

Business Context: Key for Successful Risk Management

Philip Aldrich, CISSP, CISM, CISA, CRISC, CIPP
Program Director, Risk Management EMC



Obvious Fact: Traditional Security & Risk Management is Not Working



Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

96% of attacks were not highly difficult

99% of breaches led to compromise within “days” or less & 85% took weeks or more to discover

63% of recommended preventative measures are “simple & cheap”

97% of breaches were avoidable through simple or intermediate controls

96% of victims subject to PCI DSS had not achieved compliance

Overload of Threat Information

Internal Threat Sources



DLP



SIEM



Anti Virus



Patch Management



Vulnerability Assessments



Security, Risk & Compliance Operations

External Threat Sources



Geo-Political Alerts



Risk Intelligence Agents



Trusted CERTs



Technology Vendors



Underground Organisations



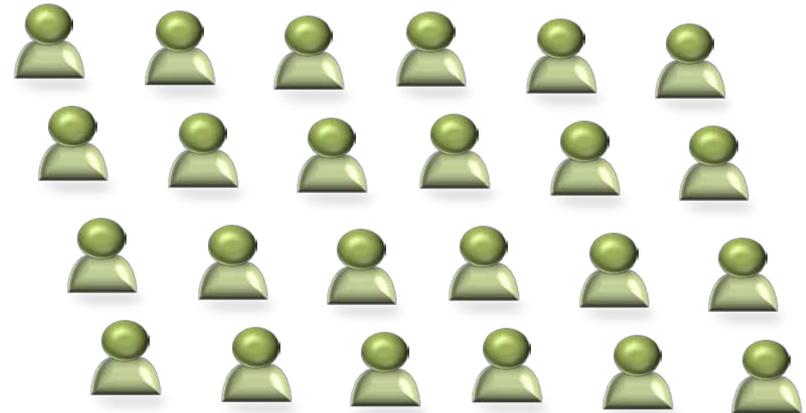
Where are the most critical exposures?



7 Years ago & Today



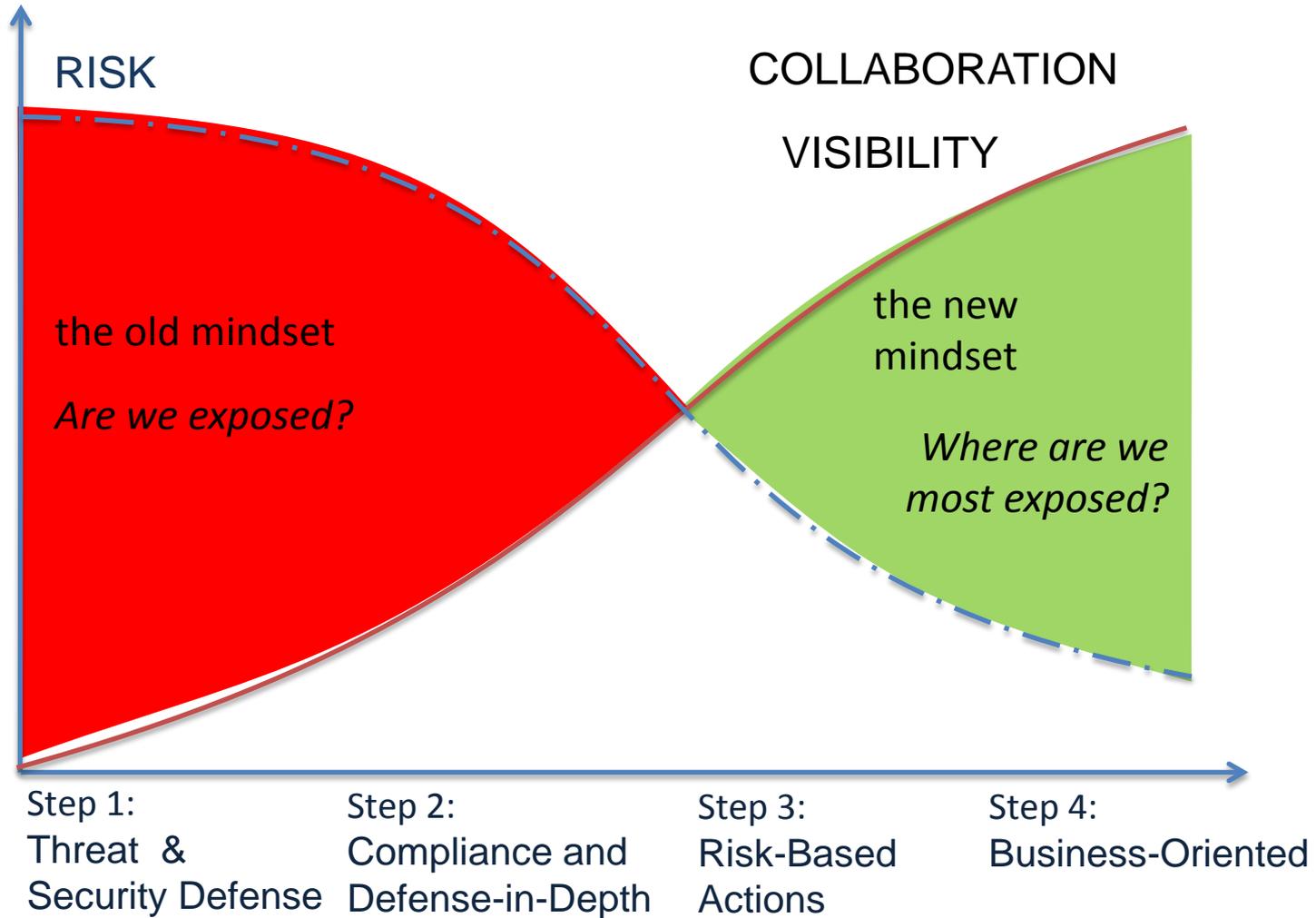
Risk, Security & Compliance Teams



REGULATORS



Striving for a Better Approach



The Case for Risk-Based Business Context

“We must distill down vast amounts of data into security intelligence — prioritized, actionable insight. To prioritize actions, there must be linkages to the business value of the assets and an improved understanding of the risk they represent.”

- Gartner

Context-Aware Intelligence

Model, Simulate, Act



Community



Context

Patterns, meaningful anomalies

Knowledge

Analyze

Information

Collect, Correlate

Dependencies, relationships

Big Data

Data

Data

Data

Data

Logs, Events, Costs, Usage, Attacks, Breaches

Source: Information Security Is Becoming a Big Data Analytics Problem
Published: 23 March 2012 Gartner research by Neil MacDonald



Understand Your Enterprise

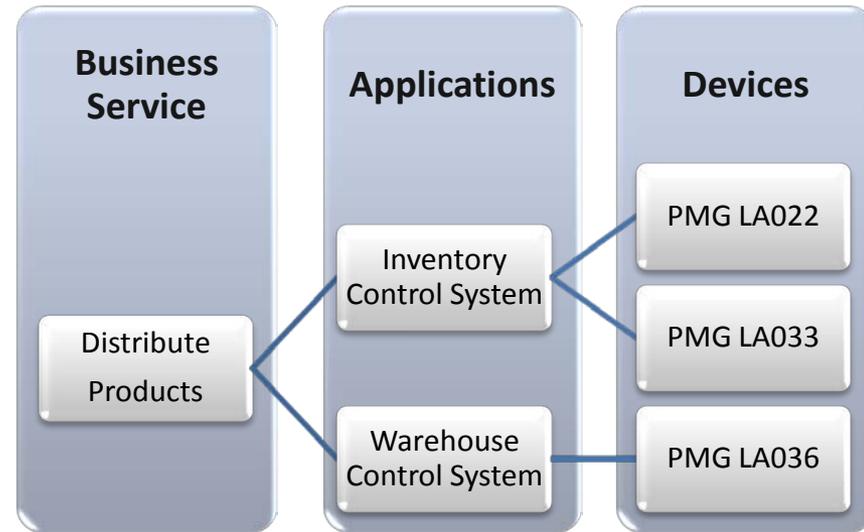


- Visibility
- Accountability
- Collaboration
- Criticality

Capturing Relationships

How?

- ❖ CMDDBs
- ❖ BPM
- ❖ GRC platforms

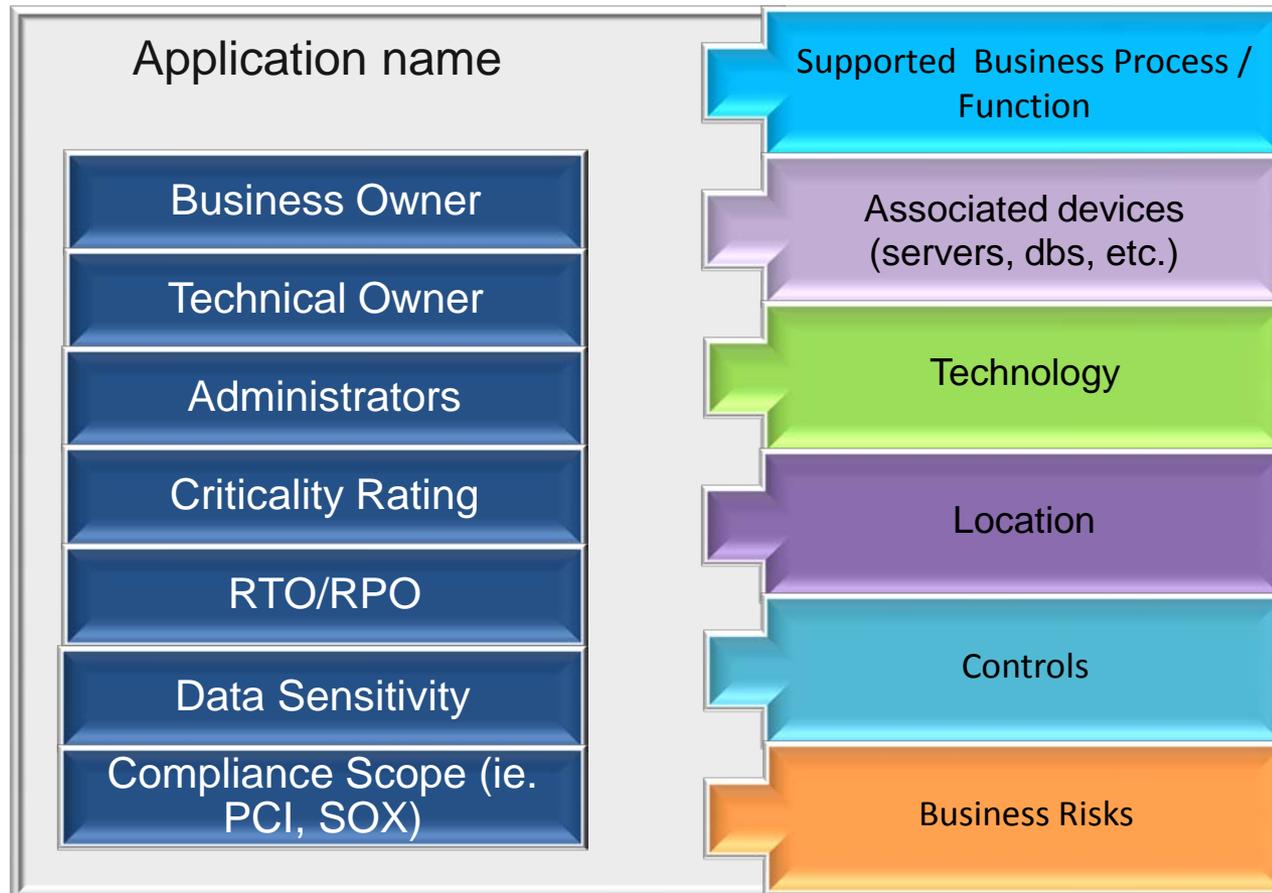


Products & Services by Risk Rating | Options ▾

Drag a column name here to group the items by the values within that column.

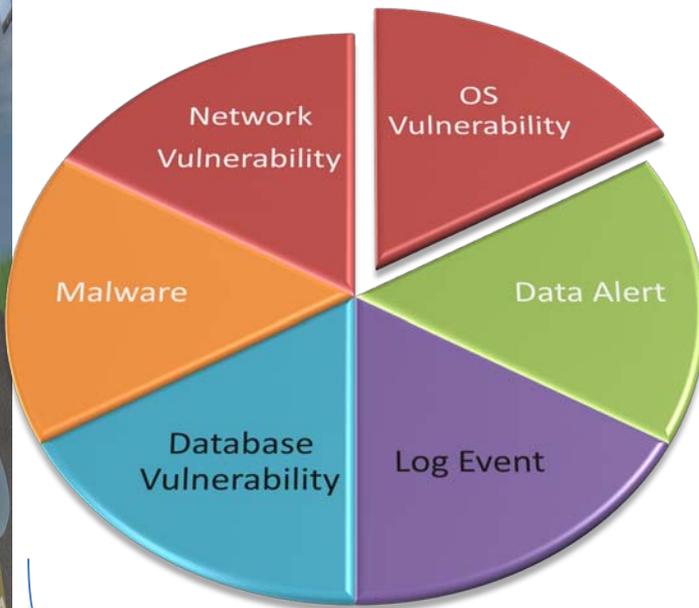
Product/Service Name ▲	Category	Description	Business Unit	Division/Office	Customer Impacting	Risk Rating	Applications	Devices
Archer eGRC Platform	External	The Archer eGRC Platform provides a simple yet powerful way to design, build and manage applications that can evolve right along with your business. You can create your own enterprise-class, security-assured applications, package them into comprehensive solutions and deploy them in a way that works for your organization.	North American IT Shared Services	Americas Services Division	No	-----	Archer SmartSuite Framework	EFIL SRV022 ELA001 ELAP006 ELAP007
Distribute Products	Internal	Shipping of products from warehouse to POS locations.	EMEA Shared Services South American Services	Asia Pac Southern Rim	Yes	-----	Inventory Control System Warehouse Control System	PMG LA022 PMG LA033 PMG LA036
On Demand Application Development	External	Development of On Demand applications within the Archer SmartSuite Framework.	North American Human Resources		No	-----	Archer SmartSuite Framework	FILSRV006 FILSRV007 FILSRV013
Respond to Customer Requests	External	This service ensures customer satisfaction.	Saskatchewan	Americas Services Division	Yes	-----	Customer Self-Service Website Customer Service Center Customer Support Platform	APPSRV003 DBSRV002 DPC001
Risk and Compliance Management	Internal	Identifies risks and tracks their mitigation and resolution by automating the creation and delivery of targeted risk assessment campaigns.	North American IT Shared Services	U.S. Domestic Operations	No	-----	Archer SmartSuite Framework	APPSRV002 APPSRV002
Sales Support & Business Development	Internal	This service oversees the overall sales support and business development programs for this company, including marketing and sales to R&D and long-term business strategies.	South American Services	U.S. Domestic Operations	Yes	-----	Customer Relationship Management (CRM)	

Putting Context together = Better Picture

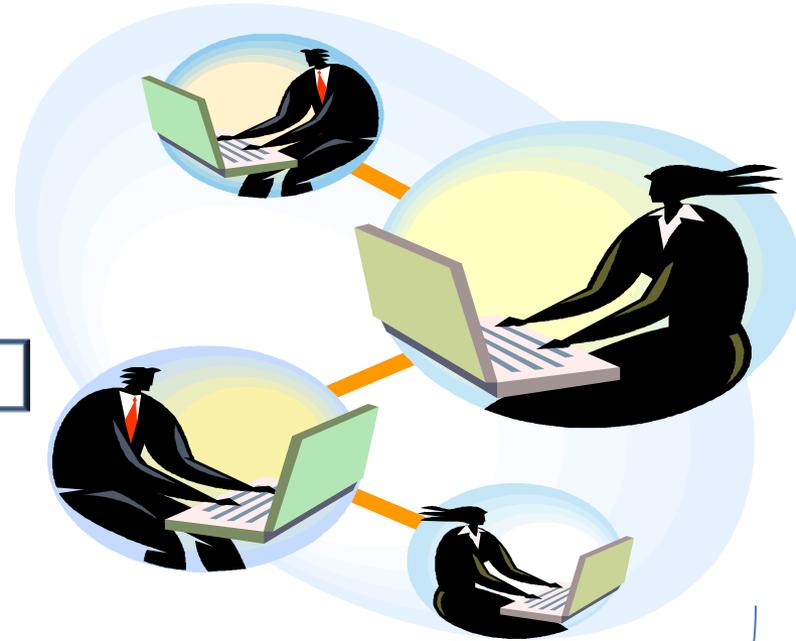


Context is an essential ingredient

Threat Criticality

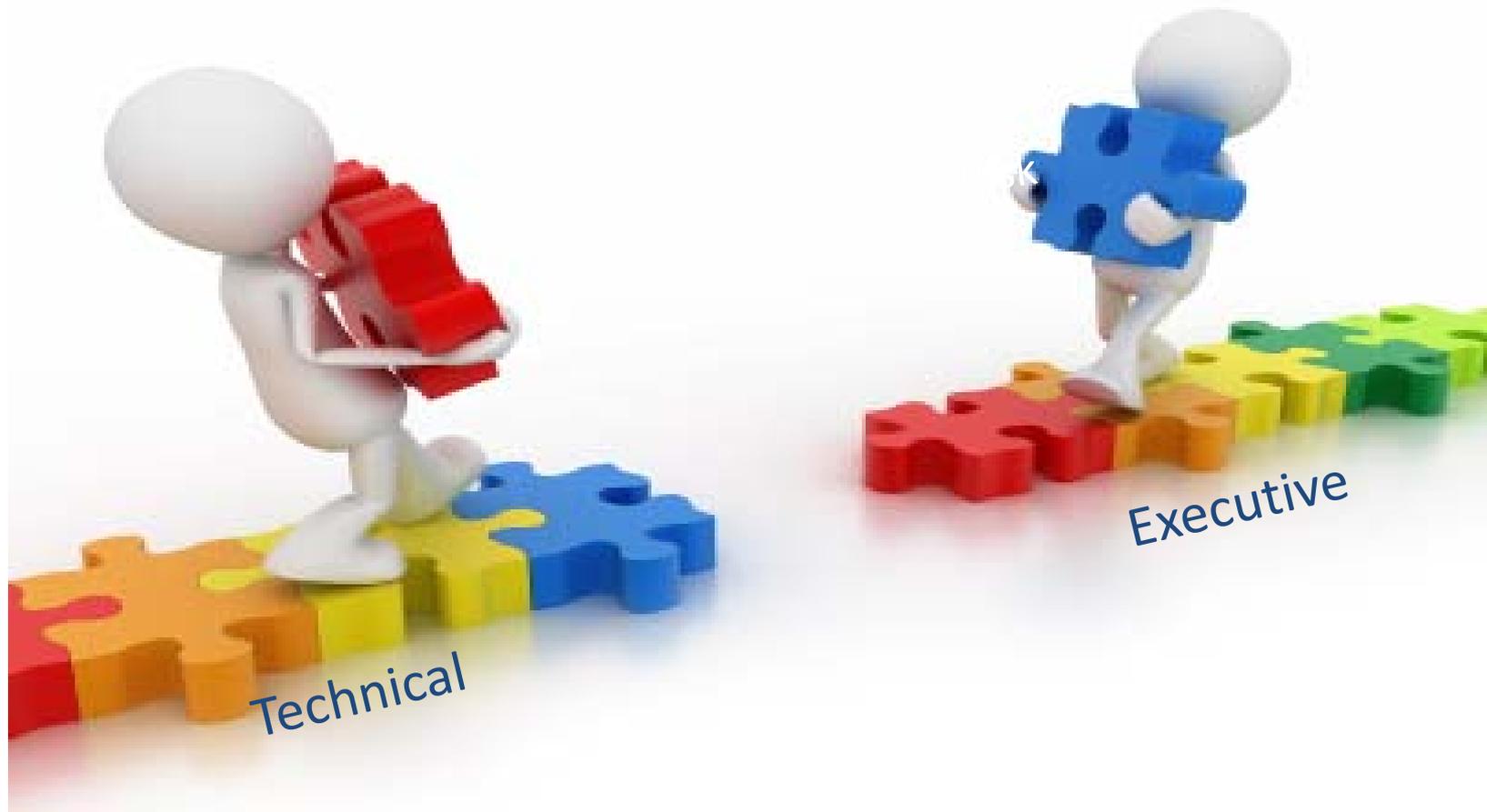


Business Context

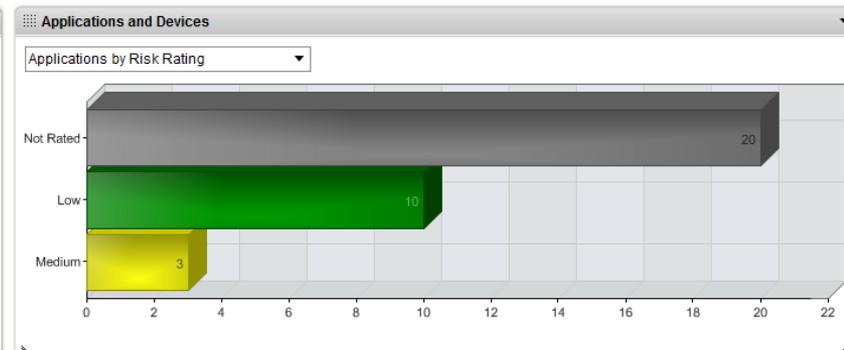
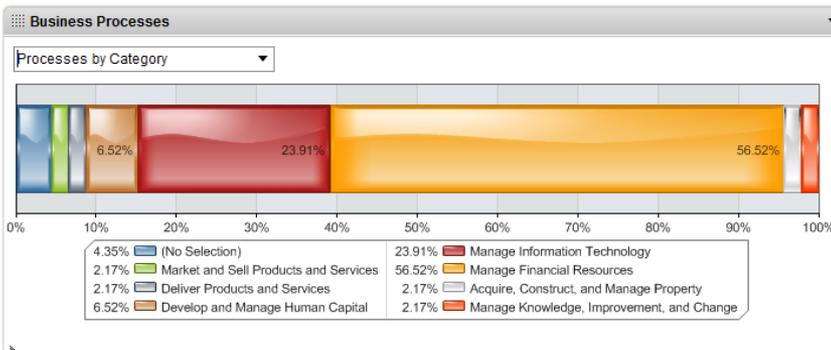
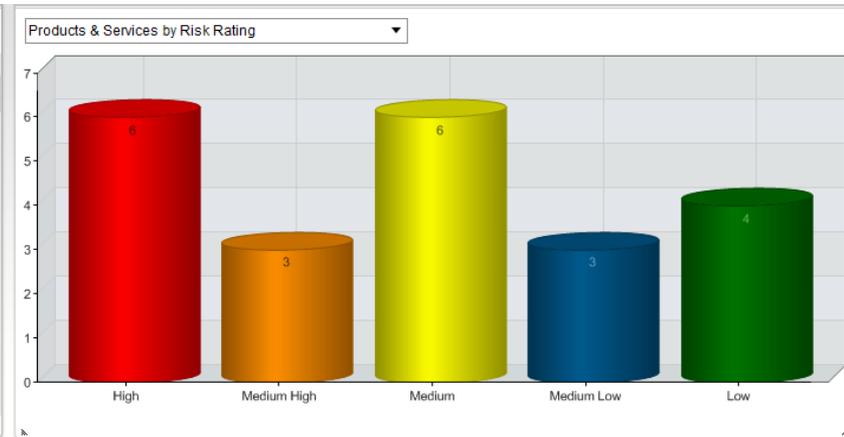
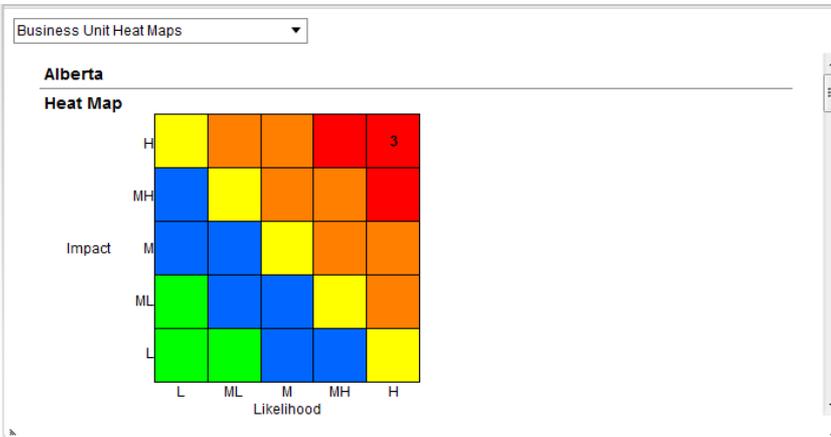


Prioritized Risk Treatment Response

Building the Risk Communication Bridge



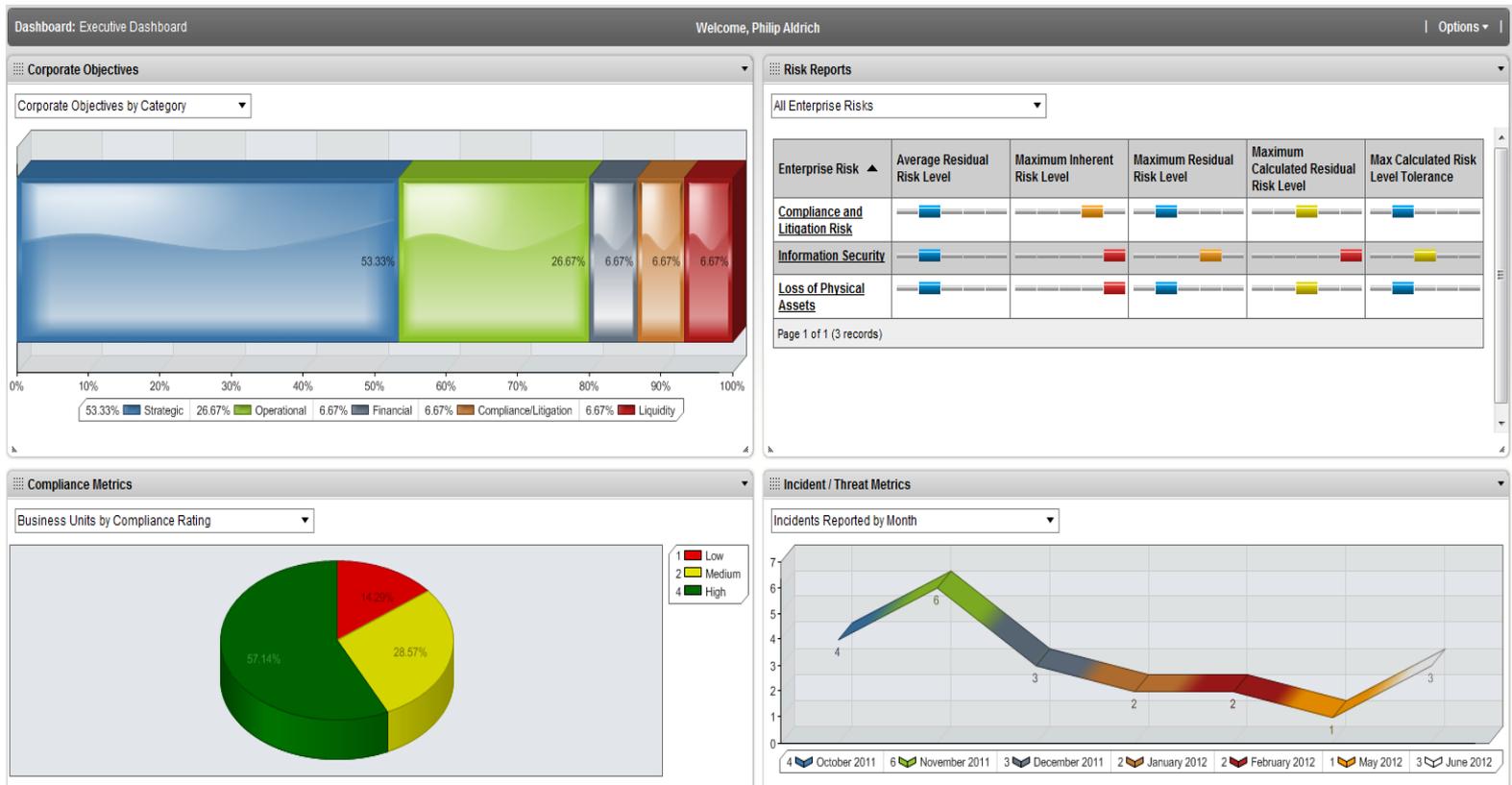
Use Context for a Top Down Risk Management Approach



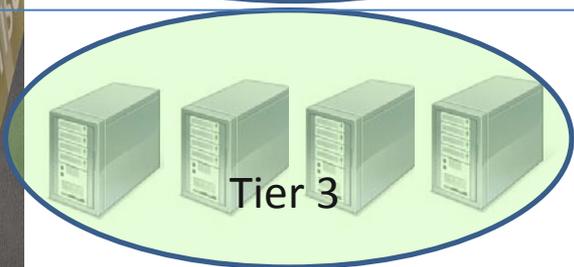
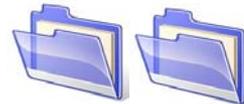
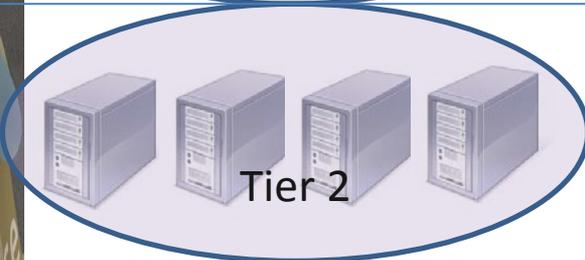
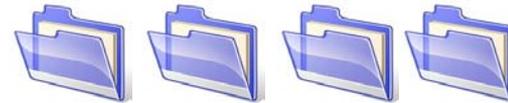
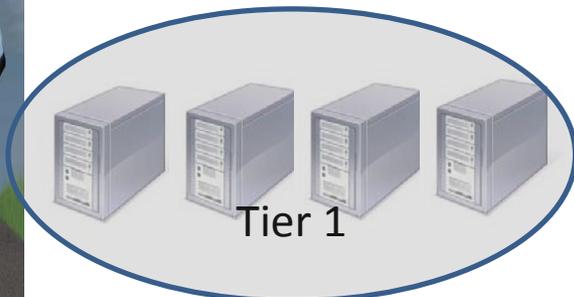
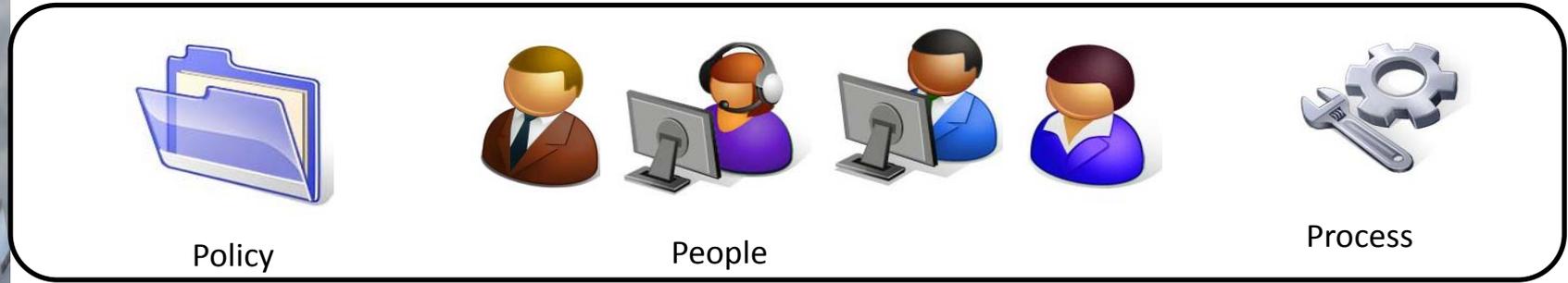
KRI's & KPI's to measure impact against: Business Strategy, Risk Register, Critical Assets, and Compliance requirements

Dashboards focused on Critical Business Impact

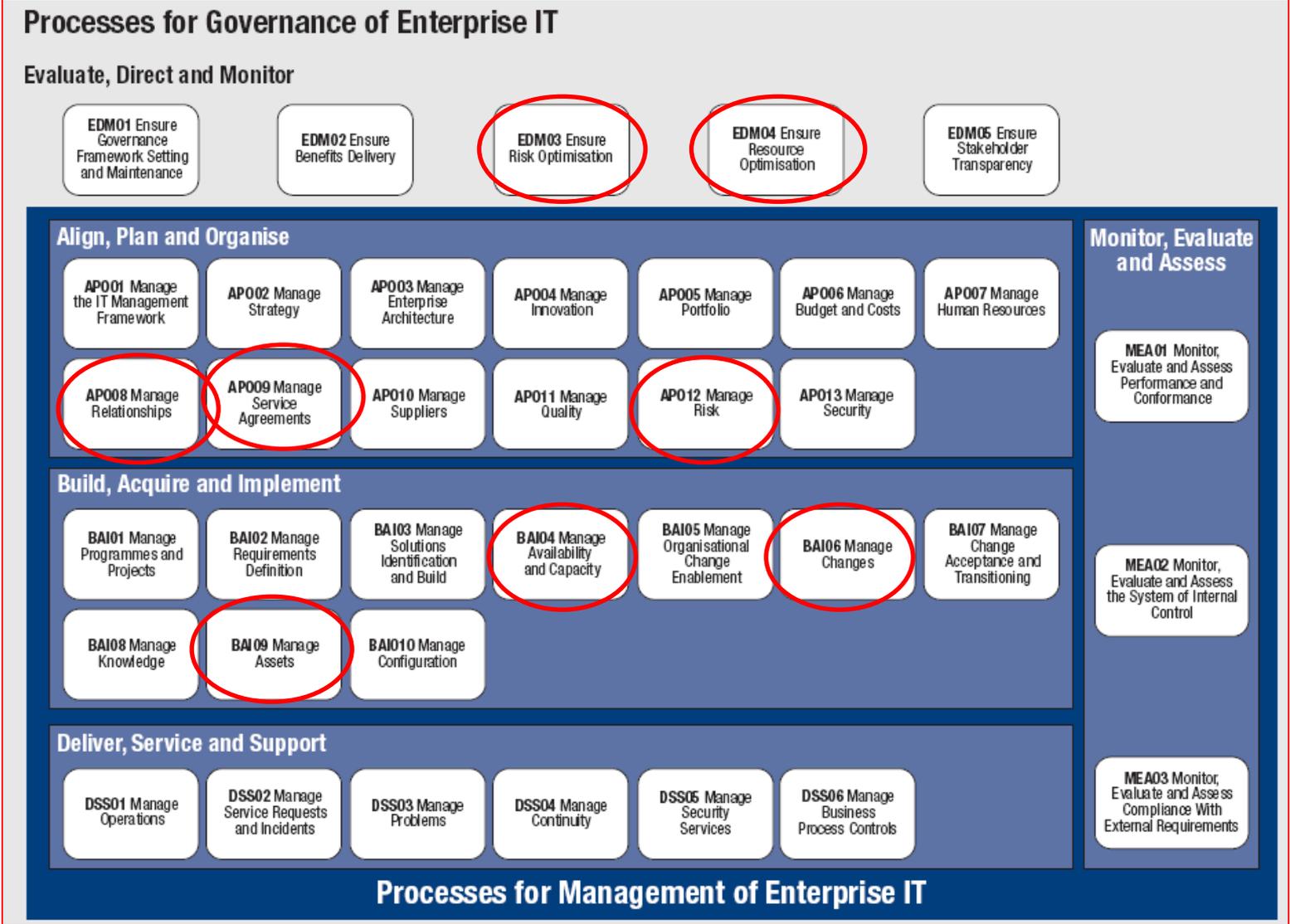
Incidents involving Tier 1, Critical Assets, must be mapped to Tier 1 SLA responses



Organizational control environment



Business Context is a critical function in COBIT 5



Ongoing Business Impact Analysis

Execute Risk Treatment

6

Identification of Assets

1



Determine SLA response & Control Mapping

5

Define & Map Relationships

2



Understand & Add Business Context

3

Business Validation

4



Bringing it together: Executing the plan

1. **Know your Assets**
 - Identify & consolidate your CMDBs, repositories, etc. into 1 risk view
2. **Identify Business Relationships**
 - Capture interdependencies b/w assets, processes, data
3. **Verify Business Criticality with Business Owners**
 - Send periodic surveys to align business with IT
4. **Tier Assets based on Criticality**
5. **Organize your control environment to business criticality**
6. **Monitor, Test & Validate**
 - Create Dashboards focused on Critical Assets → FOCUS!

Infrastructure Metrics

Business Unit Asset Distribution

Business Unit ▲	Total Products & Services	Total Processes	Compliance Rating	Residual Risk	Total Applications	Total Devices	Total Information Assets	Total Facilities
Alberta	0	0			0	0	0	0
Asia Pac Shared services	0	1			0	13	1	0
EMEA Shared Services	3	7			8	21	0	0
North American Human Resources	2	1			0	1	0	0
North American IT Shared Services	5	8			7	54	1	1



THANK YOU!