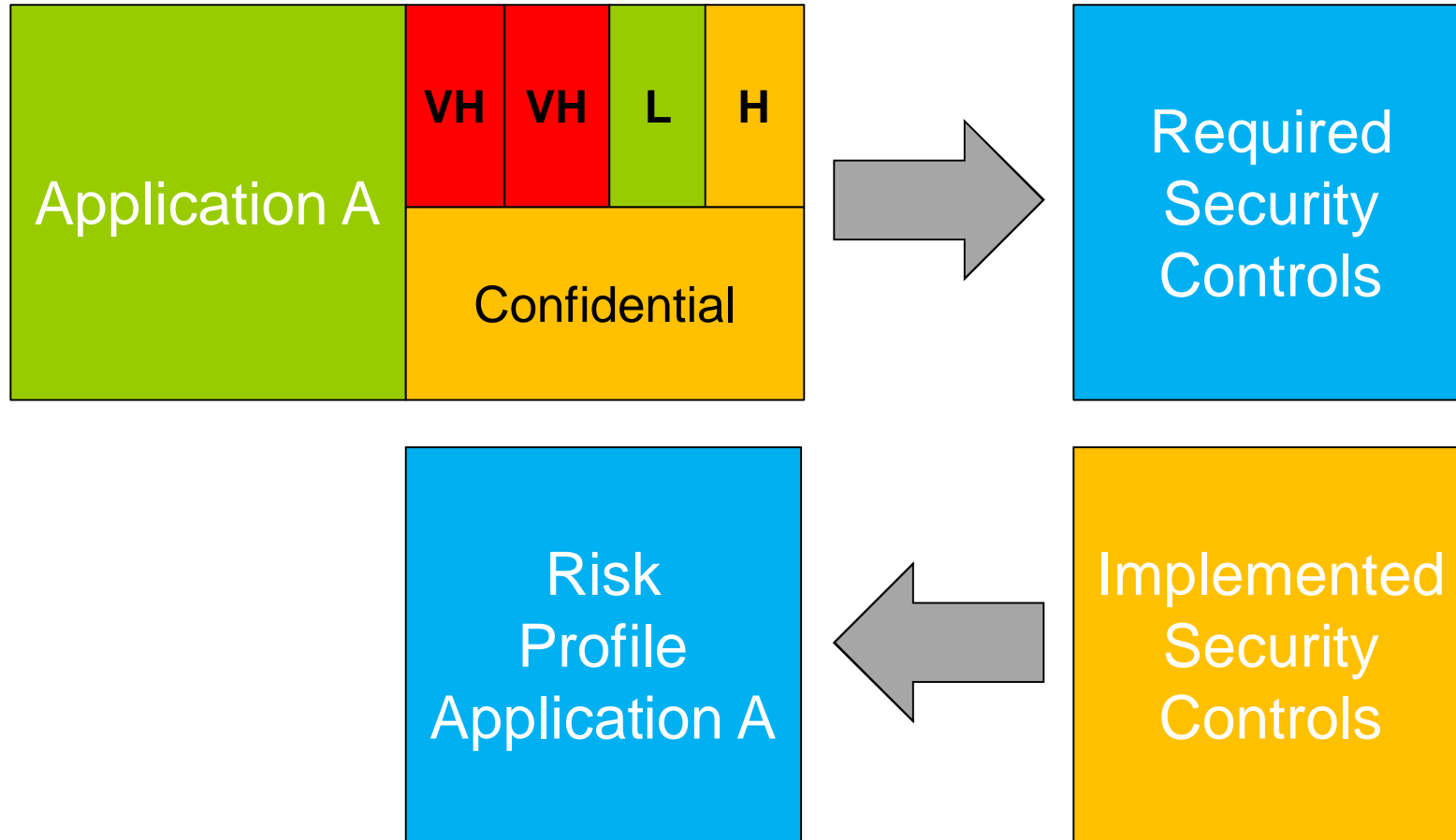
Add-On

Risk
Profiles

Security
Controls

Gap
Analysis

Gap analysis



Where can I store my data?

Application	Public	Internal	Confidential	Secret
Collabnet	✓	✓	✓	✗
Enovia	✓	✓	✓	✗
DesignSync	✓	✓	✓	✗
Office365	✓	✓	✓*	✗
File Shares	✓	✓	✓	✗
Wiki	✓	✓	✓	✗
Email	✓	✓	✓*	✗

* No technical IP or Personal Employee information

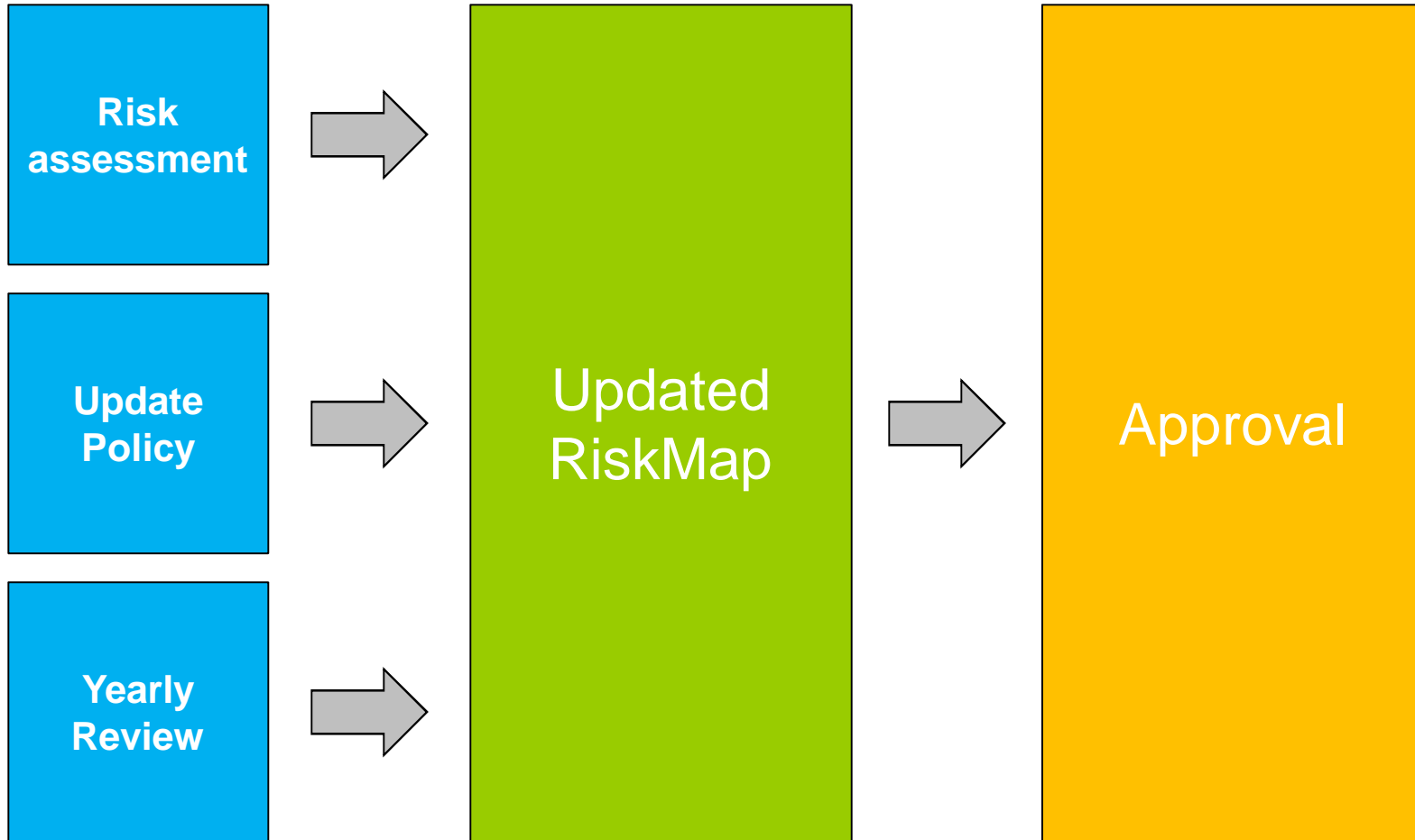
Add-On

Maintenance

Change
Management

Review
cycle

Review cycle



Lessons learned



- ▶ Management buy-in
- ▶ Business impact reference
- ▶ Uniformity (assets / rating)
- ▶ Moderation of workshops
- ▶ Start small, grow steady
- ▶ Calibration
- ▶ Approval
- ▶ Maintenance

