Rethinking Information Security Risk Management

Tanya Scott

Risk and Controls Senior Program Manager, Autodesk

Professional Strategies – S31

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

CyberSizeIT

SF ISACA FALL CONFERENCE

NOVEMBER 9-11, 2015

HOTEL NIKKO-SAN FRANCISCO

Disclaimer

The views expressed are my own, and do not reflect the official policy or position of any of my current or previous employers or clients.

Session Objectives & Agenda

Session Objectives

- Explore the definition of 'risk'
- Discover five concepts that can be utilized to guide the design and/or enhance an Information Security Risk Management (ISRM) program
- Identify creative ways to enhance your ISRM program

Agenda

- Overview
- Risk 101
- Deep Dive into 5 ISRM Concepts
- Closing Remarks

OVERVIEW

RISK 101

DEEP DIVE INTO 5 ISRM CONCEPTS

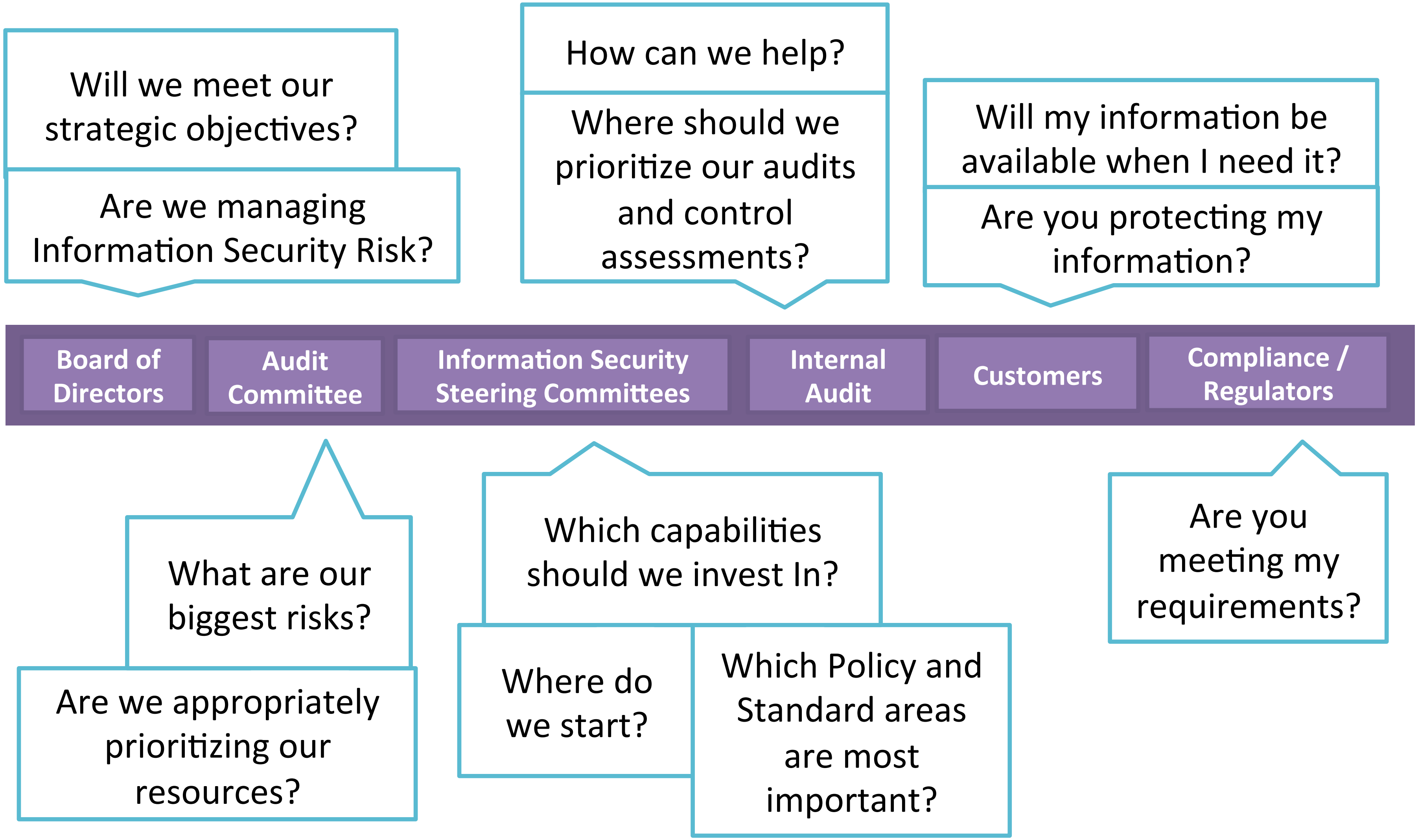
CLOSING REMARKS

Current State

Information security risk management is becoming more critical (and difficult) to implement

- Increasing publication and transparency of incidents
- Value of information is increasing, competitive advantage
- Work environment, how we access information is changing
- Increasing shadow IT, business-led IT
- Continuously changing threat environment
- Rapidly changing compliance and regulatory requirements
- Increased scrutiny by stakeholders

Stakeholder Questions



Will we meet our strategic objectives?

Are we managing Information Security Risk?

How can we help?

Where should we prioritize our audits and control assessments?

Will my information be available when I need it?

Are you protecting my information?

Board of Directors

Audit Committee

Information Security Steering Committees

Internal Audit

Customers

Compliance / Regulators

What are our biggest risks?

Are we appropriately prioritizing our resources?

Which capabilities should we invest In?

Where do we start?

Which Policy and Standard areas are most important?

Are you meeting my requirements?

OVERVIEW

RISK 101

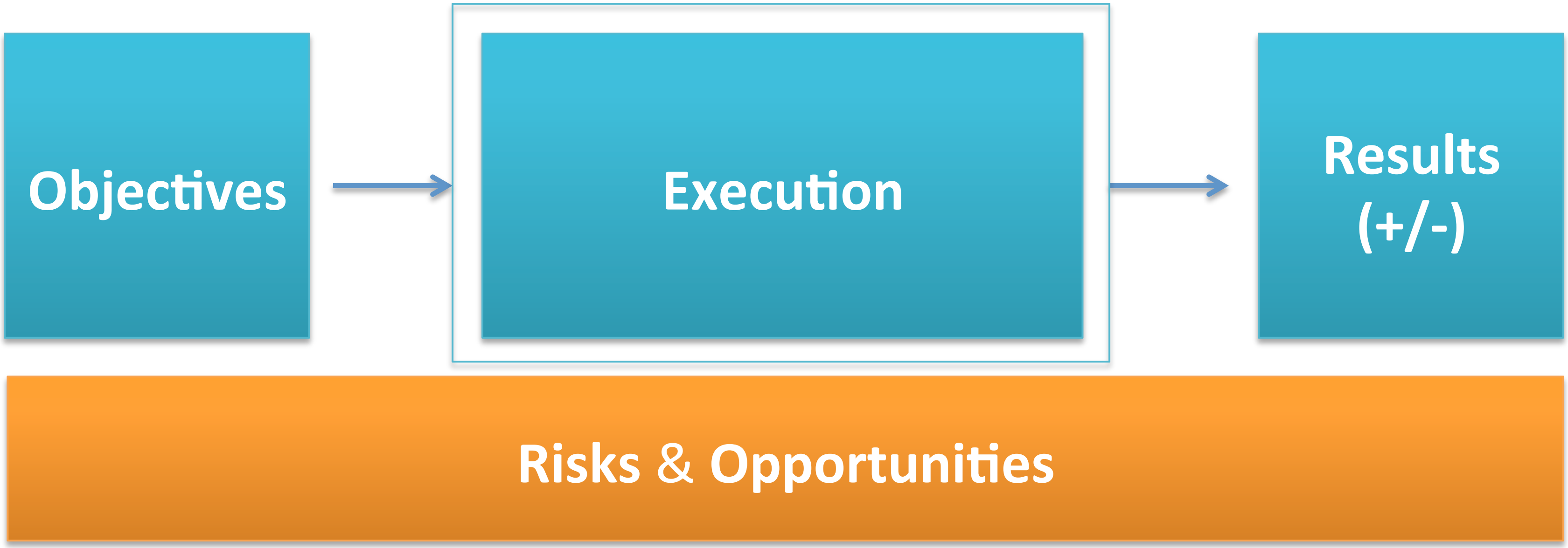
DEEP DIVE INTO 5 ISRM CONCEPTS

CLOSING REMARKS

What is Risk?

Organization	Definition of Risk
ISO Guide 73:2009	Effect of uncertainty on objectives
ISO 27000	Effect of uncertainty on objectives *NOTE: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization. (Focus on negative outcomes).*
IRM	Risk can be defined as the combination of the probability of an event and its consequences. Consequences can range from positive to negative.
IIA	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
COSO ERM	The possibility that an event will occur and adversely affect the achievement of objectives.

Simply Stated



An event that may occur which positively or negatively affects the achievement of objectives

Key Principles

- Risk ≠ Vulnerabilities

  Risk ≠ Controls

- Risk = Threat + Vulnerability

  Without relevant threats (and vulnerabilities), there is no risk

- Risks are dynamic

OVERVIEW

RISK 101

DEEP DIVE INTO 5 ISRM CONCEPTS

CLOSING REMARKS

5 Concepts

1. ISRM Program
2. Setting the Context
3. Threat Identification
4. Integration
5. Value Proposition

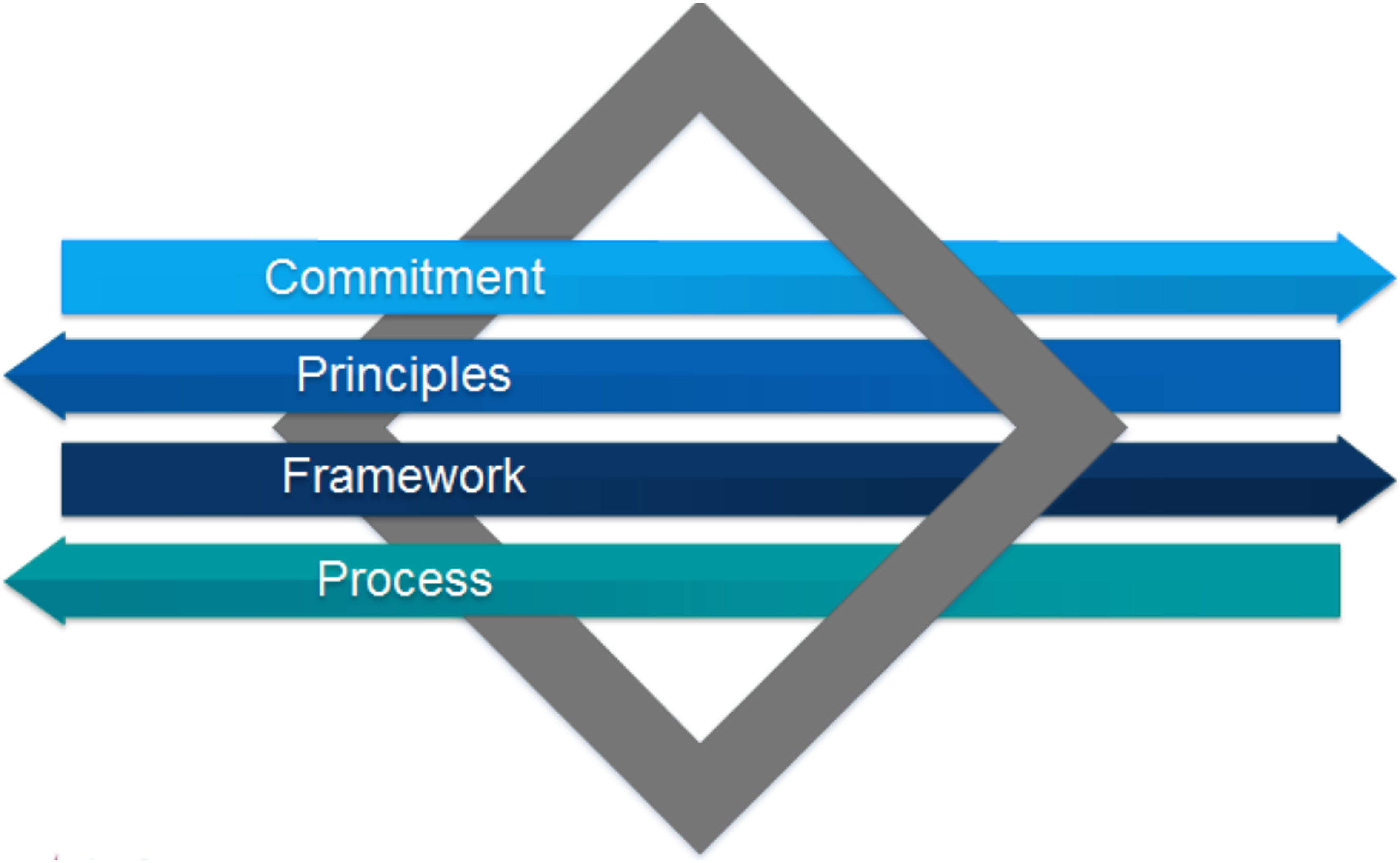
1. ISRM Program

Risk management is more than a process.

The Focus: Develop a holistic program for managing all levels of information security risks.

Why: Having a solid foundation can lead to more **s**ustainable and repeatable risk processes, helps increase stakeholder buy-in and alignment.

Using ISO 31000 as a Guide



Key Considerations

What is important to you and your organization?

- Consistent language and framework
- Covers various risks and impacts
- Embed risk management where it matters most/value driven
- Actionable, enforceable
- Awareness and training

What does success look like?

- Reduce uncertainty, volatility
- Increase consistency, assurance, credibility, accountability, understanding, prioritization, awareness
- Balance risk and cost
- Being able to express technical risk as business risk

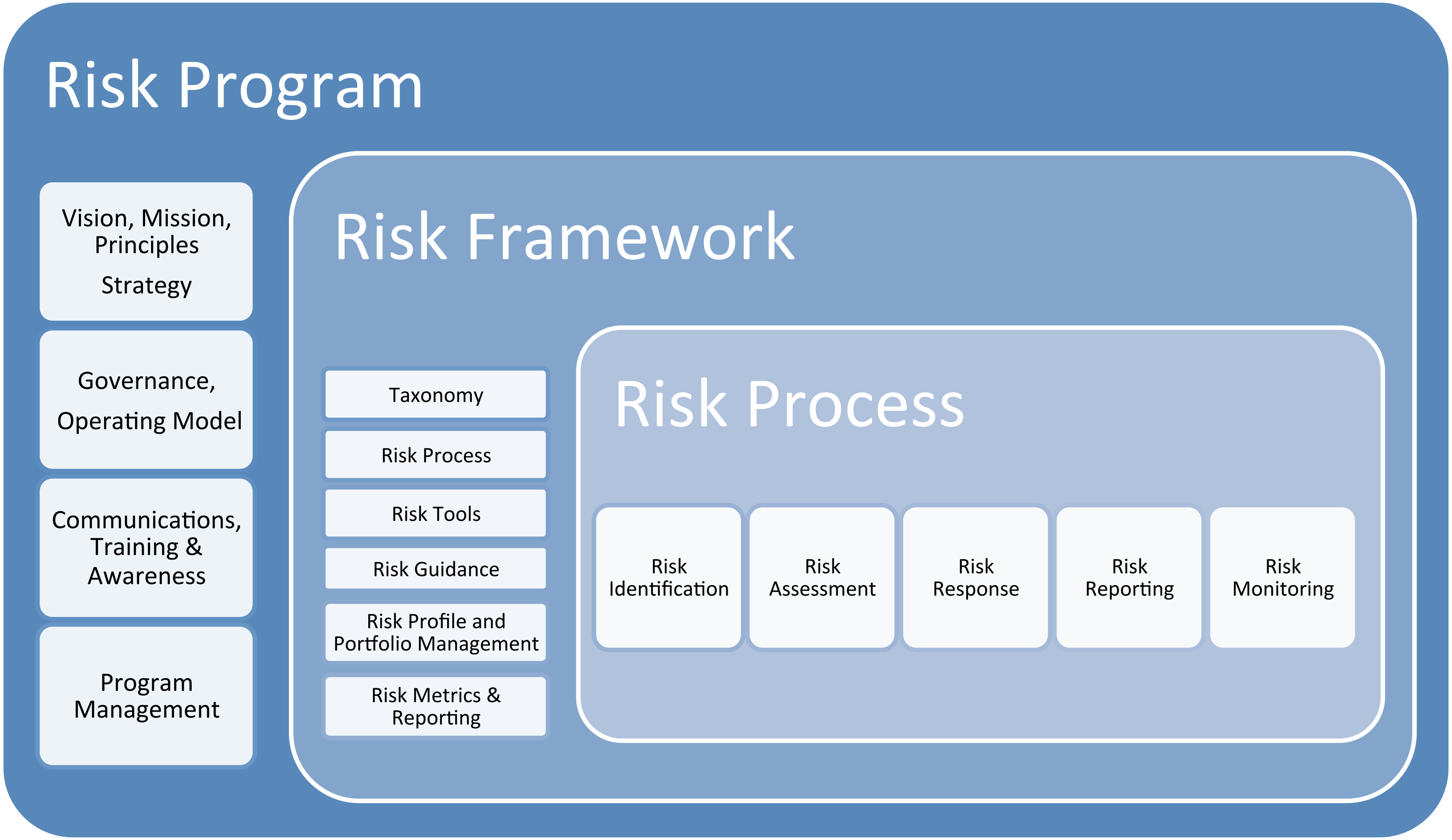
Sample Program Vision, Mission & Principles

Vision	Mission
Deliver epic information security risk management capabilities that optimize investments and creates competitive advantage for the organization.	**Support management's ability to make informed resource allocation decisions by providing visibility into key information security risks.**

Guiding Principles for FYXX

- Develop a **program for Information Security Risk Management** which allows the organization to communicate in a common language understood by senior management and the Board
- **Build foundational components with an emphasis on "fit"** (within the culture and operating style)
- **Guide management** in proactively reducing the risks associated with high priority areas
- Make risk **decisions at the appropriate level**
- Make **informed resource allocation decisions**
- **Establish relationships** between the organization and key stakeholders

Consider a Nested Model



Risk Program

Vision, Mission, Principles
Strategy

Governance, Operating Model

Communications, Training & Awareness

Program Management

Risk Framework

Taxonomy

Risk Process

Risk Tools

Risk Guidance

Risk Profile and Portfolio Management

Risk Metrics & Reporting

Risk Process

Risk Identification

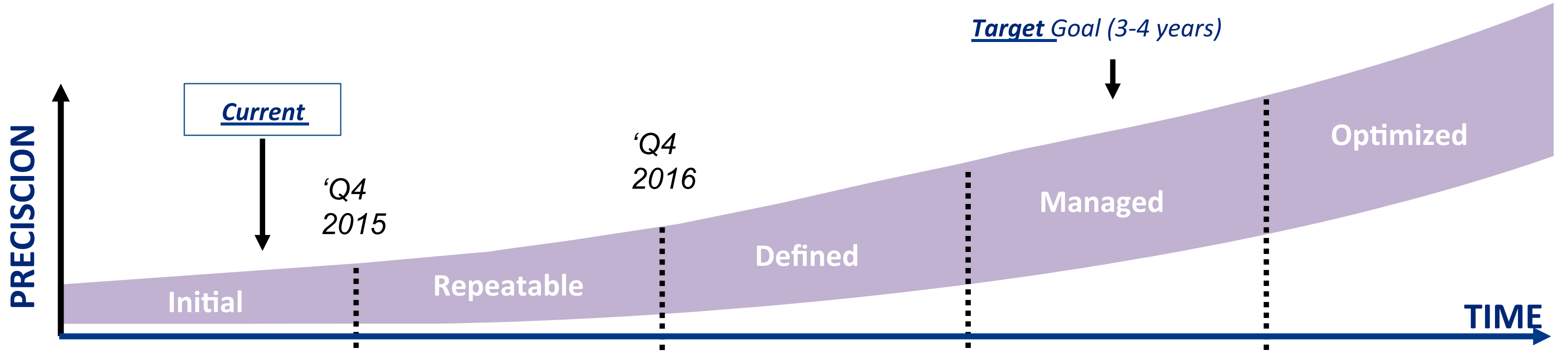
Risk Assessment

Risk Response

Risk Reporting

Risk Monitoring

Sample Roadmap Highlighting Key Phases



Key Milestones

- **Establish Risk Program**
  Establish foundation for the risk program, including the vision, mission, strategy, and process and framework for identifying risks
- **Conduct IS Risk Assessments**
- Conduct first formal risk assessments utilizing framework
- **Risk Governance**
  Develop policy, and determine risk governance activities, roles & responsibilities
- **Risk Reporting**
  Provide senior management with update on top risks, and responses

- **Enhance Risk Tools**
- **Conduct Quarterly Risk Assessments**
- **Risk Governance**
  Strengthen 3 line of defense model, enterprise wide
- **Enhance Risk Reporting**

- **Automate Risk Tools**
- **Mature Risk Reporting with full catalog of KRIs**

- **Risk Aware Operations**
- **Investment Portfolio Management / Risk Valuation**

Charts showing the maturity of the ISRM program increasing over time helps convey the program vision and the commitment to continuous improvement

2. Setting the Context

Risk and risk management activities are dependent upon the context.

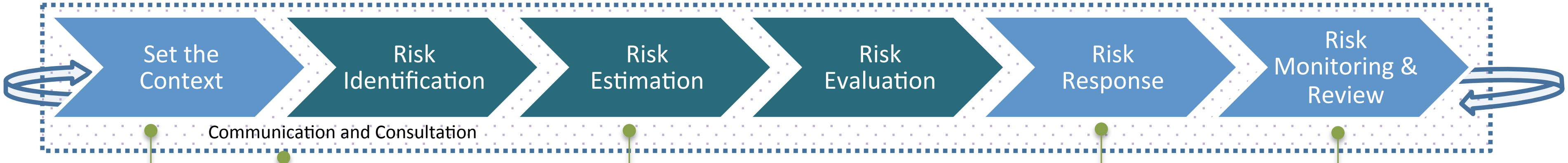
The Focus: Ensure that risks have context and are communicated in a consistent manner.

Why: When the context is clear, everything else falls into place. Results in greater alignment, less churn.

How do you report on risk?

- *Network Breach*
- Back office systems are breached, leading to an exposure of financial reporting data.
- A key third party service provider experiences a data breach or massive outage impacting our customers' information or services
- *As a result of server theft, an unauthorized disclosure of sensitive customer data for all customers may occur, which would require breach notifications to regulators and affected clients.*
- *System administrator passwords for Application ABC are transmitted across the network in clear text, and are subject to eavesdropping by a malicious insider. Should the information be intercepted, the insider could gain unauthorized access to highly sensitive financial information. A breach of this magnitude could result in noncompliance, and significant financial and reputational loss.*

The Risk Process



- Identify relevant threats/events
- Estimate the impact of threats
- Assess existing capabilities, processes, controls
- Identify those areas that need the most attention

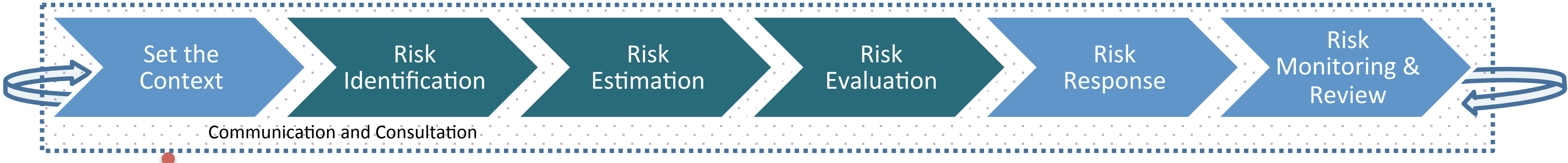
- Identify security objectives
- Identify level of focus (enterprise vs. business unit, strategic vs. technical)

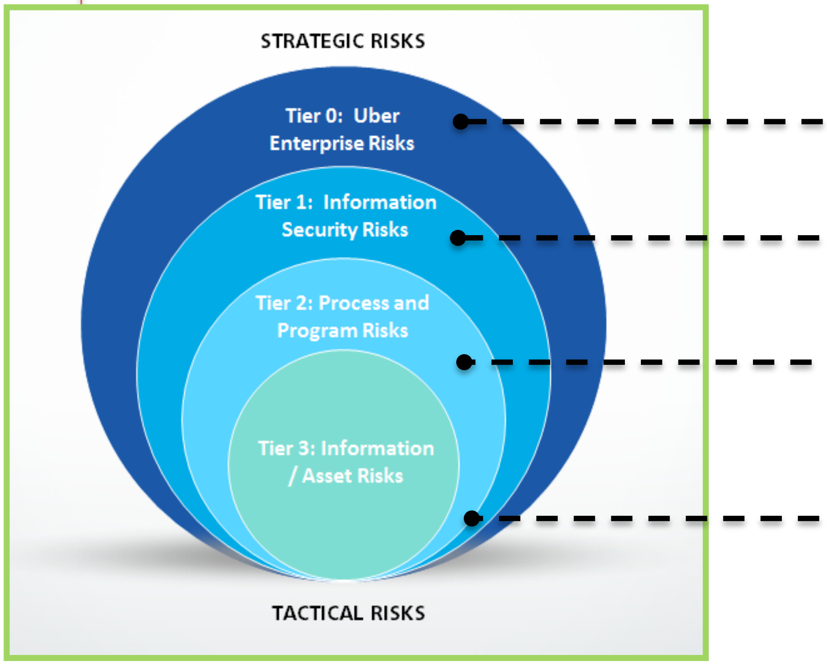
- Regularly report on top risks, risk posture, and treatment plans

- Consider risk treatment options & valuation
- Formally respond to the risk
- Prepare and implement risk treatment plans

- Track risk treatment progress
- Track capabilities, controls
- Monitor emerging risks
- Monitor changes & trends

Risk "Levels"




STRATEGIC RISKS
Tier 0: Uber Enterprise Risks
Tier 1: Information Security Risks
Tier 2: Process and Program Risks
Tier 3: Information / Asset Risks
TACTICAL RISKS

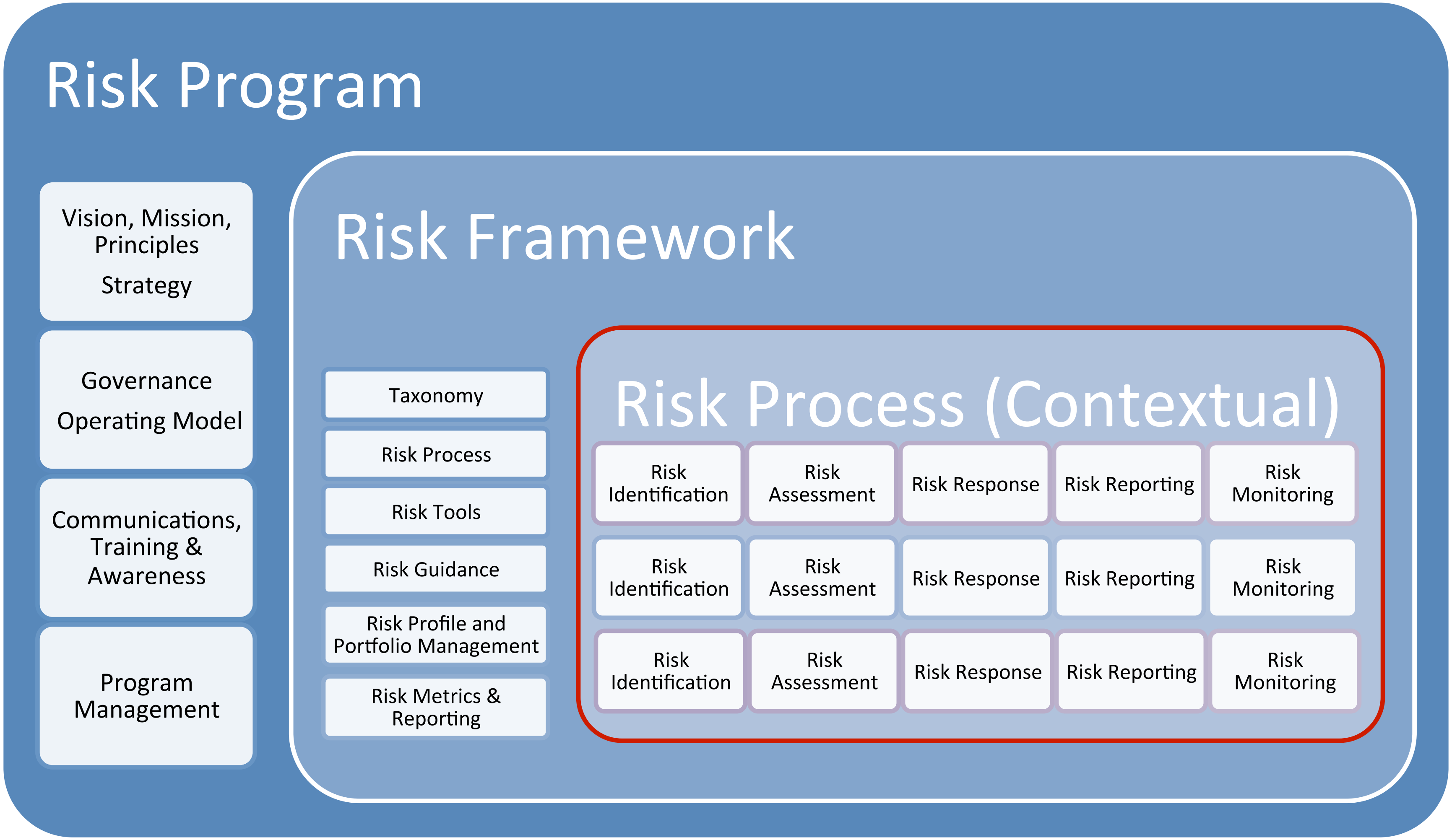
security-related **strategic risks** as reported out of ERM

key **enterprise** information security risks

information security risks at the **process and program level**

information security risks at the **system or information asset level**

Revised Nested Model



Risk Program

Vision, Mission, Principles

Strategy

Governance

Operating Model

Communications, Training & Awareness

Program Management

Risk Framework

Taxonomy

Risk Process

Risk Tools

Risk Guidance

Risk Profile and Portfolio Management

Risk Metrics & Reporting

Risk Process (Contextual)

Risk Identification	Risk Assessment	Risk Response	Risk Reporting	Risk Monitoring
Risk Identification	Risk Assessment	Risk Response	Risk Reporting	Risk Monitoring
Risk Identification	Risk Assessment	Risk Response	Risk Reporting	Risk Monitoring

3. Threat Identification

Information Security Risk Management entails identifying and addressing relevant threats.

The Focus: Identify and inventory relevant threats, and utilize the information to assess various levels of risk.

Why: Threat identification and management resonates with information security practitioners and can ultimately increase the precision of risk information.

Threat

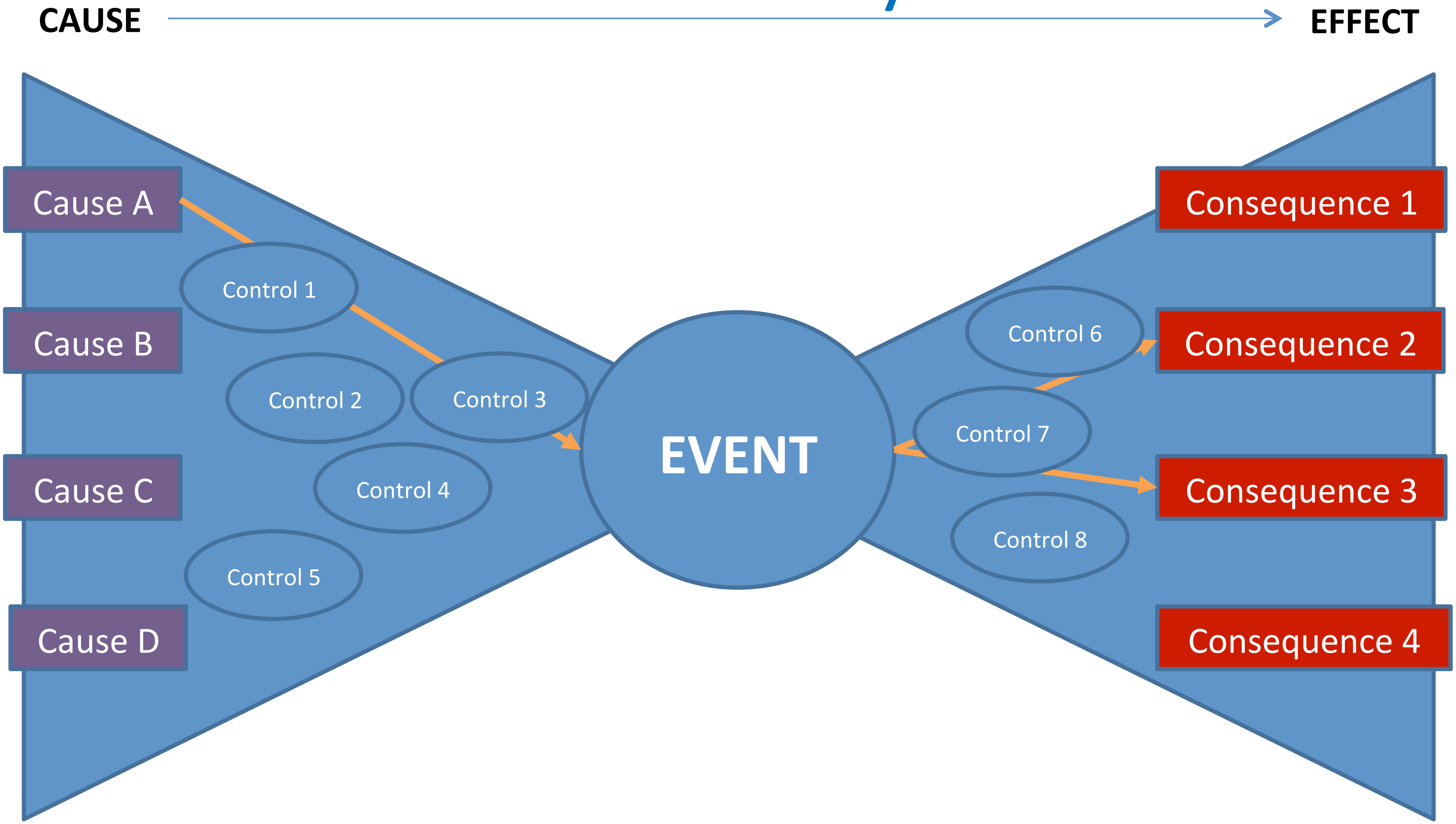
Risk **=** an event that may occur which positively or negatively affects the achievement of objectives

Risk **= Threat + Vulnerability**

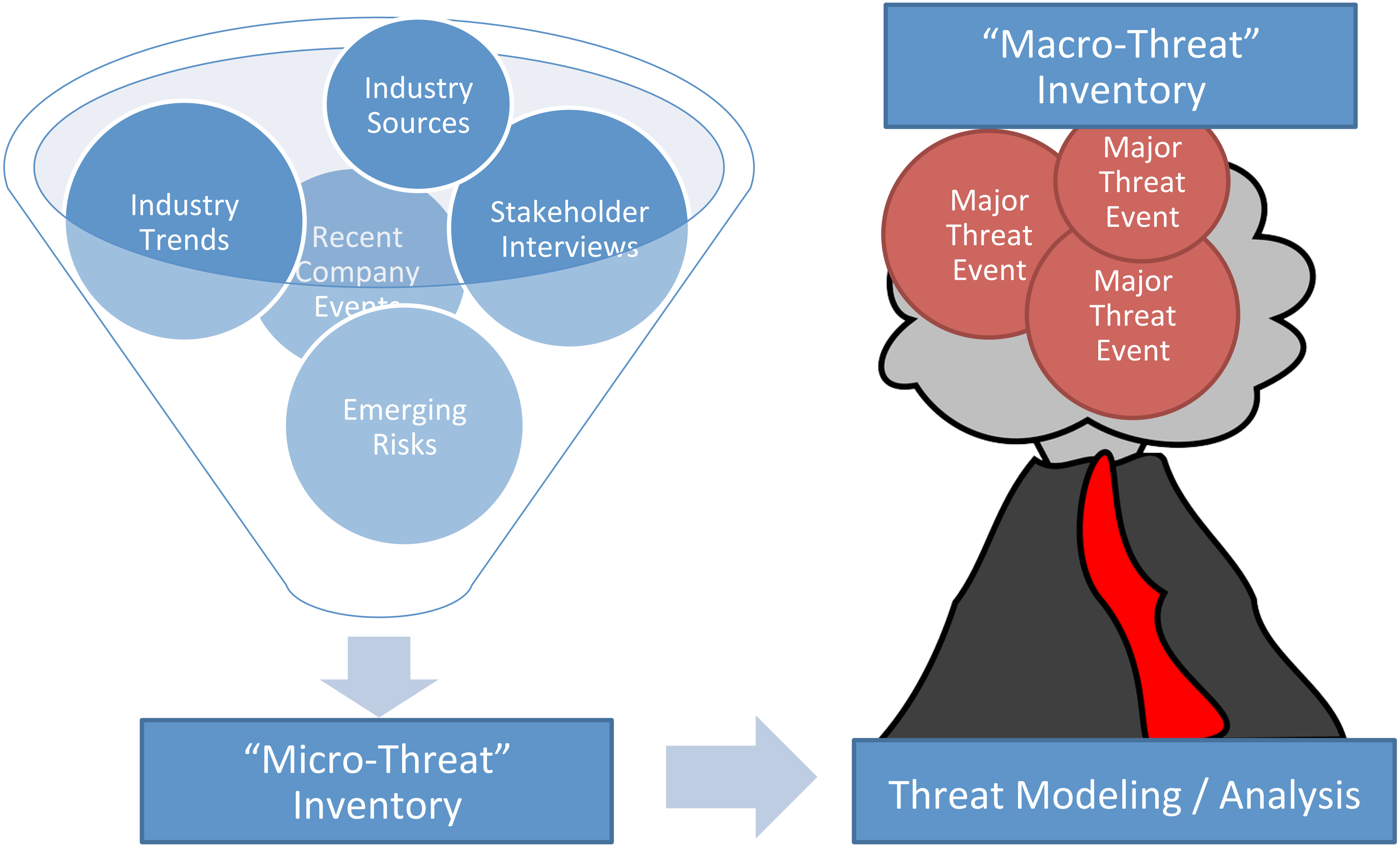
Without relevant threats (and vulnerabilities), there is no risk

Threat *=* potential cause of an unwanted event, which may result in harm to assets (including individuals, systems) or the organization

Bowtie Analysis



Threat Modeling



Industry Sources

Industry Trends

Recent Company Events

Stakeholder Interviews

Emerging Risks

“Micro-Threat” Inventory

“Macro-Threat” Inventory

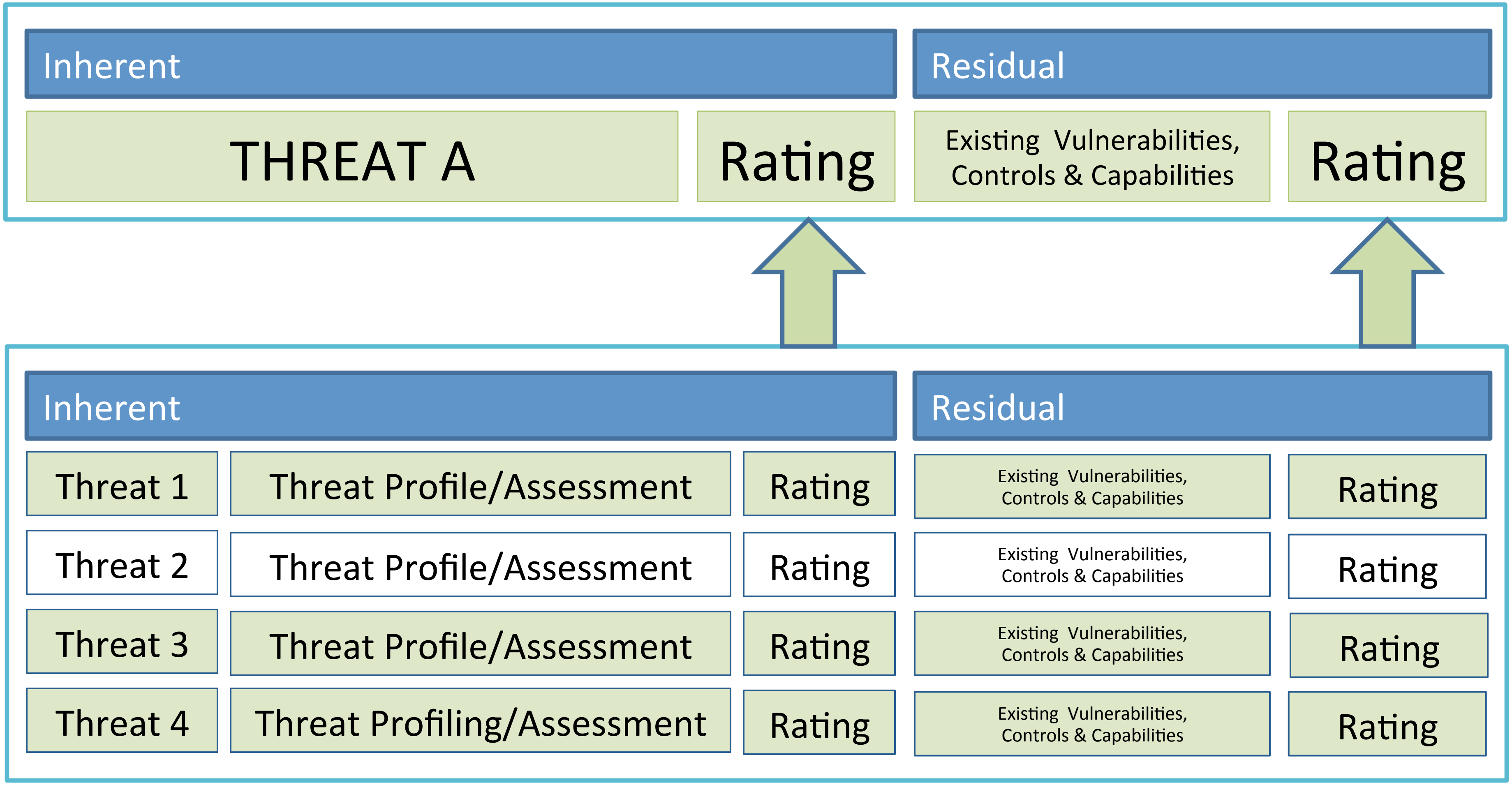
Major Threat Event

Major Threat Event

Major Threat Event

Threat Modeling / Analysis

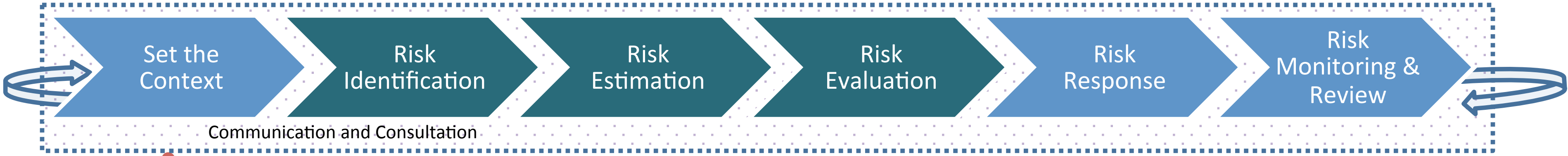
“Micro Threats” and “Macro Threats”

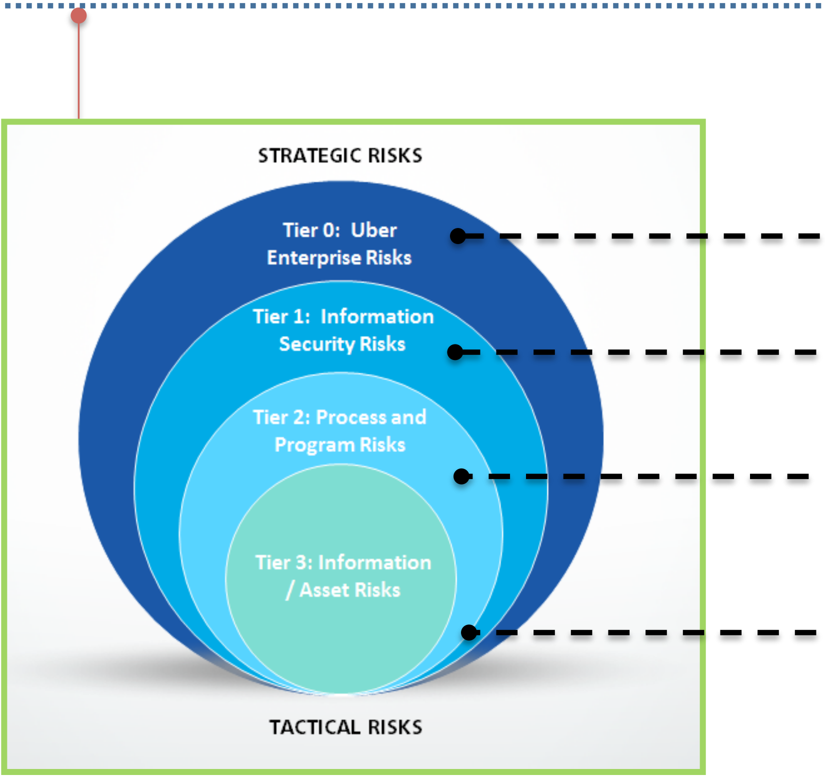


Inherent		Residual	
THREAT A	Rating	Existing Vulnerabilities, Controls & Capabilities	Rating

Inherent			Residual	
Threat 1	Threat Profile/Assessment	Rating	Existing Vulnerabilities, Controls & Capabilities	Rating
Threat 2	Threat Profile/Assessment	Rating	Existing Vulnerabilities, Controls & Capabilities	Rating
Threat 3	Threat Profile/Assessment	Rating	Existing Vulnerabilities, Controls & Capabilities	Rating
Threat 4	Threat Profiling/Assessment	Rating	Existing Vulnerabilities, Controls & Capabilities	Rating

Threats by Risk "Level"




STRATEGIC RISKS
Tier 0: Uber Enterprise Risks
Tier 1: Information Security Risks
Tier 2: Process and Program Risks
Tier 3: Information / Asset Risks
TACTICAL RISKS

security-related **strategic risks** as reported
o

k s

"Macro-Threat" Inventory

information security risks at the **process and**
p

ir **or**
information asset level

"Micro-Threat" Inventory

4. Integration

Risk activities inform, and are informed by, other information security activities.

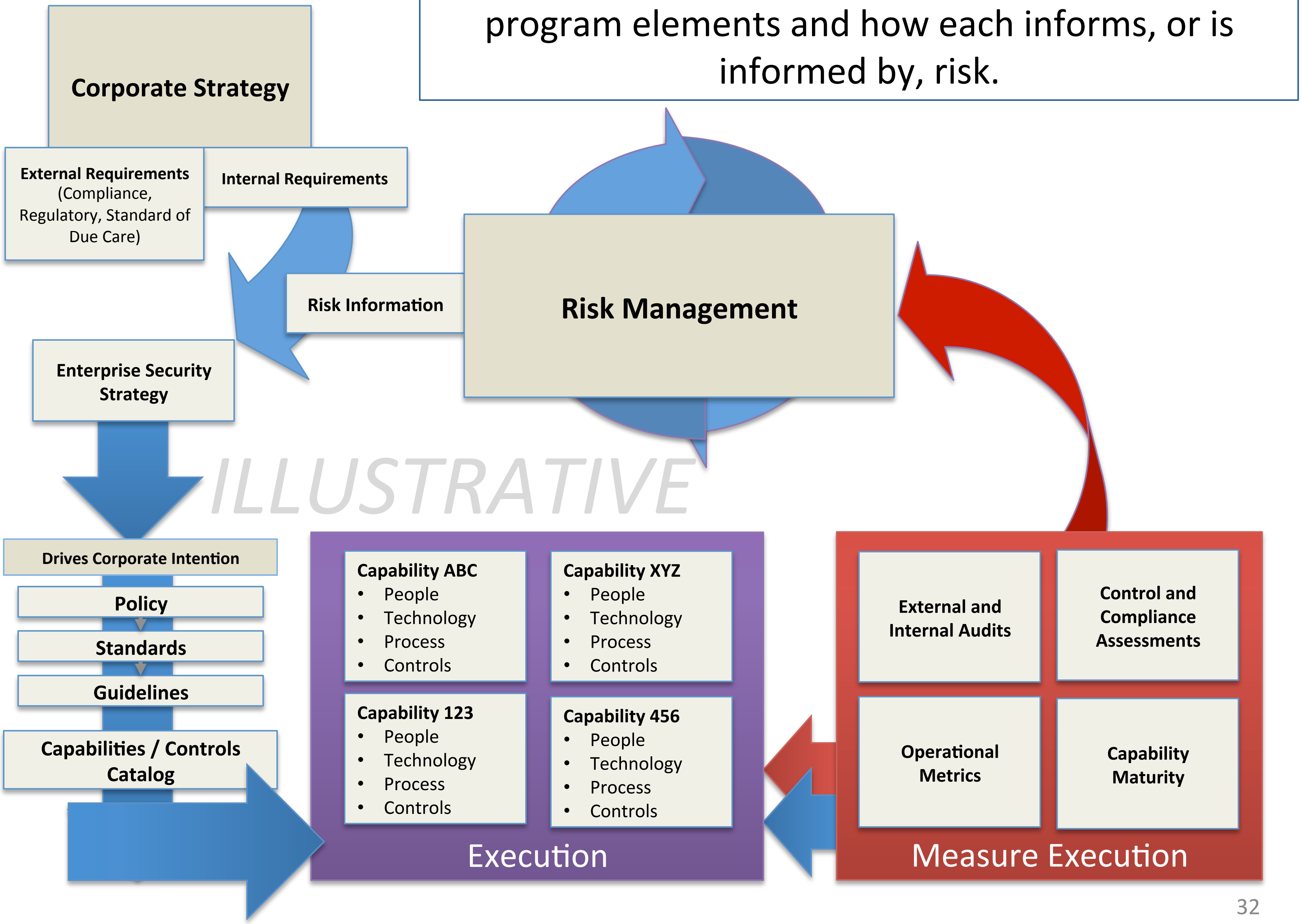
The Focus: Align ISRM program components with other information security-related initiatives and capabilities.

Why: Alignment increases collaboration, increases precision of risk information.

Consider How Risk Relates To…

Strategy	Policy	Standards
Internal & External Requirements	Services	Capabilities
People	Processes	Controls
Technology	Operational Metrics	Business Liaisons

Consider mapping all of the information security program elements and how each informs, or is informed by, risk.



Corporate Strategy

External Requirements (Compliance, Regulatory, Standard of Due Care)

Internal Requirements

Risk Information

Risk Management

Enterprise Security Strategy

Drives Corporate Intention

Policy

Standards

Guidelines

Capabilities / Controls Catalog

Capability ABC
- People
- Technology
- Process
- Controls

Capability XYZ
- People
- Technology
- Process
- Controls

Capability 123
- People
- Technology
- Process
- Controls

Capability 456
- People
- Technology
- Process
- Controls

Execution

External and Internal Audits

Control and Compliance Assessments

Operational Metrics

Capability Maturity

Measure Execution

5. Value Proposition

Risk isn't always doom and gloom – it can help management achieve (and exceed) objectives

The Focus: Highlight the upside of risk, and consider estimating the value proposition of investments.

Why: Increases participation and interest, management can make more informed resource allocation decisions.

Focus on the Upside

Mergers & Acquisitions

Downside

A large acquisition may result in a significant increase in information security threats and vulnerabilities.

Results in:

- Loss of sensitive data
- Service interruptions

Organizational objectives potentially impacted:

- Customer Trust
- Customer Service Excellence

Upside

A large acquisition may result in additional security personnel, skills, and technology.

Results in:

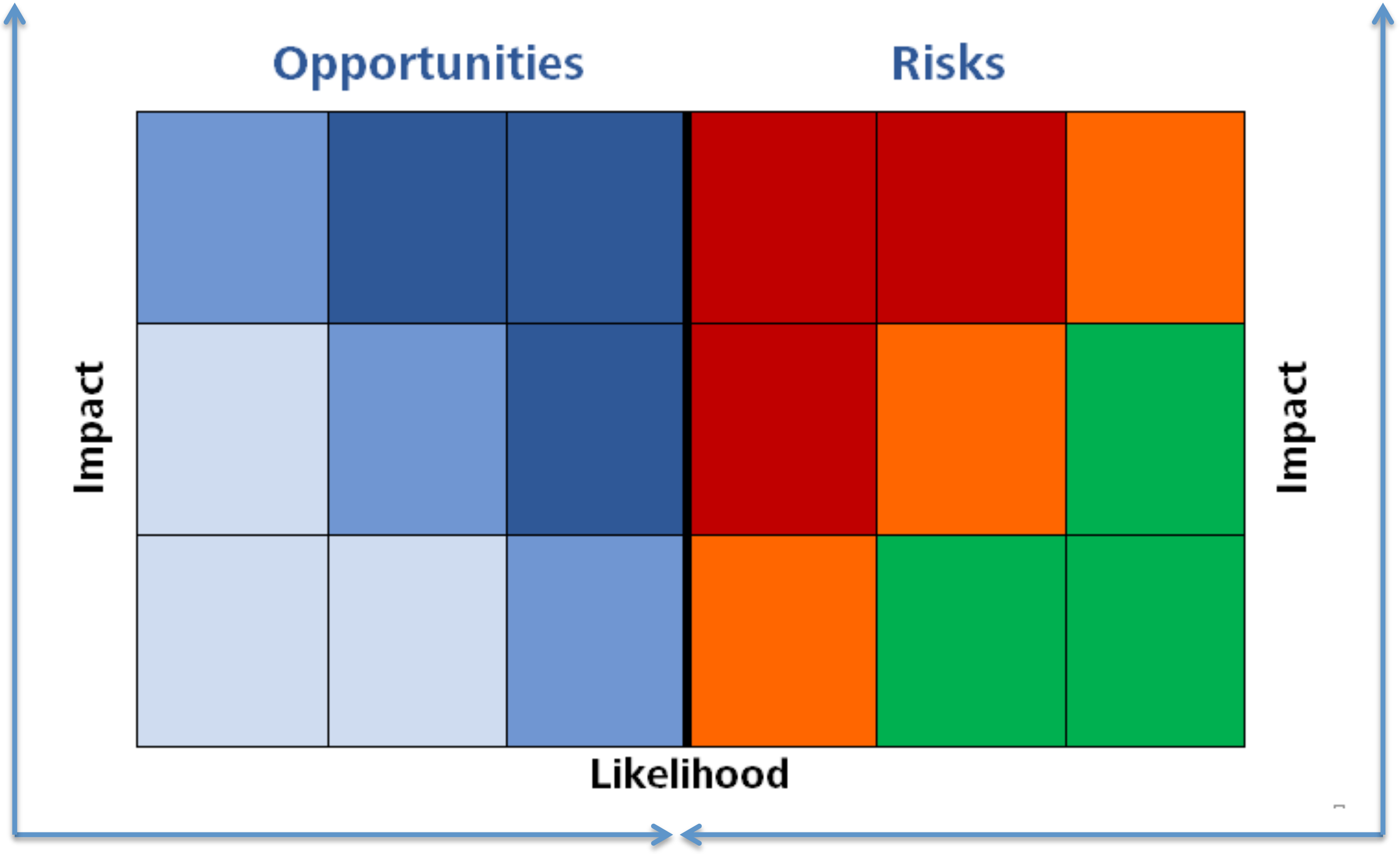
- Increased morale
- Increasing capability maturity

Organizational objectives potentially impacted:

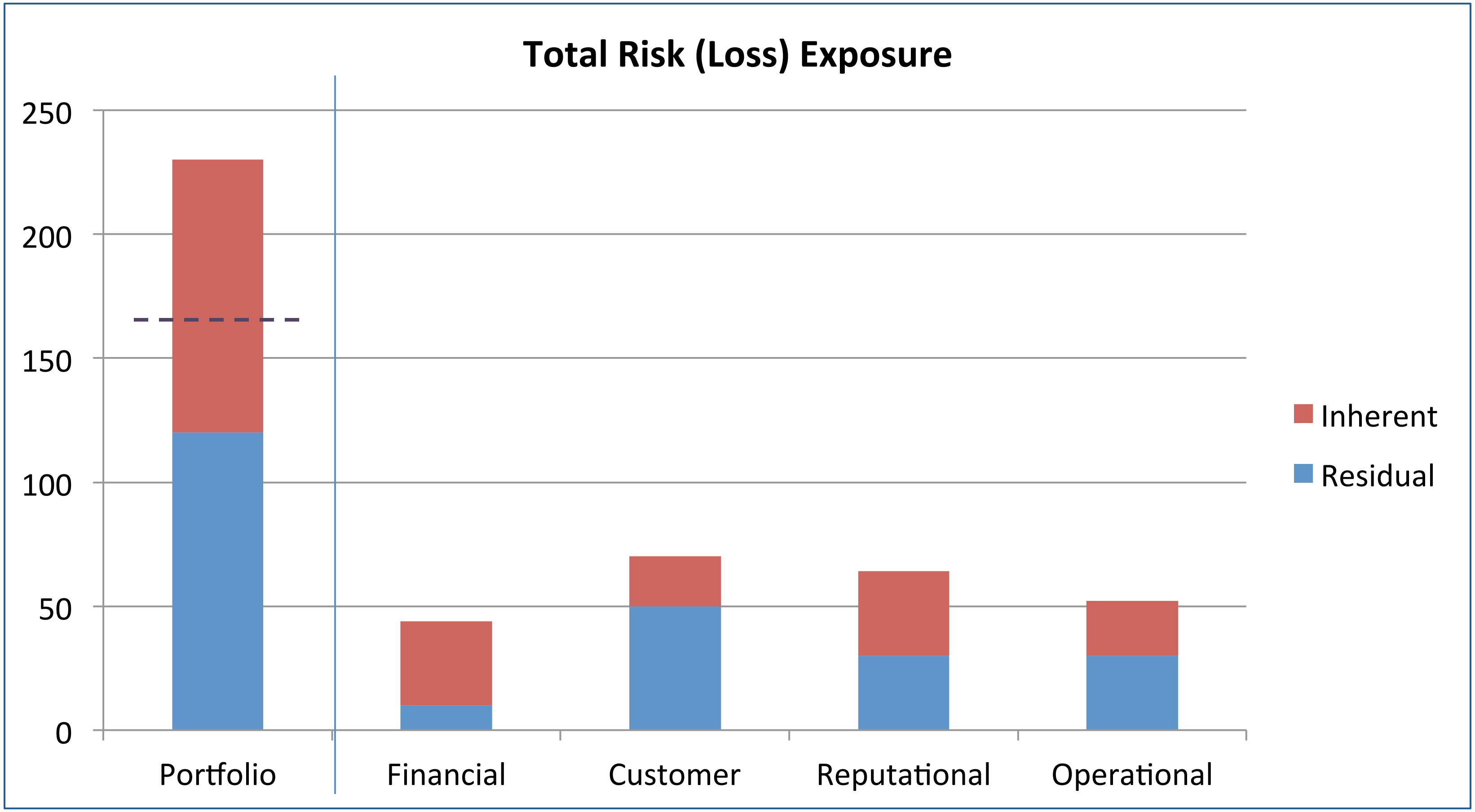
- Customer Trust
- Customer Service Excellence

Highlight Both the Upside & Downside

CREATE VALUE **PRESERVE VALUE**

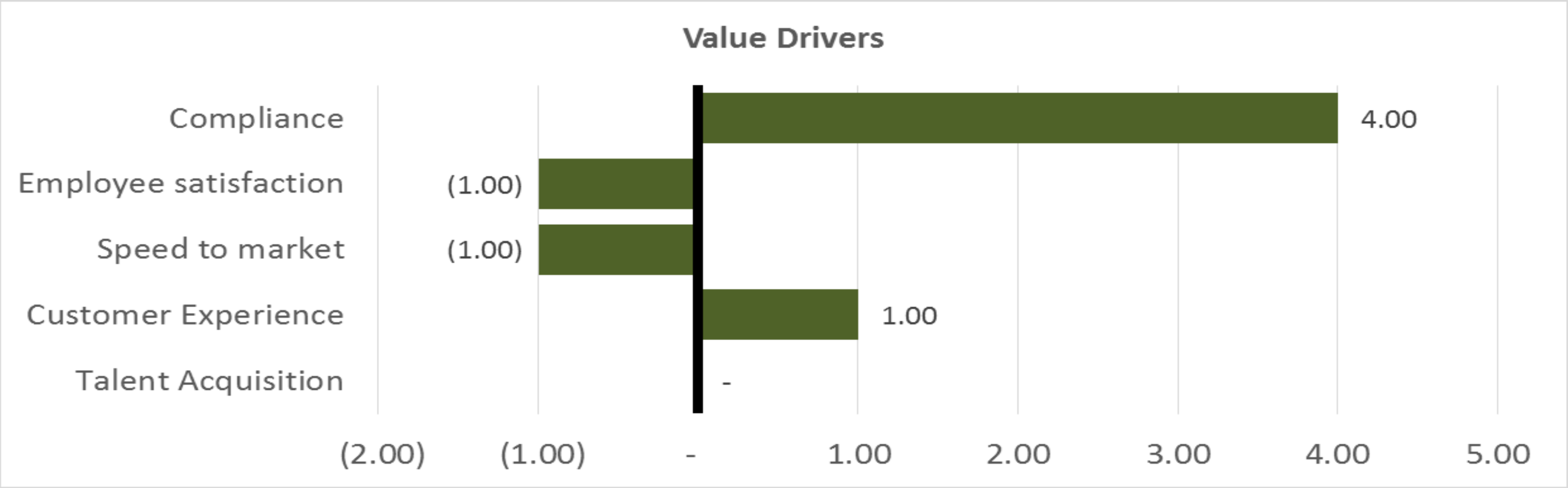


Define and Quantify Risk Exposure

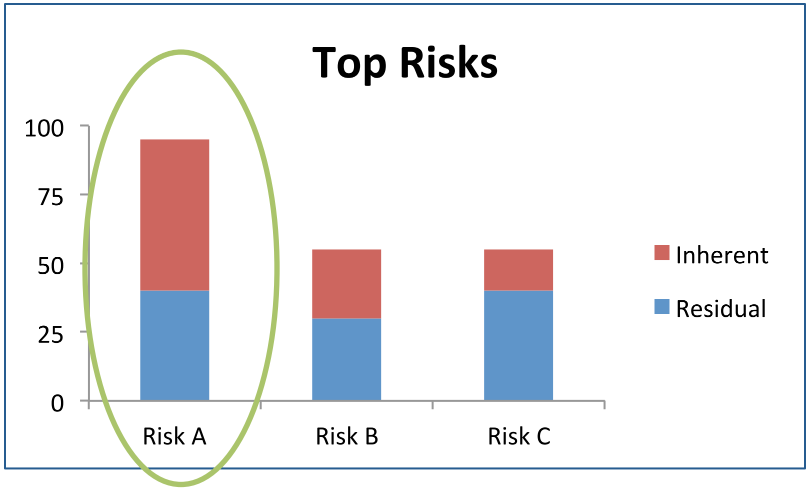


Define and Quantify Value Drivers

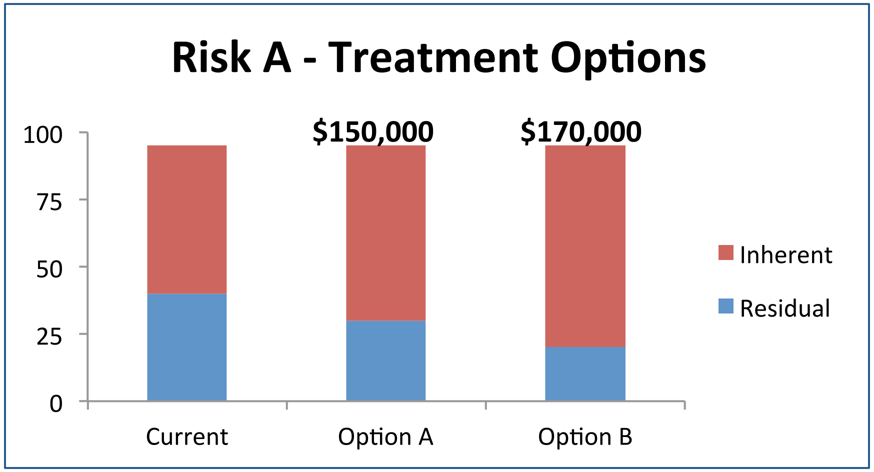
- Improve customer experience
- Increase customer trust
- Increase employee productivity
- Increase employee satisfaction
- Improve process efficiency
- Improve reputation
- Improve talent acquisition
- Increase compliance
- Decrease costs
- Increase speed to market



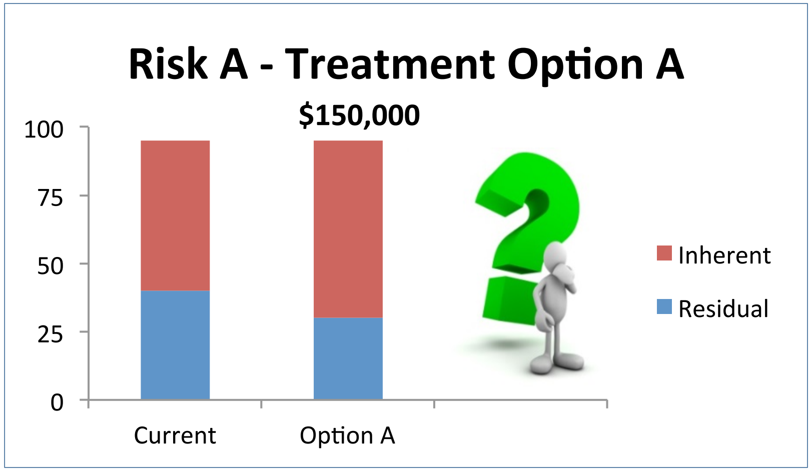
Informed Investments



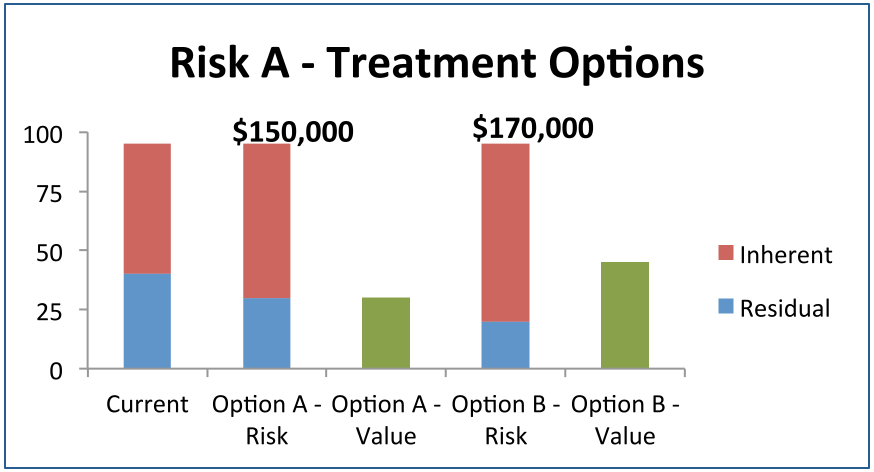
Top Risks



Risk A - Treatment Options



Risk A - Treatment Option A



Risk A - Treatment Options

OVERVIEW

RISK 101

DEEP DIVE INTO 5 ISRM CONCEPTS

CLOSING REMARKS

Considerations…

- ❑ Clearly define 'Risk' for your organization
- ❑ Create an inspiring ISRM program vision
- ❑ Construct a nested ISRM model
- ❑ Develop risk levels and associated processes
- ❑ Design a consistent model for managing threat information
- ❑ Increase integration with other security capabilities
- ❑ Consider upside of risk and investment valuation

Session Objectives

- Explore the definition of ‘risk’
- Discover five concepts that can be utilized to guide the design and/or enhance an IS Risk Program
- Identify creative ways to enhance your Information Security Risk Management program

Questions?

Resources

- ISO 31000:2009 – Risk Management Principles and Guidelines
- ISO/IEC 31010:2009 - Risk Assessment Techniques
- ANSI/ASIS/RIMS Risk Assessment Standard (RA.1-2015)
- ISO 27000 series – Information Security Standards
- COSO 2004 - Enterprise Risk Management - Integrated Framework
- OCEG "Red Book" 2.0: 2009 - a Governance, Risk and Compliance Capability Model
- A Risk Management Standard – IRM
- COBIT 5
- COBIT 5 for Information Security
- COBIT 5 for Risk
- Corporate Executive Board
- Gartner
- Forrester

THANK YOU!

TANYA SCOTT

TANYA.SCOTT@AUTODESK.COM