

Project Management Institute
Risk Management SIG
Project Risk Symposium 2004

May 18, 2004

A Disciplined Risk Management Approach to E-Commerce Projects

Presented by:

Art Drake

Director of Business Assurance Services

Executive Chair PMI-PMOSIG

- ▶ **Define e-commerce project risks**
- ▶ **How e-commerce risks relate to enterprise risks**
- ▶ **Define an appropriate risk management process for e-commerce projects**
- ▶ **Mitigation strategies relevant during and after an e-commerce project implementation**
- ▶ **A Case study**

E-Commerce Stats

- ▶ **E-commerce vs. e-business – no differentiation**
- ▶ **E-commerce boom**
 - **Electronic transactions = US Census Bureau**
 - **Cost of doing business = \$90.00 vs \$4.44 (ePaynews.com)**
 - **B2B transactions in 2004 = \$1.1T (Keenan Vision)**
 - **US e-comm revenues for 2004 = \$3.5T, worldwide = \$6.0T (Forrester)**
- ▶ **E-commerce includes: bill payment, supply chain, education, auctions, entertainment**

E-Commerce Challenges

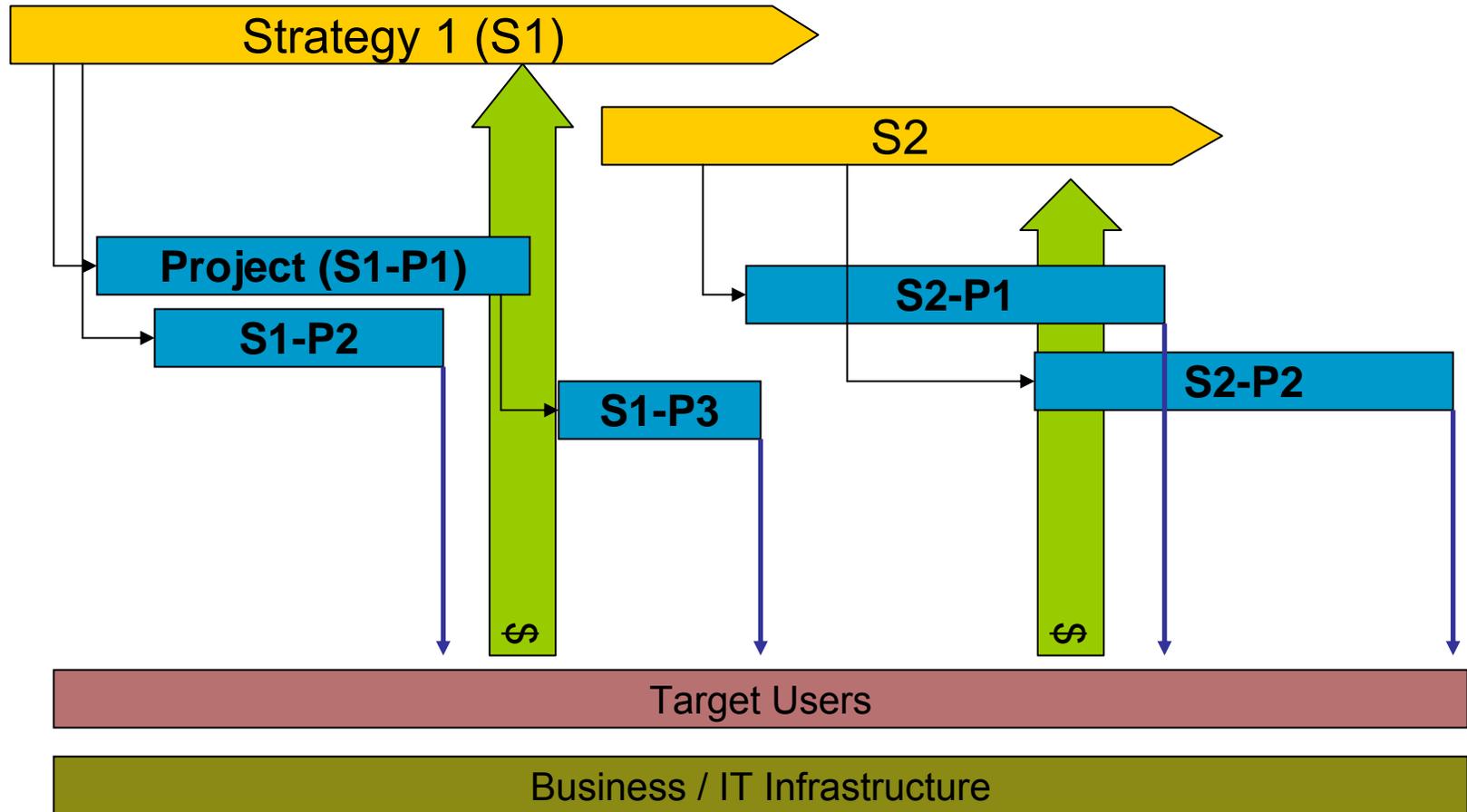
► Drivers

- Increase revenue (new markets, broader reach)
- Decrease cost (more efficient processes)
- Build brand strength
- Faster response to market changes

► Requires a new business model (if not forced)

- Logistics (fulfillment, distribution, inventory mgmt, virtual sourcing)
- Learning (customers as users, knowledge management)
- Human factors (ease of use, usage monitoring, managing expectations)
- Trust (security, integrity, accuracy)
- Reliability (availability, performance, continuity)
- Optimization (business process reengineering)

Agile Project Delivery



Common Project Risks

► The Usual Suspects

- Cost
- Schedule
- Quality
- Poor requirements
- New technologies
- Delayed deliveries
- Budget pressures
- Changing personnel
- Lack of commitment
- Over committed resources
- Lack of testing
- Competing priorities
- Playground politics
- Unavailable technology



Project Risk Management

► PMBOK Basics

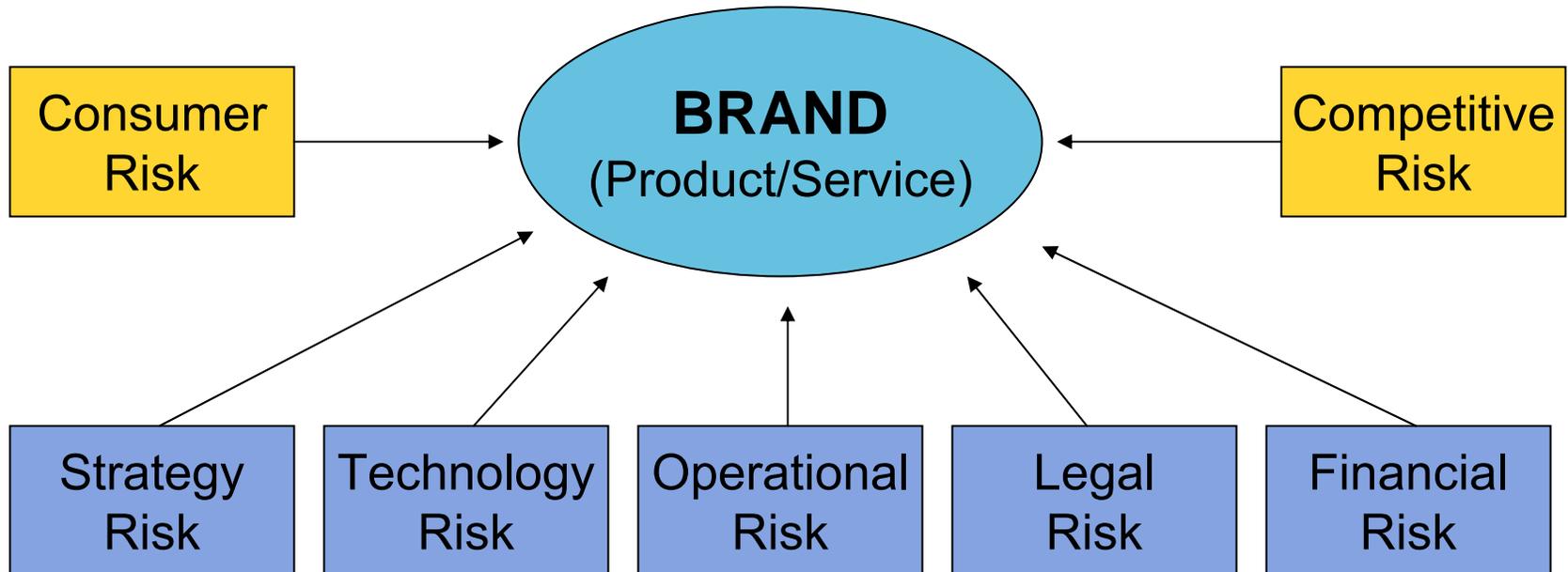
- **Risk Management Planning** – *how are we going to manage risk?*
- **Risk Identification** – *how will we identify and understand risks?*
- **Qualitative Risk Analysis** – *what types of risks are we dealing with and in what priority?*
- **Quantifiable Risk Analysis** – *what's the probability and potential consequences of each identified risk?*
- **Risk Response Planning** – *how will we respond in the event a risk is realized?*
- **Risk Monitoring** – *how will we incorporate and communicate changes in our risk planning and tracking?*

Enterprise Risk Perspectives

“As business interdependency grows – the total cost and probability of downtime soars.”

“With business dependency on technology growing, senior executives must take care to understand how and where their risk have changed and take the necessary steps to protect themselves, or else face suffering serious disruptions and loss of productivity at best, and at worst irreparable damage to their reputation, severe legal penalties, or even the loss of the entire business.”

The Enterprise Perspective



▶ Relationship to Enterprise Risks

- Direct impact on revenues
- Direct impact on profitability
- Real liabilities
 - Litigation - class-action lawsuits – share value failures
 - Brand theft/damage – loss of 2.1% market share
 - Intellectual property loss - \$2.7m/incident
 - Non-compliance fines – not yet tested to the limit (HIPAA)

▶ Residual Risks

▶ **Consumer Risk**

- Alternative products
- Level of satisfaction with experience

▶ **Competitive Risk**

- New or improved competitive product
- New strategy

▶ **Strategy Risk**

- Continued alignment with company strategy
- Execution and window of opportunity

▶ **Operational Risk**

- Increased logistics (value chain)
- Lost productivity due to new and/or parallel processes

▶ **Legal Risk**

- Compliance with controls, privacy and security regulations
- Litigation of failed value delivery
- Digital copyrights

▶ **Financial Risk**

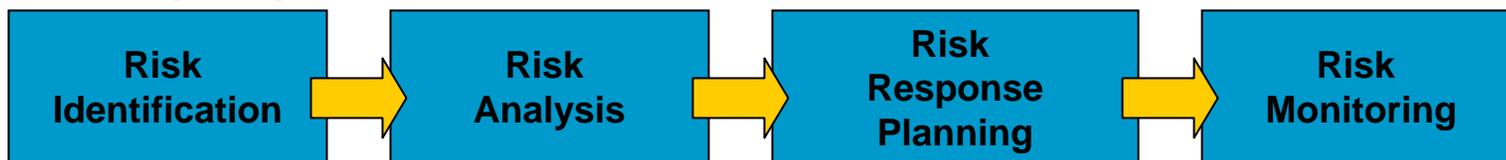
- Missed return-on-investment obligations
- Fraud
- Loss due to interruption

▶ **Technology Risk**

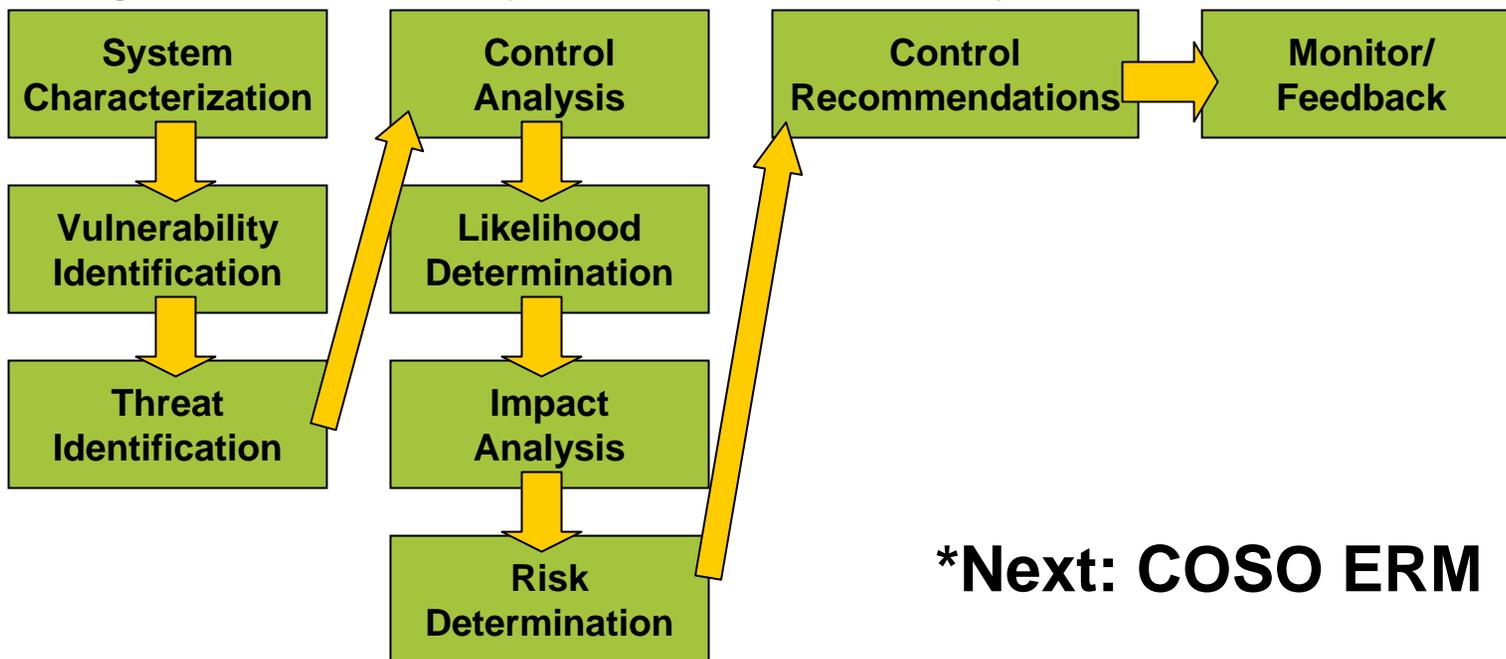
- Security failure
- Compromised data and/or applications
- Increased failure points

Existing Frameworks

► Project Risk (PMI)



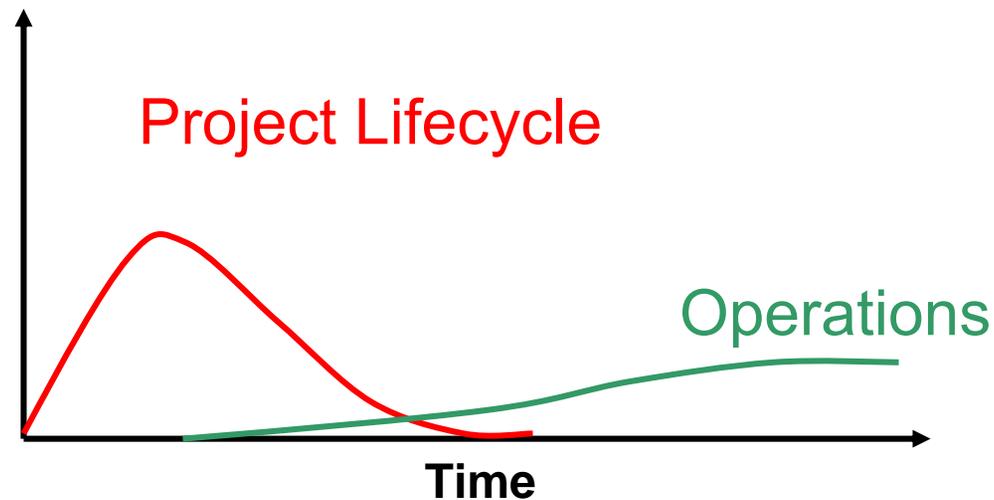
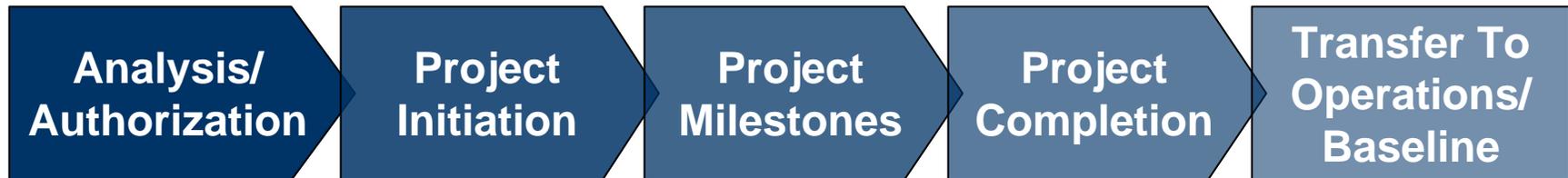
► Risk Management (Security) for Information Systems (NIST)



***Next: COSO ERM**

Project Governance

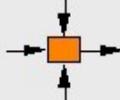
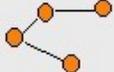
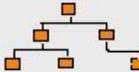
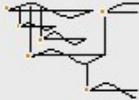
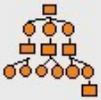
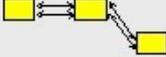
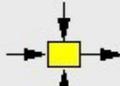
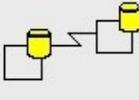
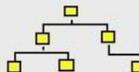
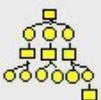
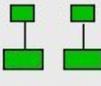
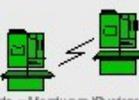
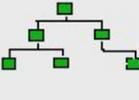
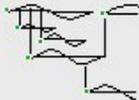
► Extended Project Lifecycle



Risk Fundamentals

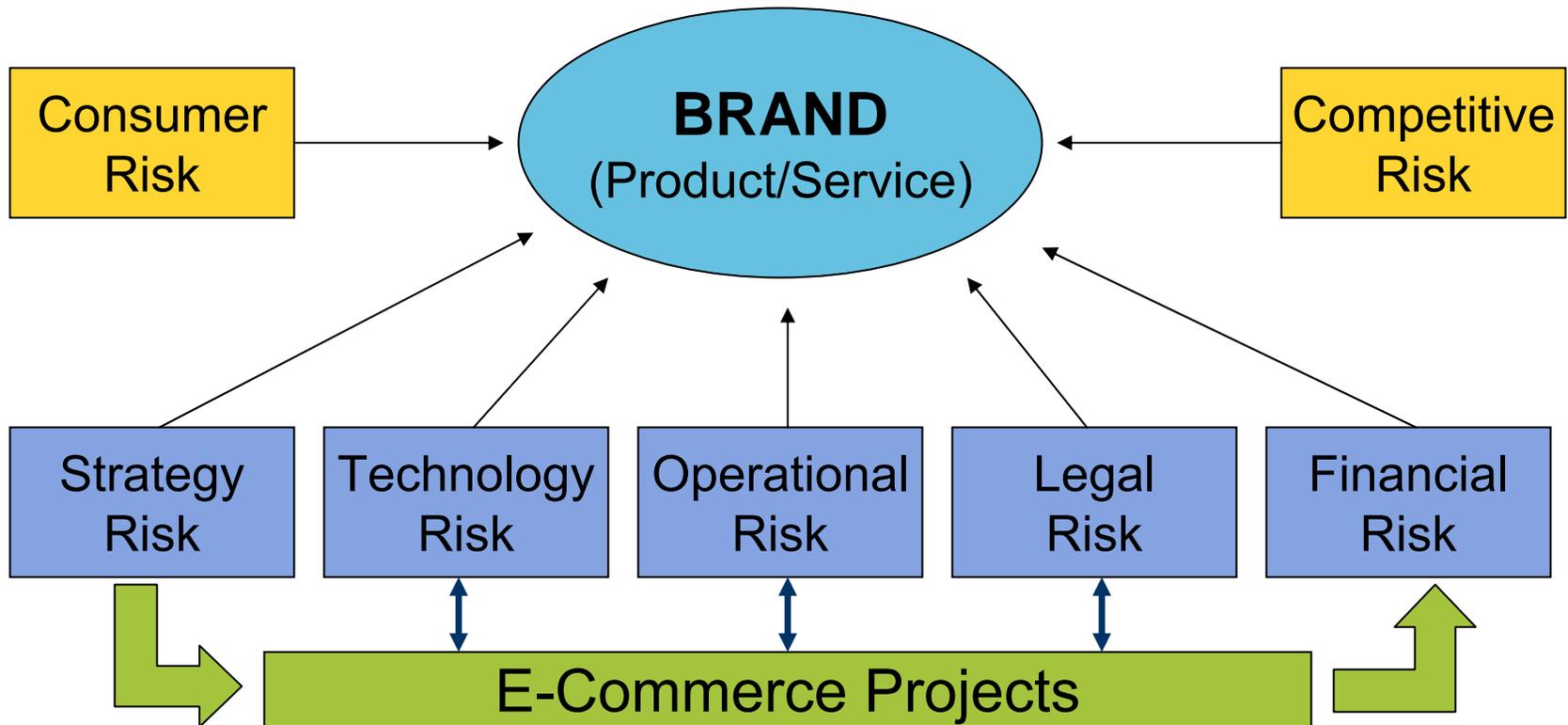
- ▶ **Awareness: What are we up against?**
- ▶ **Context Why is this an issue?**
- ▶ **Contemplation: What are our options and when do we act?**
- ▶ **Reflection: Has the situation or conditions changed?**
- ▶ **Anticipation: What can we expect as a result of conditions or our actions?**

An Enterprise View

abstractions	DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION
perspectives	What	How	Where	Who	When	Why
SCOPE <i>Planner</i> contextual	List of Things - Important to the Business  Entity = Class of Business Thing	List of Processes - the Business Performs  Function = Class of Business Process	List of Locations - in which the Business Operates  Node = Major Business Location	List of Organizations - Important to the Business  People = Class of People and Major Organizations	List of Events - Significant to the Business  Time = Major Business Event	List of Business Goals and Strategies  Ends/Means=Major Business Goal/Critical Success Factor
ENTERPRISE MODEL <i>Owner</i> conceptual	e.g., Semantic Model  Entity = Business Entity Rel. = Business Relationship	e.g., Business Process Model  Process = Business Process IO = Business Resources	e.g., Logistics Network  Node = Business Location Link = Business Linkage	e.g., Work Flow Model  People = Organization Unit Work = Work Product	e.g., Master Schedule  Time = Business Event Cycle = Business Cycle	e.g., Business Plan  End = Business Objective Means = Business Strategy
SYSTEM MODEL <i>Designer</i> logical	e.g., Logical Data Model  Entity = Data Entity Rel. = Data Relationship	e.g., Application Architecture  Process = Application Function IO = User Views	e.g., Distributed System Architecture  Node = IS Function Link = Line Characteristics	e.g., Human Interface Architecture  People = Role Work = Deliverable	e.g., Processing Structure  Time = System Event Cycle = Processing Cycle	e.g., Business Rule Model  End = Structural Assertion Means = Action Assertion
TECHNOLOGY CONSTRAINED MODEL <i>Builder</i> physical	e.g., Physical Data Model  Entity = Tables/Segments/etc. Rel. = Key/Point/etc.	e.g., System Design  Process = Computer Function IO = Data Elements/Sets	e.g., Technical Architecture  Node = Hardware/System Software Link = Line Specifications	e.g., Presentation Architecture  People = User Work = Screen/Device Format	e.g., Control Structure  Time = Execute Cycle = Component Cycle	e.g., Rule Design  End = Condition Means = Action
DETAILED REPRESENTATIONS <i>Subcontractor</i> out-of-context	e.g. Data Definition  Entity = Field Rel. = Address	e.g. Program  Process = Language Statement IO = Control Block	e.g. Network Architecture  Node = Addresses Link = Protocols	e.g. Security Architecture  People = Identity Work = Job	e.g. Timing Definition  Time = Interrupt Cycle = Machine Cycle	e.g. Rule Specification  End = Sub-condition Means = Step
FUNCTIONING ENTERPRISE	DATA Implementation	FUNCTION Implementation	NETWORK Implementation	ORGANIZATION Implementation	SCHEDULE Implementation	STRATEGY Implementation

John A. Zachman, Zachman International

E-nterprise Risks



► How do we know our risk strategies are working?

Risk Area	Feedback / Indicators
Strategy	<ul style="list-style-type: none">■ Negative change in revenue/operating costs■ Decline of customer base■ Decline in market share
Operations	<ul style="list-style-type: none">■ Increased operating and/or per-unit costs■ Lost productivity■ Decline in quality and/or on-time performance
Legal	<ul style="list-style-type: none">■ Increase in complaints/litigation■ Increase in audits and resulting fines
Financial	<ul style="list-style-type: none">■ Negative change in revenue/operating costs■ Missed ROI performance■ Loss in share value
Technology	<ul style="list-style-type: none">■ Security?■ Reliability?

Strategy Risks

Strategic	Tactical
<ul style="list-style-type: none">■ Project is clearly aligned with business objectives	<ul style="list-style-type: none">■ Value Owner is identified and participates as project sponsor
<ul style="list-style-type: none">■ Project success factors are tied directly to key performance indicators (KPIs)	<ul style="list-style-type: none">■ Milestones deliver measured value to business unit(s)
<ul style="list-style-type: none">■ Use portfolio management techniques to monitor project performance and relevance	<ul style="list-style-type: none">■ Milestones align with overall strategic implications (market opportunity, marketing objectives, etc.)

Operational Risks

Strategic	Tactical
<ul style="list-style-type: none">■ Establish sound governance program (Sarbanes-Oxley)	<ul style="list-style-type: none">■ Incorporate governance principles into project charter, project quality assurance plan, project risk management plan.
<ul style="list-style-type: none">■ Clearly defining how the new application will affect people and process	<ul style="list-style-type: none">■ Ensure affected business units are represented in discovery and requirements phases
<ul style="list-style-type: none">■ Clearly define transition plan that accounts for budget and productivity impacts	<ul style="list-style-type: none">■ Begin transfer process as early as possible to build commitment

Strategic	Tactical
<ul style="list-style-type: none">■ Establish sound compliance program (Sarbanes-Oxley, HIPAA, etc.)	<ul style="list-style-type: none">■ Incorporate compliance principles into project charter, project quality assurance plan, project risk management plan.
<ul style="list-style-type: none">■ Establish sound system controls program (Sarbanes-Oxley, HIPAA, others)	<ul style="list-style-type: none">■ Project deliverables must meet compliance requirements and be approved
<ul style="list-style-type: none">■ Establish sound security program principles (policy, procedures, design requirements)	<ul style="list-style-type: none">■ Project deliverables must meet security requirements and be approved

Financial Risks

Strategic	Tactical
<ul style="list-style-type: none">■ Monitor project portfolio performance to ensure all projects are still viable	<ul style="list-style-type: none">■ Continually monitor project progress and financial results (this should also include related project costs)
	<ul style="list-style-type: none">■ Complete post-project review to determine accuracy of costs and schedule

Technology Risk

- ▶ **All projects can affect and be affected by:**
 - **People**
 - **Process**
 - **Technology**

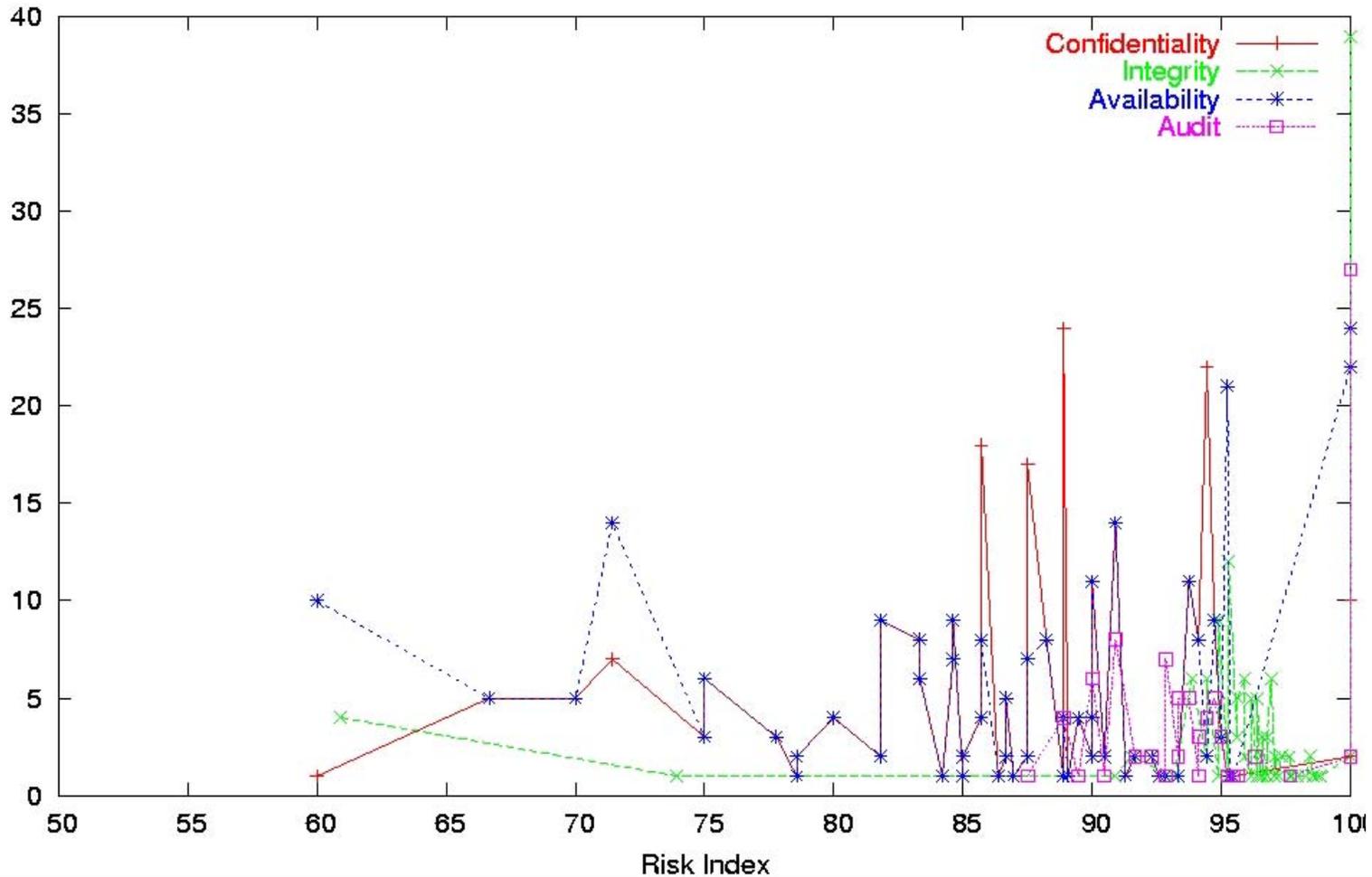
- ▶ **We can narrow technology risks into four areas:**
 - **Security**
 - **Reliability**
 - **Quality**
 - **Continuity**

Technology Risk

- ▶ **Security: Confidentiality, Integrity, Availability, Audit**
- ▶ **Reliability: Consistent, Responsive, Optimized**
- ▶ **Quality: Tested, User-Centric, Complies with requirements, Data Integrity, Bug-free**
- ▶ **Continuity: Managed, Recovery, Continuous Operation**

Measuring Technology Risk

SAMPLE ACME
Enterprise Risk Matrix
1/1/4



Business Assurance

- ▶ **A Framework For Addressing Technology Risks**
 - **Security**
 - **Reliability**
 - **Quality**
 - **Continuity**

	Security	Reliability	Quality	Continuity
Confidentiality	✓		✓	
Integrity	✓	✓	✓	✓
Availability	✓	✓		✓
Audit	✓	✓	✓	

Security Components

- ▶ **Availability of a Structured Security Program**
 - Charter, policies, standards, audit & monitoring, organizational competencies defined
- ▶ **Integration of a Security Review and Approval**
 - New technologies, integration, validation of outsourced hosting vendors, code review, incorporate security testing requirements into QA process, system performance issues (adding layers can add response time)
- ▶ **Legal Review and Approval**
 - Approval of content, privacy statement

Reliability Components

- ▶ **System Performance Monitoring & Optimization**
 - Determine how 'new' application will affect current production
 - Model 'new' application to determine opportunities for optimization
- ▶ **Overall System Architecture Review**
 - Determine impact of new application (sub-systems) on overall system architecture
 - Identify areas of vulnerability or potential failures
 - Determine redundancy (and load-balancing) requirements
- ▶ **Enforcing Data Integrity Standards**
 - Ensure the application follows data standards
 - Ensure the application information architecture standards

Quality Components

- ▶ **Well Defined and Execute Software QA Program**
 - Structured and automated software testing
 - Incorporate risk-based software testing techniques
 - Testing results feed into software improvement
- ▶ **Tighter Integration of Requirements to Testing**
 - Integrate QA requirements into requirements process
 - Establish critical testing criteria
- ▶ **Use of Release Management vs. Milestones**
 - Build on successful releases
 - Requires strong configuration management
- ▶ **Better Documentation**
 - Incorporate release notes into user documentation
 - Ensure user can learn the application with use

Continuity Components

- ▶ **Continuity Planning and Information Security Are Integrated**
 - Both groups are addressing risk
 - Both groups share responsibility for defining recovery policies and procedures
- ▶ **Alignment With Business Strategies and Priorities**
 - Determine any specific continuity/recovery procedures necessary due to the new application
 - Determine if new application affects existing Business Impact Analysis

	Risks	Mitigation Strategies
People	Lacking proper organizational structure	Recommend organizational requirements,
Process	Lack of procedures to authorize and/or terminate users	Include manual procedures as a business and design requirement – how should users be managed
Technology	Application code may contain 'holes' for hackers	Have code reviewed before production use

Industry	Financial Services – Large National Bank
Challenges	<ul style="list-style-type: none">■ Multiple online banking initiatives by multiple and diverse business units■ Technological “smorgasbord” from acquired/merged organizations■ Post-project technology assessment – bad news too late■ Post-implementation overruns
Changes	<ul style="list-style-type: none">■ Business units still retained autonomy in developing applications; but must have sign-off by IT operations on security, reliability and continuity.■ Pre-deployment technological assessment to determine potential risks and related mitigation costs

Thank You

Questions/Comments are always welcome.

Art Drake

adrake@upstreamsolutions.com

Art Drake,

Art Drake is currently the Director of Business Assurance Services for Upstream Solutions in Minneapolis, Minnesota. Mr. Drake has served in a wide range of consulting assignments covering program and project management, project quality assurance, project risk management, business process management, e-commerce project management, and implementing product quality assurance methodologies. Currently, Mr. Drake is involved with the development and implementation of risk management programs and strategies for clients that support security, business continuity, and compliance initiatives (e.g., HIPAA, Sarbanes-Oxley and GLBA). Art has consulted with clients in the financial services, manufacturing, healthcare and telecommunications industries. Art is an active member of the Project Management Institute (PMI), and is the Executive Chair of the PMI *Program Management Office Specific Interest Group (PMOSIG)*. Art also serves as the Chair of the local PMI *Risk Management Local Interest Group*. He can be reached at adrake@upstreamsolutions.com or at 612-961-4415.

