



IBM Security Framework

..... being a step ahead.....

2011/05/18
Roman TUMA, IBM Security
Solutions
Asia Pacific Executive

IBM **Security** Summit
IBM Security Solutions. Secure By Design.

Agenda

- IBM's Security Framework and its application in the real world
- Secure by Design and better prevention of threats



Security enables us to address these risks and innovate



Safe Adoption of new Forms of technology



Protection of digital identities and Privacy



New Business Models like outsourcing and teleworking



Adoption of virtualization and cloud computing



Addressing compliance complexity



Information availability and integrity for real time decision making

IBM focuses on solving key security challenges associated with the Smarter Planet



Key drivers for security projects

Increasing Complexity



Soon, there will be **1 trillion** connected devices in the world, constituting an “internet of things”

Rising Costs



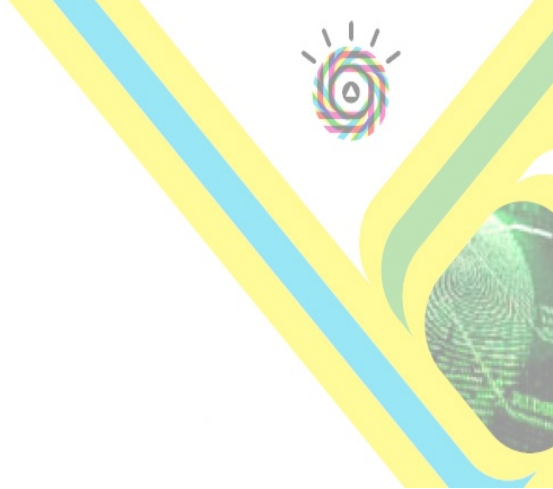
Spending by U.S. companies on governance, risk and compliance will grow to **\$29.8 billion** in 2010

Ensuring Compliance

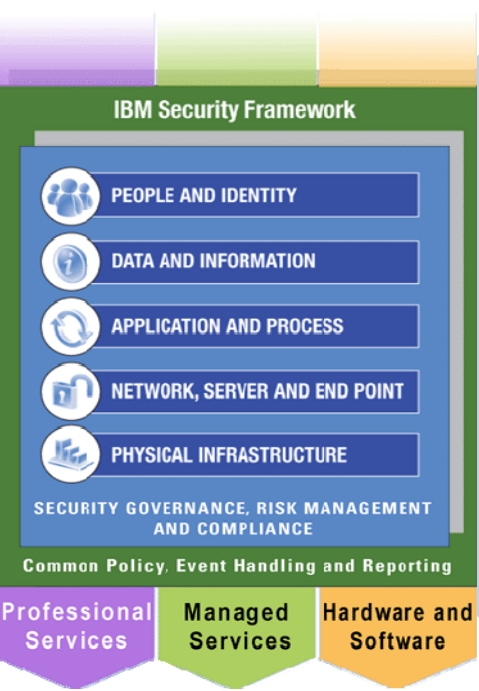


The cost of a data breach increased to **\$204** per compromised customer record¹

IBM Security Framework - Fundamentals



IBM Security Framework - Strategy



PEOPLE AND IDENTITY



Mitigate the risks associated with user access to corporate resources



DATA AND INFORMATION



Understand, deploy, and properly test controls for access to and usage of sensitive data



APPLICATION AND PROCESS



Keep applications secure, protected from malicious or fraudulent use, and hardened against failure



NETWORK, SERVER AND END POINT



Optimize service availability by mitigating risks to network components



PHYSICAL INFRASTRUCTURE



Provide actionable intelligence on the desired state of physical infrastructure security and make improvements



GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE



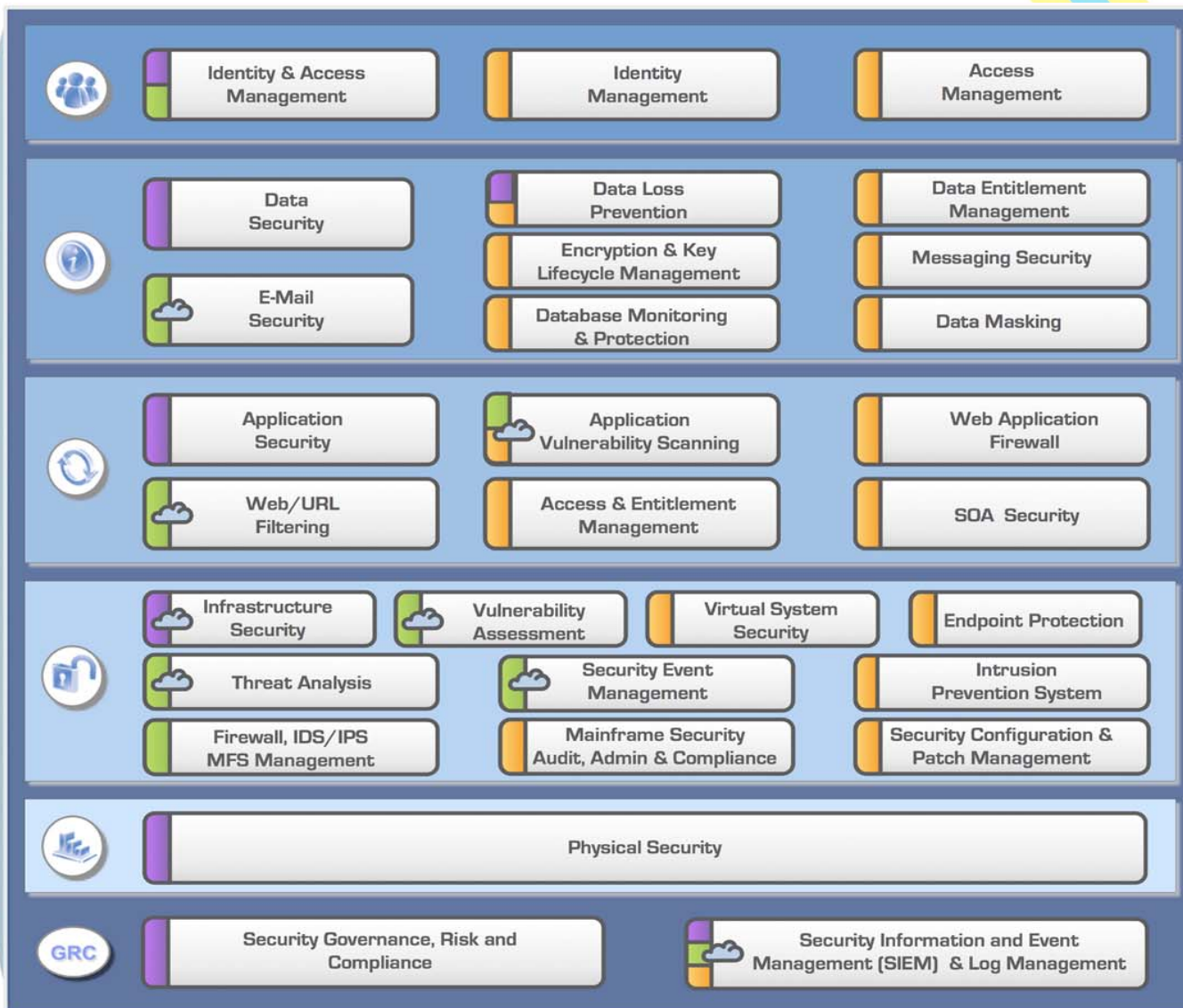
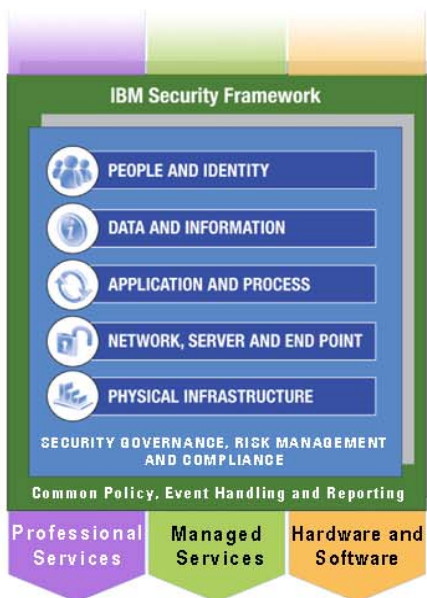
Design, and deploy a strong foundation for security & privacy



IBM Security Framework - Offering



-  Professional Services
-  Managed Services
-  Products
-  Cloud Delivered





Trusted Partner

Delivering secure products and services

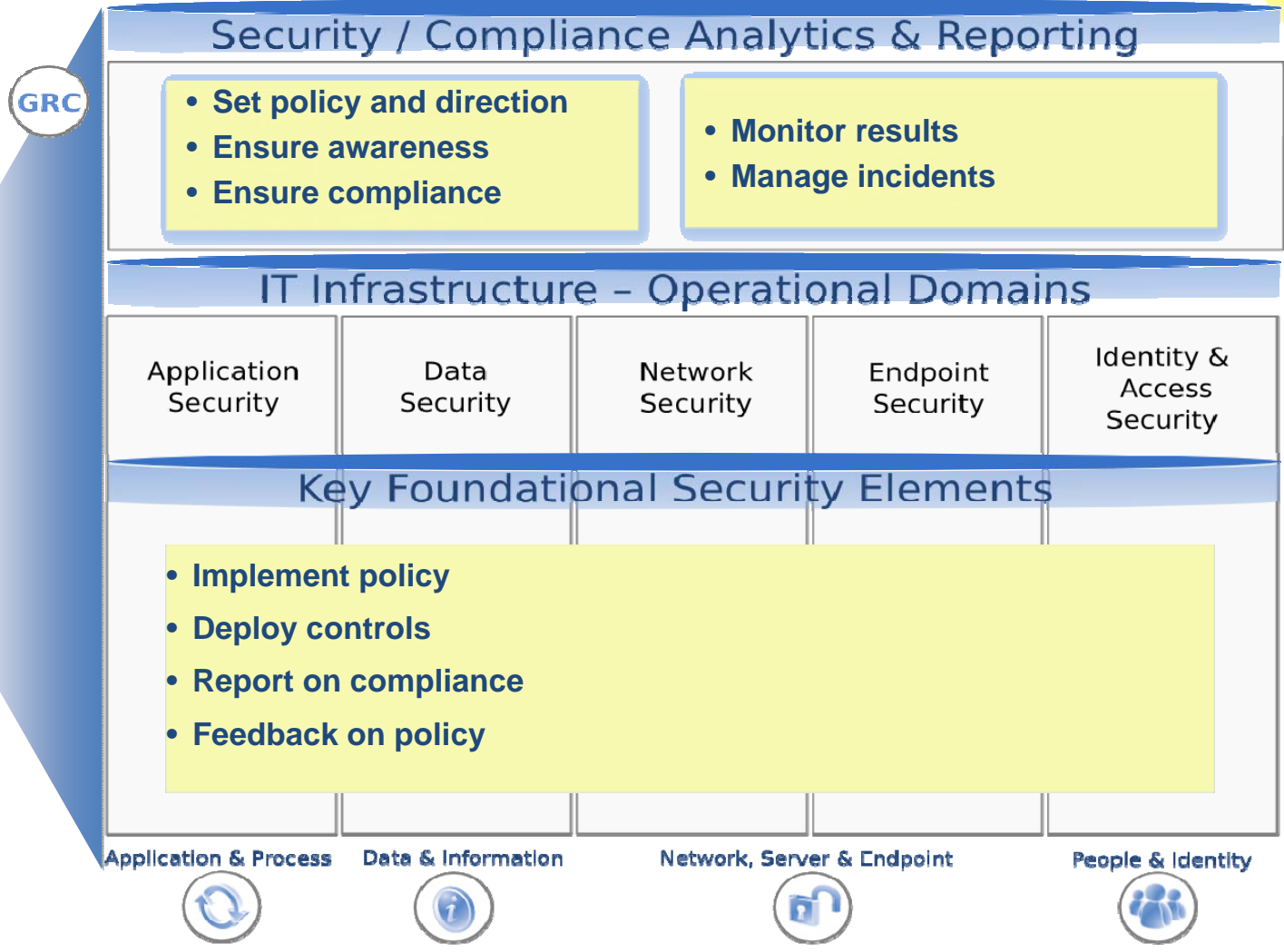
- **15,000** researchers, developers and SMEs on security initiatives
- **3,000+** security & risk management patents
- Implemented **1000s** of security projects
- **40+** years of proven success securing the zSeries environment
- Managing **over 7 Billion** security events per day for clients
- **Over 4B spent** in security company acquisitions over the last 5 years

Trusted Security Vendor

Providing end-to-end coverage across all security domains



IBM Security Framework at Customers



IBM Security Framework Addressing Hottest Issues



GRC

Security / Compliance Analytics & Reporting

- Compliance, compliance, compliance
- Understanding control sets needed
- Threat / compliance research gap
- Data overload
- Work overload
- Expertise shortage

IT Infrastructure - Operational Domains

Application Security	Data Security	Network Security	Endpoint Security	Identity & Access Security
----------------------	---------------	------------------	-------------------	----------------------------

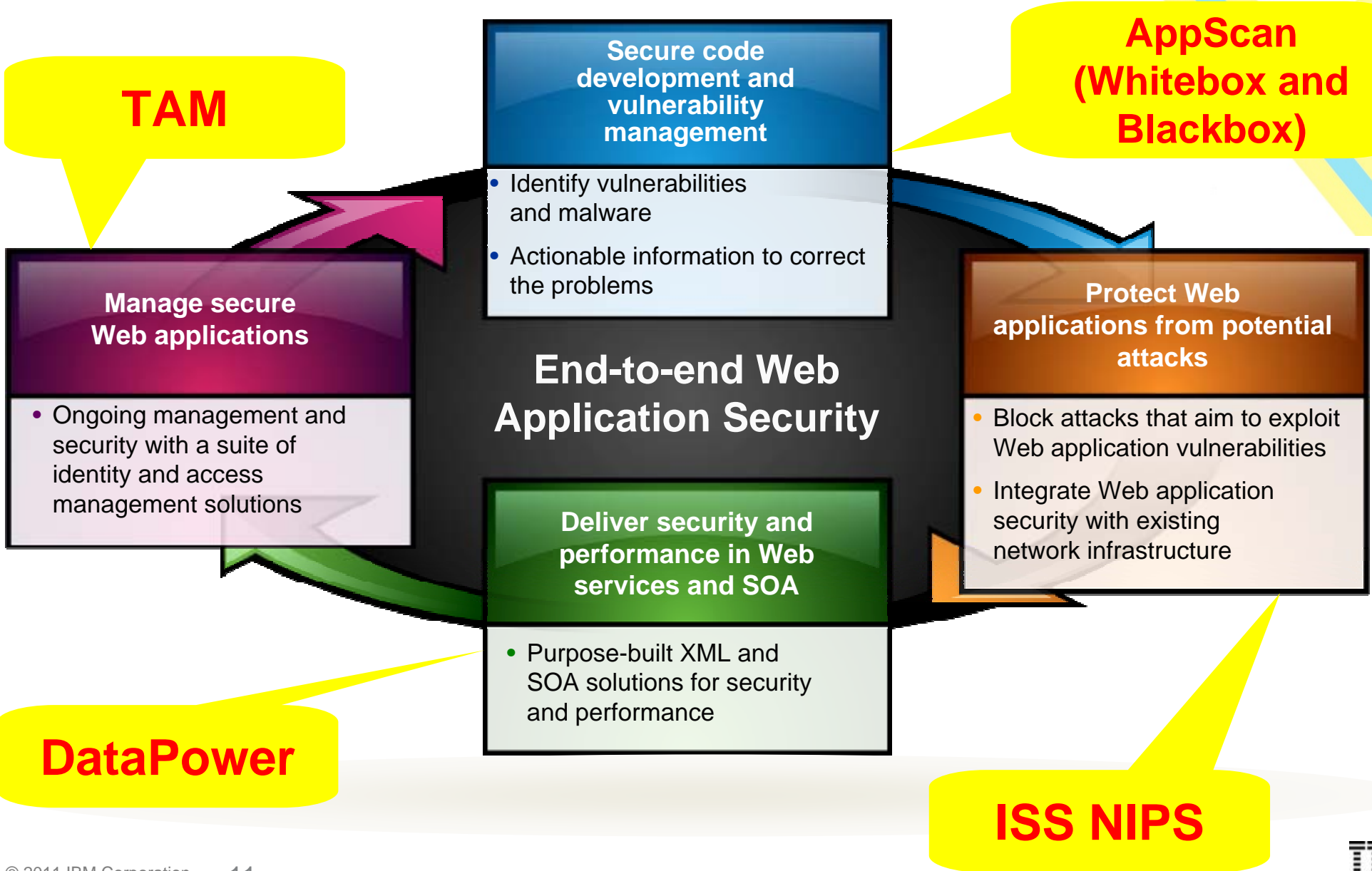
Key Foundational Security Elements

<ul style="list-style-type: none"> • #1 attack vector • Hard to patch • Testing • Getting to secure coding... 	<ul style="list-style-type: none"> • Leakage = risk = cost • Company IP is top target • Where is sensitive data?... 	<ul style="list-style-type: none"> • 10G+++ • Threat protection • Inbound and out • Layered approach... 	<ul style="list-style-type: none"> • Sprawl • Mobility • Unknown risk • ↑ control, ↓ cost... 	<ul style="list-style-type: none"> • Defining roles • Privileged user risk • ↓ cost
---	--	---	--	--

Appl cation & Process Data & Information Network, Server & Endpoint People & Identity



IBM Security Framework for Web application





Secure by Design

*...managing risks in the
Development Lifecycle of
Products & Services.*

The Planet is getting more Instrumented, Interconnected and Intelligent... and also more Risk Sensitive



Smart Supply Chains



Smart Countries



Smart Retail



Smart Water Management



Smart Weather



Smart Energy Grids



 **INSTRUMENTED**

Smart Oil Field Technologies



Smart Regions



 **INTERCONNECTED**

Smart Healthcare



Smart Traffic Systems

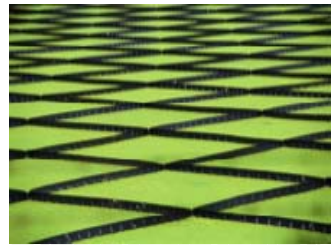


 **INTELLIGENT**

Smart Cities



Smart Food Systems

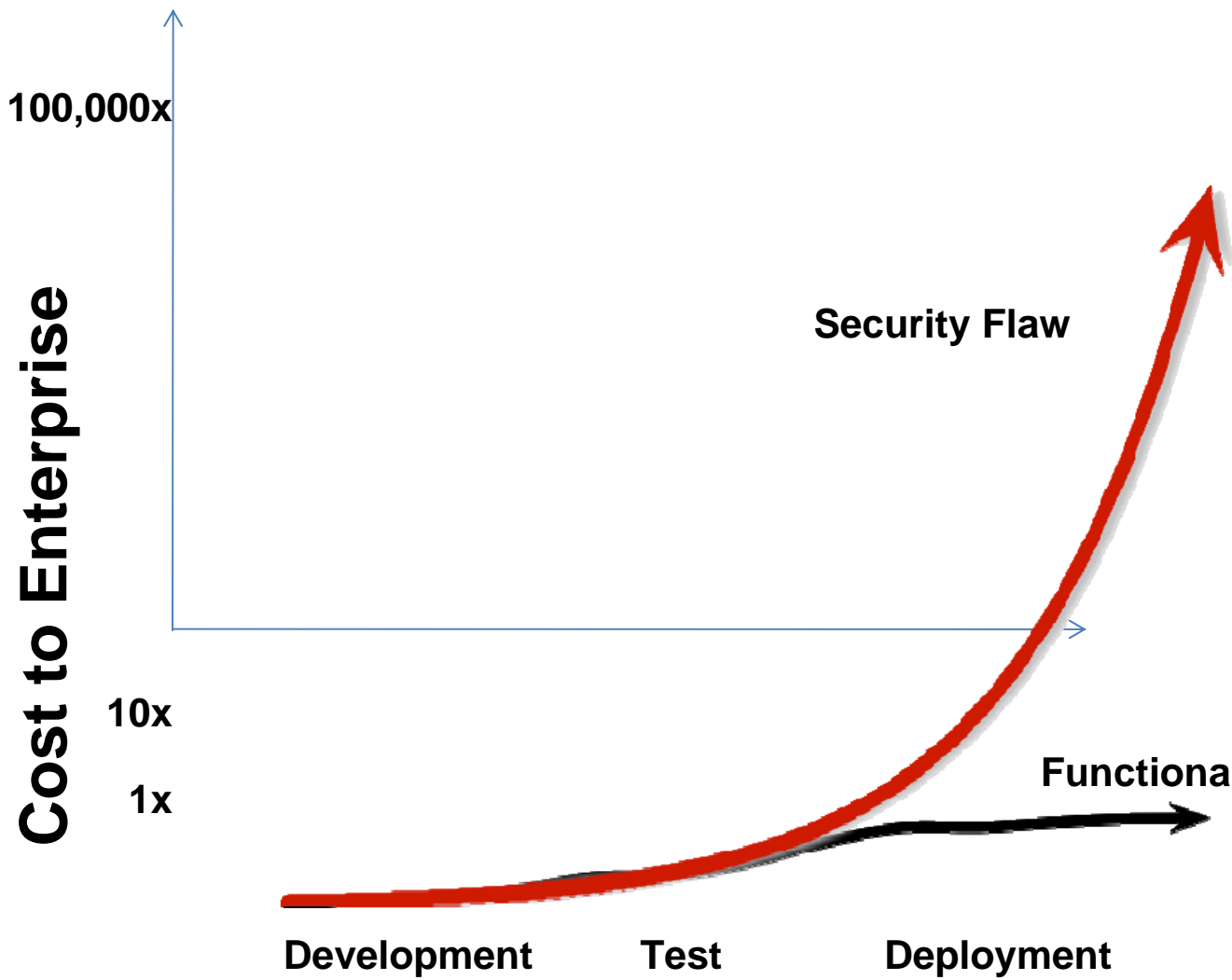




Many defects, security vulnerabilities and infrastructure failures can be traced back to the Development Process

<i>Root Cause</i>	<i>Development Process Response</i>
Insufficient knowledge	Role appropriate skills, Requirements process, System modeling and Risk analysis
Underestimation of influence	Threat modeling, Design for resilience, Fault analysis and Comprehensive test
Ignorance, carelessness, negligence	Rigorous engineering process
Forgetfulness	Training, Certification, Fitfulness
Relying upon others without control	Command Authority, Delegation of Authority
Objectively unknown situation	Complete use case definition and Test planning
Imprecise definition of responsibilities	Description of roles & responsibilities, communication and accountability
Choice of bad quality	Component selection and supply chain

The business motivator for *Secure by Design* is to control the Unbudgeted Costs from Vulnerabilities and Critical Breaches



- Unbudgeted Costs:**
- Customer notification / care
 - Government fines
 - Litigation
 - Reputational damage
 - Brand erosion
 - Cost to repair

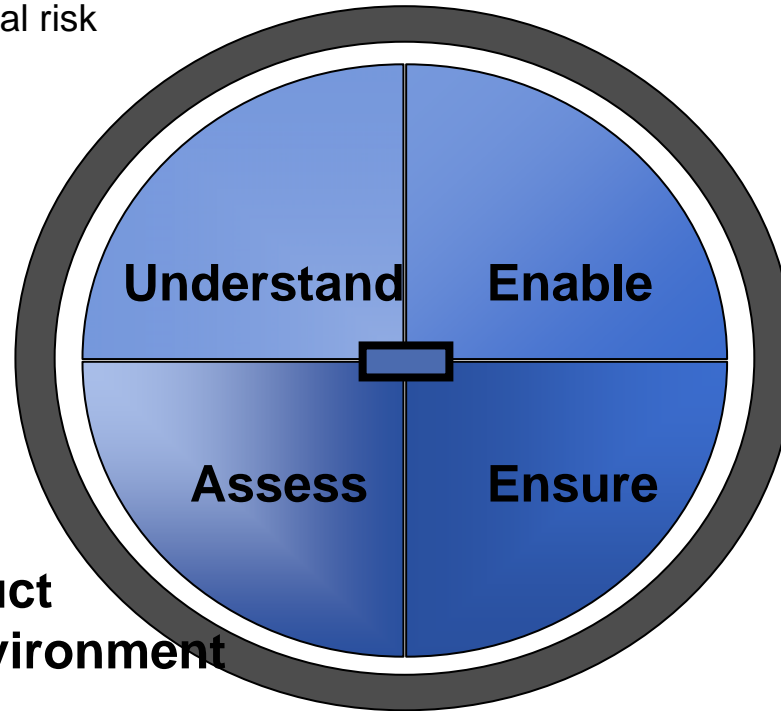




These causes and responses can be condensed into four imperatives

Understand Security Drivers

- Business, project and technical risk
- Requirements analysis
- Threats and Impacts
- System Model
- Document Use Cases and Anomaly conditions



Assess the end-product in its Operating Environment

- Test prior to deployment
- Verify security of platform configuration
- Process and schedule for regular checking
- Incident Handling process

Enable System Security

- Secure platform & configuration
- Appropriate security controls within applications
- System monitoring & logging
- Security management processes

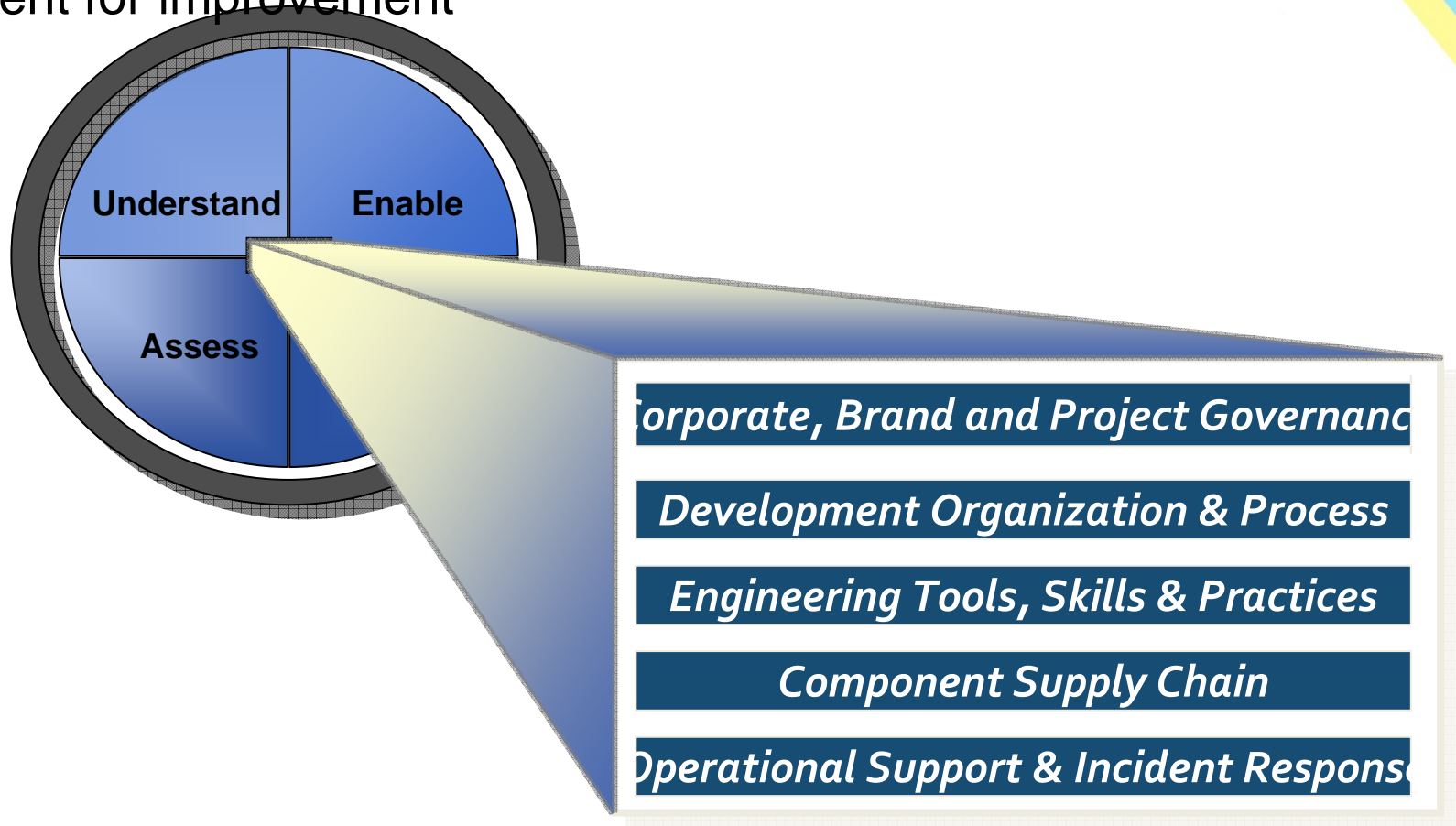
Ensure secure development

- Full attention to security in Development
- Protect development infrastructure
- Verify quality and provenance of third-party components & software
- Check system for security during coding/build/integration stages
- Accountability for process & results

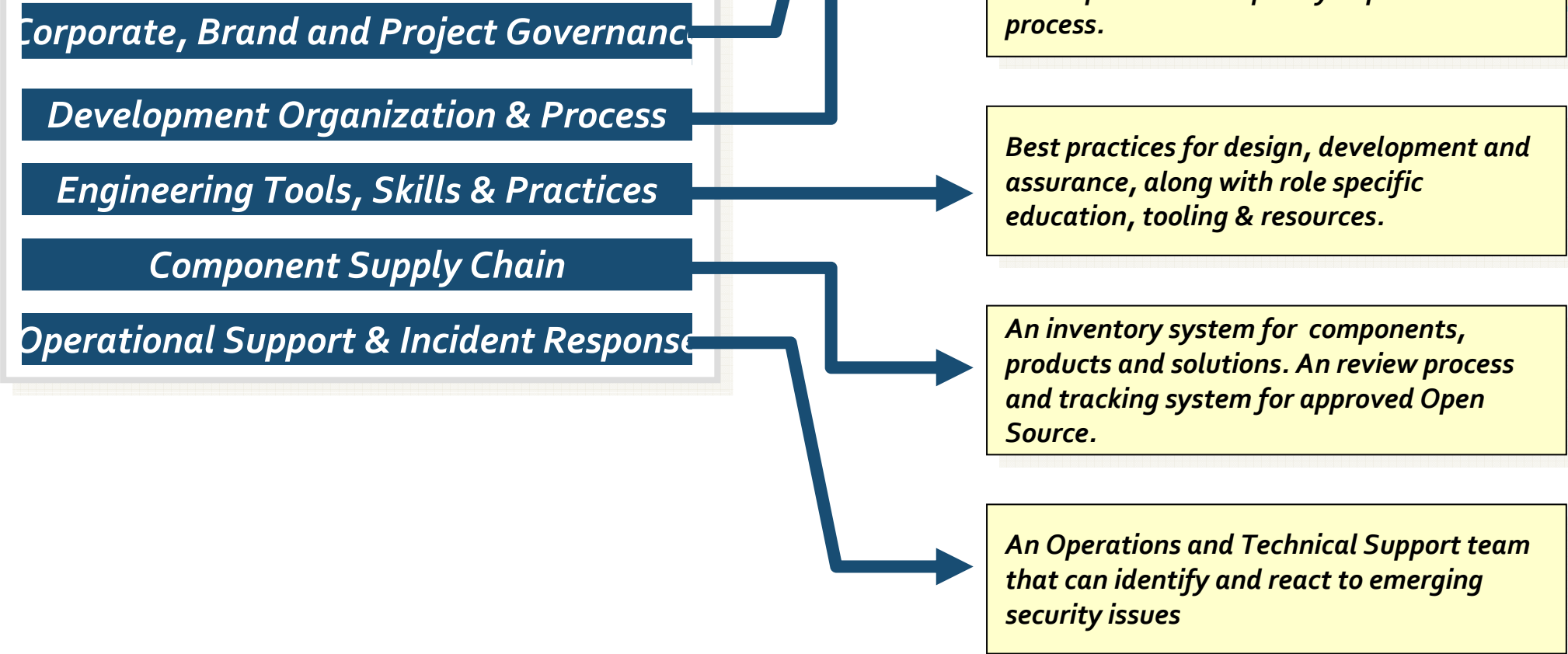


The keystones of a Secure by Design program

A successful program is built on Organizational Commitment and Process, Values Skills and Practices, a trusted supply chain and a commitment for improvement



The Keystones of a Secure by Design program





Thank you!

Roman TUMA
roman@sg.ibm.com