



Data Security

Part of Business Governance

Current Landscape

(Alignment with goals and objectives)



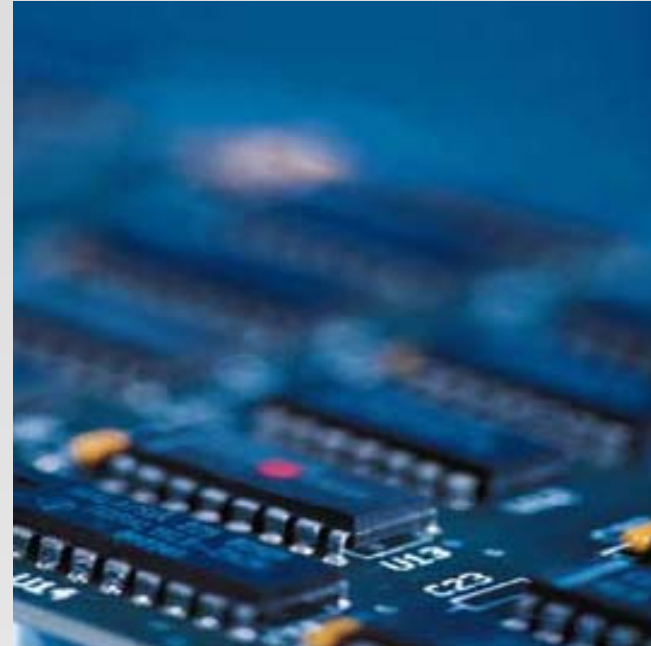
- Public and private sector enterprises today are *highly dependent* on information systems and processes to carry out their missions and business functions.
- Information is as much a *product* as any goods or services that are provided to customers or constituents
- To achieve mission and business success, enterprise information systems and processes must be *dependable* in the face of serious numerous *threats* allowable by numerous *vulnerabilities*.
- To achieve information confidentiality, integrity & availability, all systems must be appropriately *protected*.

Part of the Business Model

(Alignment with goals and objectives)



Connectivity



Complexity

The Weapons of Choice

(Very Different)



- Laptop computers, hand-held devices, cell phones.
- Sophisticated attack tools and techniques downloadable from the Internet.
- World-wide telecommunication networks including telephone networks, radio, and microwave.

Resulting in low-cost, highly destructive attack potential.

- Today's economic world is also causing internal attacks from either disgruntled or dire employees

Resulting in threats by those close to our informational assets.

Data Security Framework

(Overview)



- Framework = set of closely related processes
- What does a framework bring?
 - Consistency
 - Staff confidence
 - Customer confidence
 - Internal Customers
 - External Customers
 - Quality
 - Repeatability
- Other considerations
 - Cross-function
 - Must be managed
 - Good processes are differentiators



Data Security Frameworks

(Modules)



- Process
 - Developing process to improve efficiency
 - Designed to improve robustness in program
 - Can be routine and institutional
- Quality control
 - Improving both content and process to more effectively deliver IT services
 - Build metrics to track performance and improvement
- Governance
 - Establishing oversight measures (evaluate metrics)
 - Ensuring responsibility is defined and understood

Data Security Governance

(Reaction to outside influences)



- There is an increased need to focus on the overall value of information, protected and delivered
- In the past decade, legislatures, statutory authorities and regulators have created a complex array of new laws and regulations designed to force improvement in both security & privacy
- Best practices have influenced managers to conform to controls established by the supporting organizations
- New laws on information retention and privacy, coupled with significant threats of information systems disruptions from hackers, worms, viruses and terrorists, have resulted in a need for a governance approach to information

Data Security Governance

(Interject into the Enterprise)



- Until recently, the focus of security had been on protecting the IT systems that process and store the vast majority of information, rather than on the information itself
- To achieve effectiveness and sustainability in today's complex, interconnected world, information security must not be regarded as a technical specialty relegated to the IT department
- It addresses the universe of risks, benefits and processes involved with all information resources. It must be addressed at the total enterprise level
- Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management and reporting combination is forcing management

Strategic oversight regarding information security:

- Understanding the criticality of information and information security to the organization
- Reviewing investment in information security for alignment with the organization strategy and risk profile
- Endorsing the development and implementation of a comprehensive information security program
- Requiring regular reports from management on the program adequacy and effectiveness

IBM, *Data Governance Council, Oversight of Information Security*, USA, 2005

Data Security Governance

(Results)



The five basic outcomes of information security governance include:

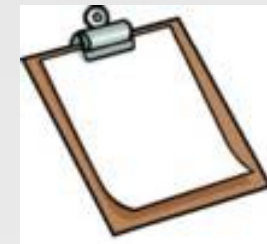
- Strategic alignment of information security with business strategy to support organizational objectives
- Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level
- Resource management by utilizing information security knowledge and infrastructure efficiently and effectively
- Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved
- Value delivery by optimizing information security investments in support of organizational objectives

Data Security Program

(Major Portions)



- Development/maintenance of security policies
- Assignment of roles, responsibilities, authority and accountability
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
- Periodic assessments of risks and business impact analyses
- Classification and assignment of ownership of information assets
- Adequate, effective and tested controls for people, processes and technology



Data Security Program

(Major Portions)



- Integration of security into all organizational processes
- Processes to monitor security elements
- Information security incident management
- Effective identity and access management processes for users and suppliers of information
- Meaningful monitoring and metrics of security performance
- Education of all users, managers and board members regarding information security requirements



Business Drivers

(Program Justification)



- Information as an asset
 - Confidentiality
 - Integrity
 - Availability

- Justifiable Security
 - Gauging effectiveness of security options

- Cost Justification
 - Cost benefit analysis
 - Return on investment

- Accountability
 - HIPAA
 - Gramm-Leach-Bliley
 - Basel II
 - Sarbanes-Oakley
 - Notification Laws at federal and state levels

What is at Risk

(Private and Public)



- Information systems supporting Defense, Civil, and Intelligence agencies at all government levels.
- Private sector information systems supporting Russian industry and businesses (intellectual capital).
- Information systems supporting critical infrastructures within the Russia (public and private sector) including:
 - Energy
 - Transportation
 - Public Health Systems / Emergency Services
 - Information and Telecommunications
 - Defense Industry
 - Banking and Finance
 - Postal and Shipping
 - Agriculture / Food / Water / Chemical

Part of the Business Model

(Alignment with goals and objectives)



- Critical infrastructure protection must be a partnership between the public and private sectors.
- Information security solutions must be broad-based, consensus-driven, and address the ongoing needs of government and industry.
- Enterprise missions and business processes drive security requirements and associated safeguards and countermeasures for the total organization.
- Highly flexible implementation; recognizing diversity in mission/business processes and operational environments.
- Senior leaders take ownership of their security plans including the safeguards/countermeasures for the total information processing.
- Senior leaders are both responsible and accountable for their information security decisions; understanding, acknowledging, and explicitly accepting resulting mission/business risk.

Information Security Programs

(Enterprise and Departmental)



Links in the Security Chain; Administrative, Technical, Operational and Physical Controls

- Risk assessment
- Security planning, policies, procedures
- Configuration management and control
- Contingency planning
- Incident response planning
- Security awareness and training
- Security in acquisitions
- Physical security
- Personnel security
- Security assessments
- Certification and accreditation
- Access control mechanisms
- Identification & authentication mechanisms (Biometrics, tokens, passwords)
- Audit mechanisms
- Encryption mechanisms
- Boundary and network protection devices (Firewalls, guards, routers, gateways)
- Intrusion protection/detection systems
- Security configuration settings
- Anti-viral, anti-spam, anti-spyware software
- Smart Cards

Apply a balanced set of controls for an defense-in-depth approach.

Risk Management Framework

(Uses)



- **The Risk Management Framework and the associated security standards and guidance documents provide a process that is:**

- **Disciplined**
- **Flexible**
- **Extensible**
- **Repeatable**
- **Organized**
- **Structured**

“Building information security into the infrastructure of the organization... so that critical enterprise missions and business cases will be protected.”

Risk Management Framework

(Scope)



- Defining Informational Risk
- Main Causes of Risk in a Technology Environment
- Primary Risk Management – A Foundation or Baseline
 - Infrastructure
 - Applications
 - Employees/staff
 - Controls and processes
 - Risk Findings

Risk Management Framework

(Must be Done Correctly)



- Risk Management takes time and money
- Risk Management more effective and efficient than Risk Avoidance



Risk Management

(Reasons)

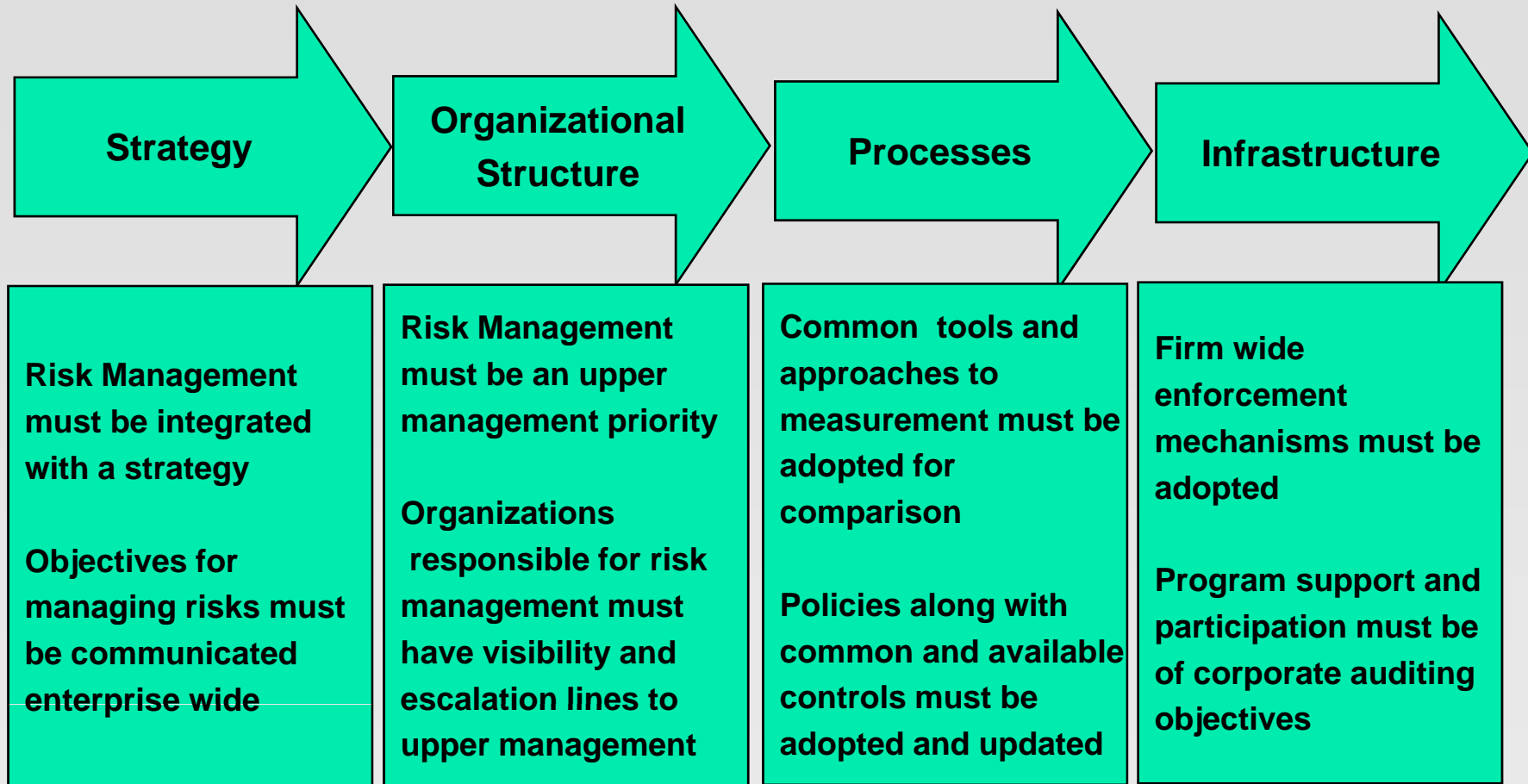


Why should one assess informational risk?

- "Information is an asset"
- BS7799 Standards
- ISO Series of Standards
- COSO
- Basel II
- NIST SP-800 Series
- ITIL
- Russian Presidential Decrees
- Constitution of the Russian Federation
- On Information, Informatization and the Defense of Information
- System for Investigations and Field Operations (SORM)

Risk Management

(Enterprise Wide Process)



Information Quality Assurance Program

(Modules)

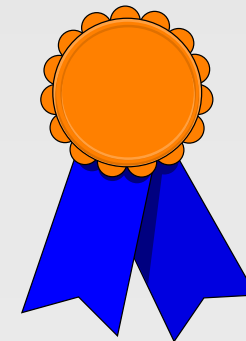


- Customer Requirements Analysis
 - Information
 - Security
 - Legal and Regulatory

- Risk Analysis
- Proprietary Controls

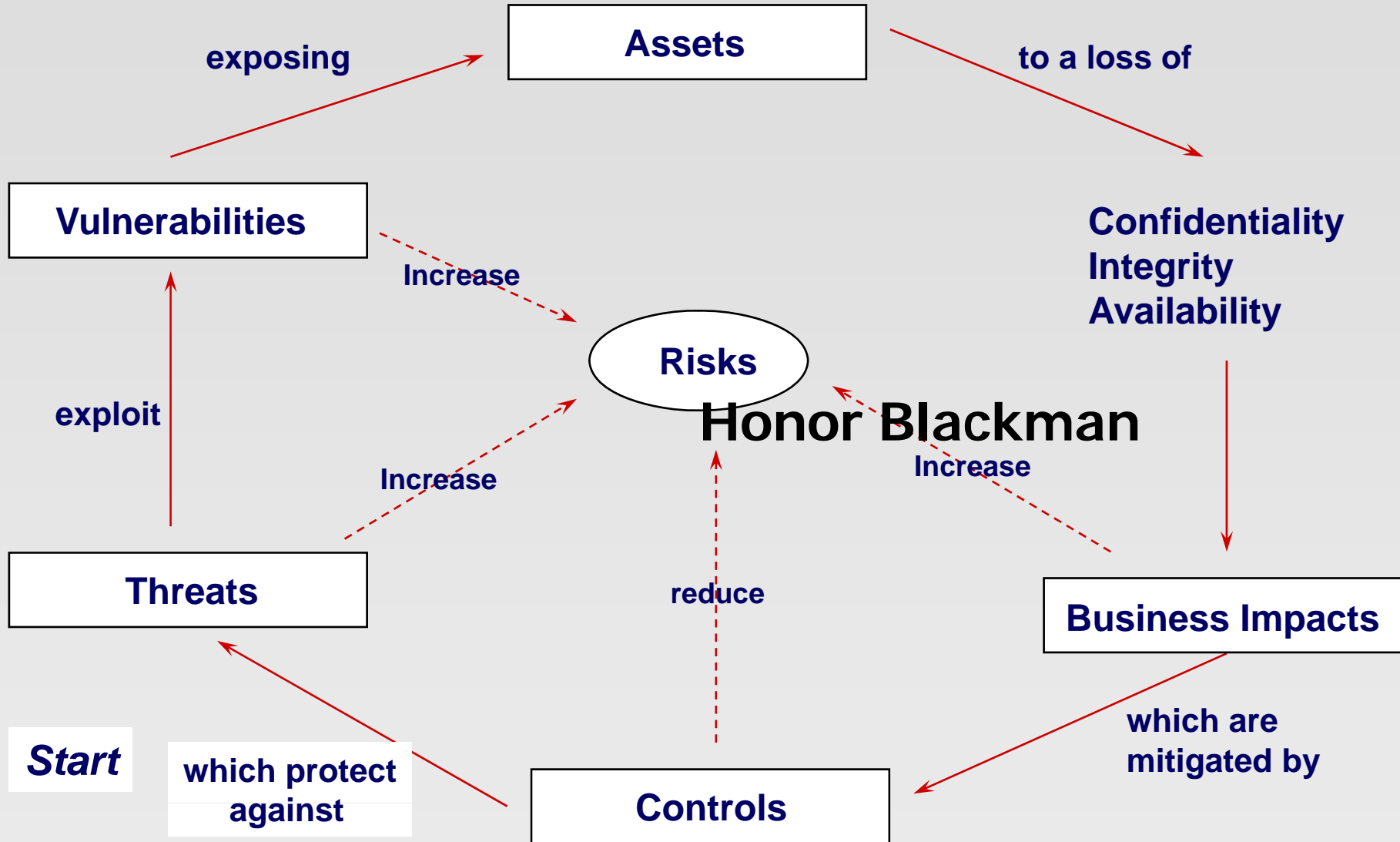
- Business Impact Analysis

- Critical Resource Analysis



Information Quality Assurance Program

(Process Diagram)



Risk Analysis

(Simple Action Report)



RISK ANALYSIS PROCESS -- ACTION PLAN

Target: _____ Date: _____

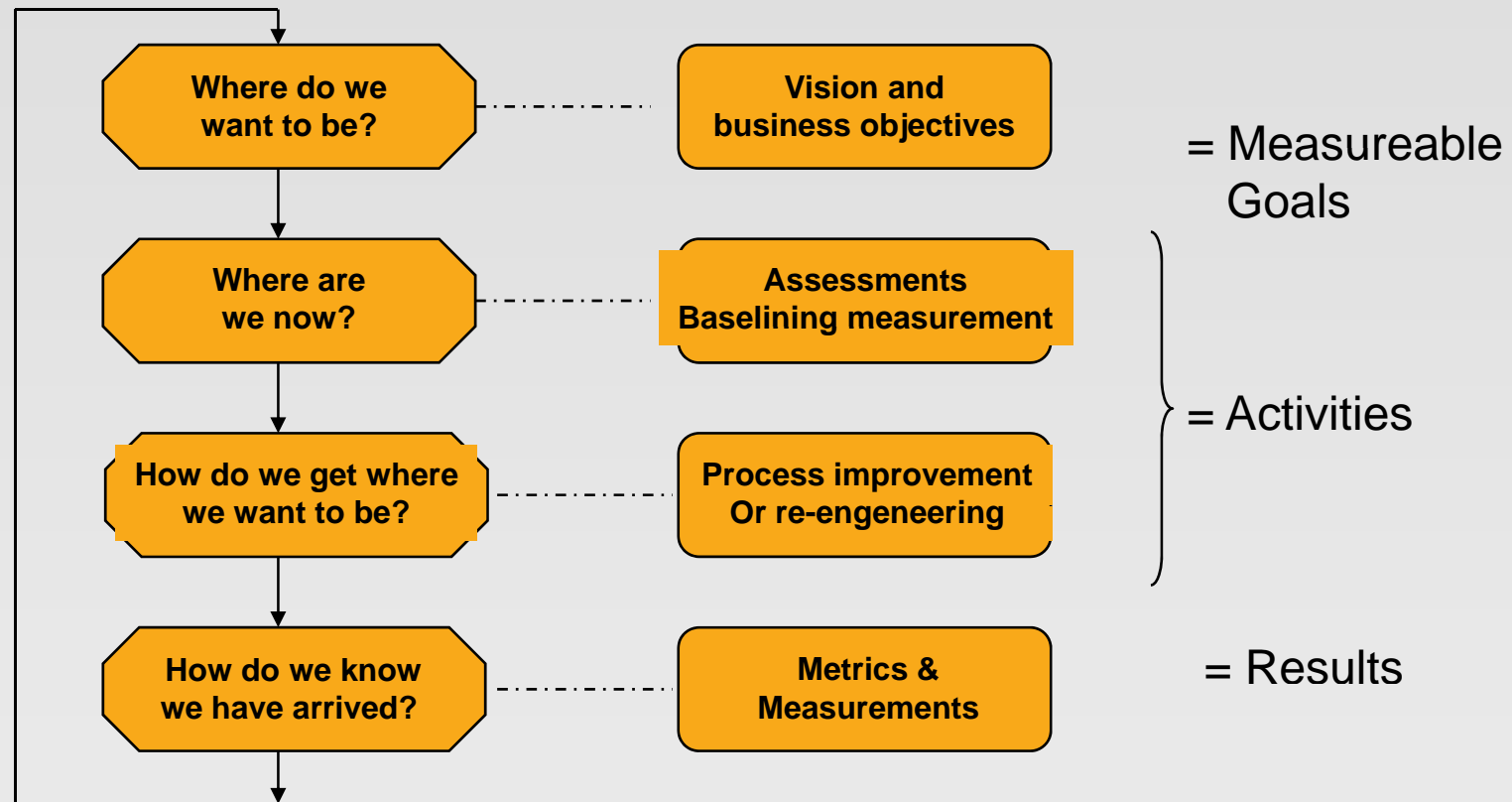
RISK #	ASSET	THREAT	VULNERABILITY	PRIOR	PRESENT CONTROLS	A/L	POTENTIAL CONTROLS	INVESTIGATION RESULTS	ACTION ITEMS	PERTINENT DATES AND STATUS

Focus on the Process for Data Security

(Uses)



Process lifecycle



Security Metrics

(Very Different)



- Capture relevant security operations information
- Create usable reports to display program performance
- Meeting enterprise objectives
- Assists in informed decision making
- Manage security as a business process
- Demonstrate the efficiency of the security program
- A way to pursue your security and privacy practice as a disciplined science and not an art form

Aligning Business and Data Security

(Four Areas)



Four Priorities

- Build and emphasize governance – how should the Data Security Organization operate?
- Identify gaps between present practice and a set of best practices
- Prioritize remediation projects that support the business processes
- Establish a conduit to the following groups
 - Data Security Organization
 - Business Units
 - Necessary Steering Committees

Governance

(Key Questions)



- Does your company have the right set of policies, procedures, standards and rules for change management, security and privacy?
- Are critical IT and data assets classified by level of importance?
- What security measures do you take to protect your informational assets?

Gap Analysis

(Key Questions)



Best Practice Deployment

- What methodology or best practice does your company employ to define and verify security requirements?
 - How is the assessment conducted?
 - How is the assessment used?

Logical Access

- How do you restrict access to informational assets?
- Who grants or provisions access rights? Who reconciles those access rights?
- Does the business apply role based or rule based access control?
- Have these roles and functions been monitored and reviewed in the past three to six months?

Remediation

(Follow-Up to Risk and Gap Analysis)



- Have you captured relevant security operations information?
 - Initial (benchmark)
 - On going)

- Have you prioritized remediation efforts based on risk prioritization?

- What are your remediation objectives for any identified deficiency?

- How will provide set reachable targets on delivering remediate controls?

- Have you developed a roadmap?

Communications Plan

(Enterprise Wide)



- Do you know what your CEO, CIO or other corporate officers need to know regarding Data Security efforts?
- Do you know what your business units need to know regarding Data Security efforts?
- Can you monitor informational risks and how to prioritize them?
- Can you to monitor, evaluate and communicate internal controls?
- Can you create reachable targets on delivering remediate controls on in-scope systems and IT processes?
- *Finally, use a lot of common sense and do not loose momentum.*

Questions