

NIST SP 800-39 Integrated Enterprise-wide Risk Management: Organization, Mission, and Information Systems Views

1-2 September 2009



Connect. Integrate. Collaborate.

Dr. Ron Ross

NIST Information Technology Laboratory Computer Security Division
FISMA Implementation Project Leader

Jennifer Fabius Greene

IC CIO Information Assurance Senior Risk Advisor



NIST

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Intelligence Community Chief Information Officer

Enterprise-wide Risk Management

- *Enterprise-wide risk management encompasses any risk that impacts an organization, including assets, mission, functions, or reputation*
- All individuals within the organization must understand their responsibilities in managing risk from operating information systems that support the mission/business functions of the organization, and take responsibility for risk consequences and mitigation
- Information systems are subject to serious threats that can have adverse affects on organizational operations, assets, individuals, other organizations, or the Nation
- Attacks on information systems today are often well organized, disciplined, aggressive, well-funded, and extremely sophisticated
- Successful attacks on public and private sector information systems result in harm to U.S. national and economic security interests



Risk-based Protection

- **Enterprise missions and business processes drive security requirements and associated safeguards and countermeasures for organizational information systems**
- **Highly flexible implementation; recognizing diversity in missions/business processes and operational environments**
- **Senior leaders are both responsible and accountable for their information security decisions**
- **Supports a balanced perspective of risks from strategic and tactical perspectives**



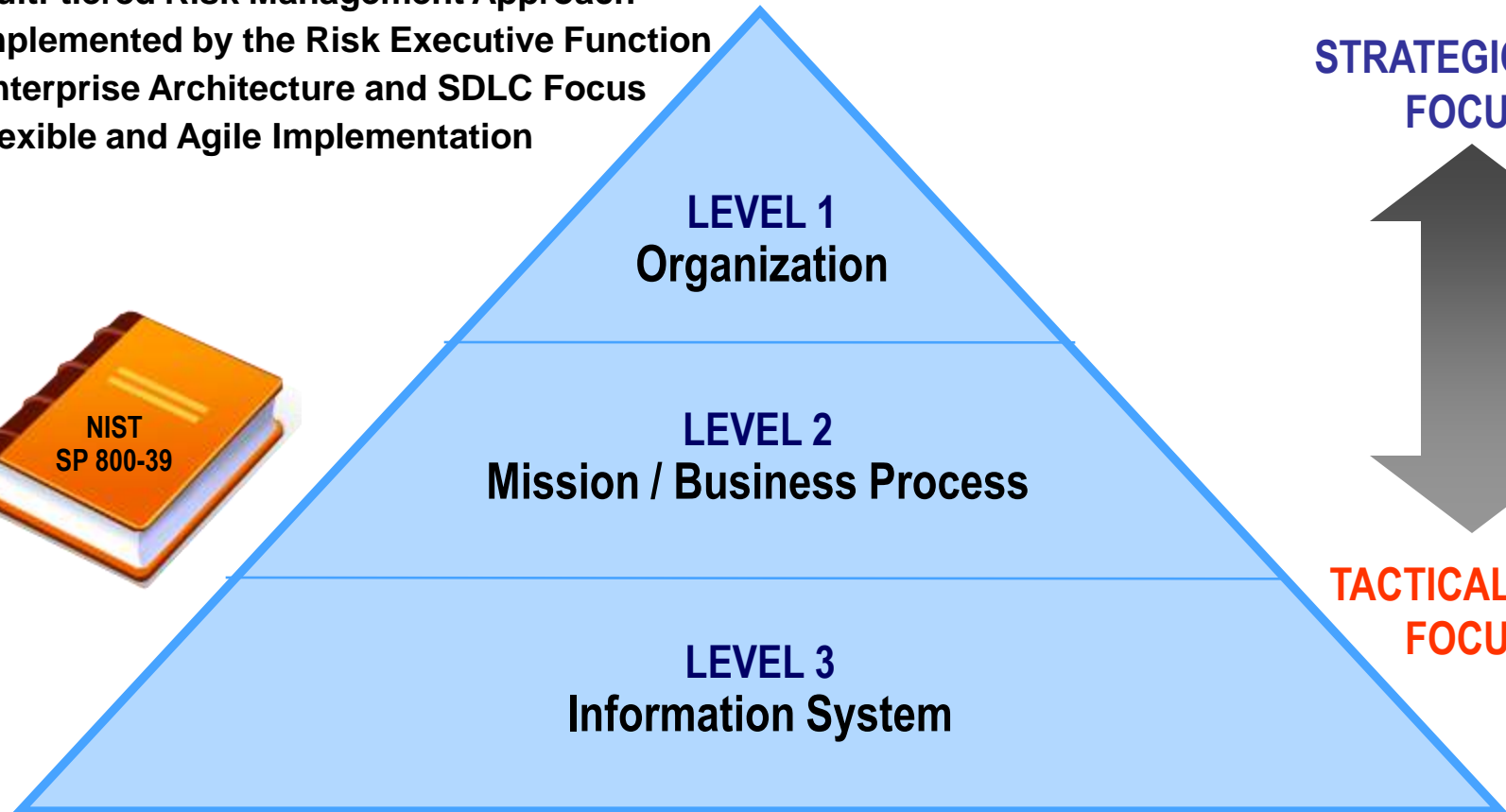
Documentation

Policy	Guidance Provided
<p>Intelligence Community Directive 503 <i>Information System Security Risk Management, Certification and Accreditation</i></p>	<p>Promulgates standards for risk management (RM) and requires IC elements to determine level of acceptable risk based on considerations beyond security</p>
<p>NIST SP 800-39 <i>Integrated Enterprise-wide Risk Management: Organization, Mission, and Information Systems Views</i> <i>[DRAFT – updated version anticipated Q4 09]</i></p>	<p>Guidelines for managing risk to organizational operations, assets, individuals, other organizations, and the Nation resulting from operation and use of IS</p> <ul style="list-style-type: none"> ✓ <i>Three-tiered risk management approach</i> ✓ <i>Cyber preparedness information</i> ✓ <i>ISO/IEC 27001 mapping to RM pubs</i>
<p>NIST SP 800-37 <i>Applying the Risk Management Framework to Information Security Systems</i> <i>[DRAFT – updated version anticipated Q4 09]</i></p>	<p>Defines roles required to authorize information systems (IS) for operation, and responsibilities for maintaining authorization</p>



Risk Management Hierarchy

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation

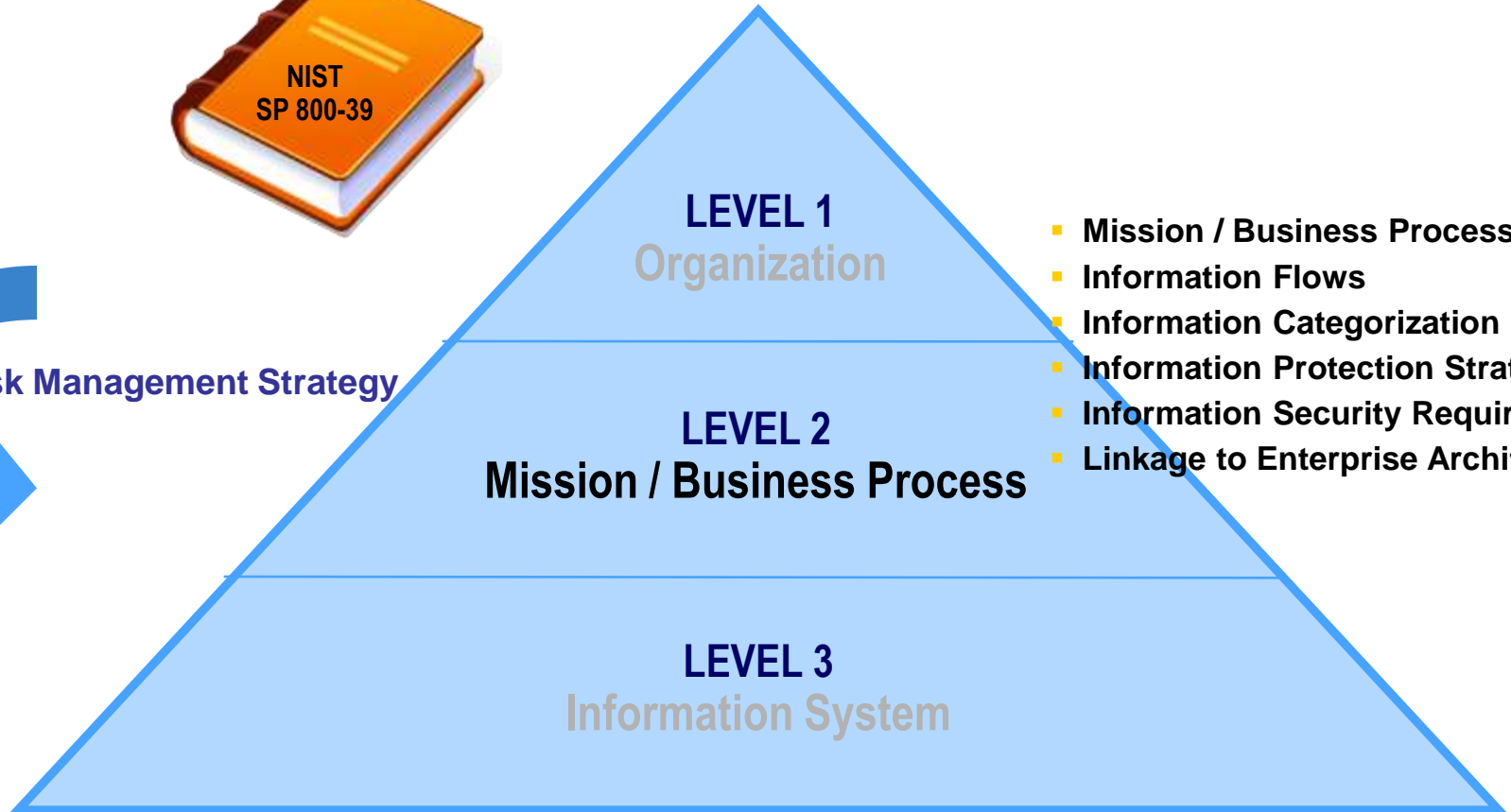


Risk Management Hierarchy

- Risk Executive Function
- Risk Assessment Methodologies
- Risk Mitigation Approaches
- Risk Tolerance
- Risk Monitoring Approaches
- Linkage to ISO/IEC 27001



Risk Management Hierarchy



- Mission / Business Processes
- Information Flows
- Information Categorization
- Information Protection Strategy
- Information Security Requirements
- Linkage to Enterprise Architecture



Risk Management Hierarchy



LEVEL 1
Organization

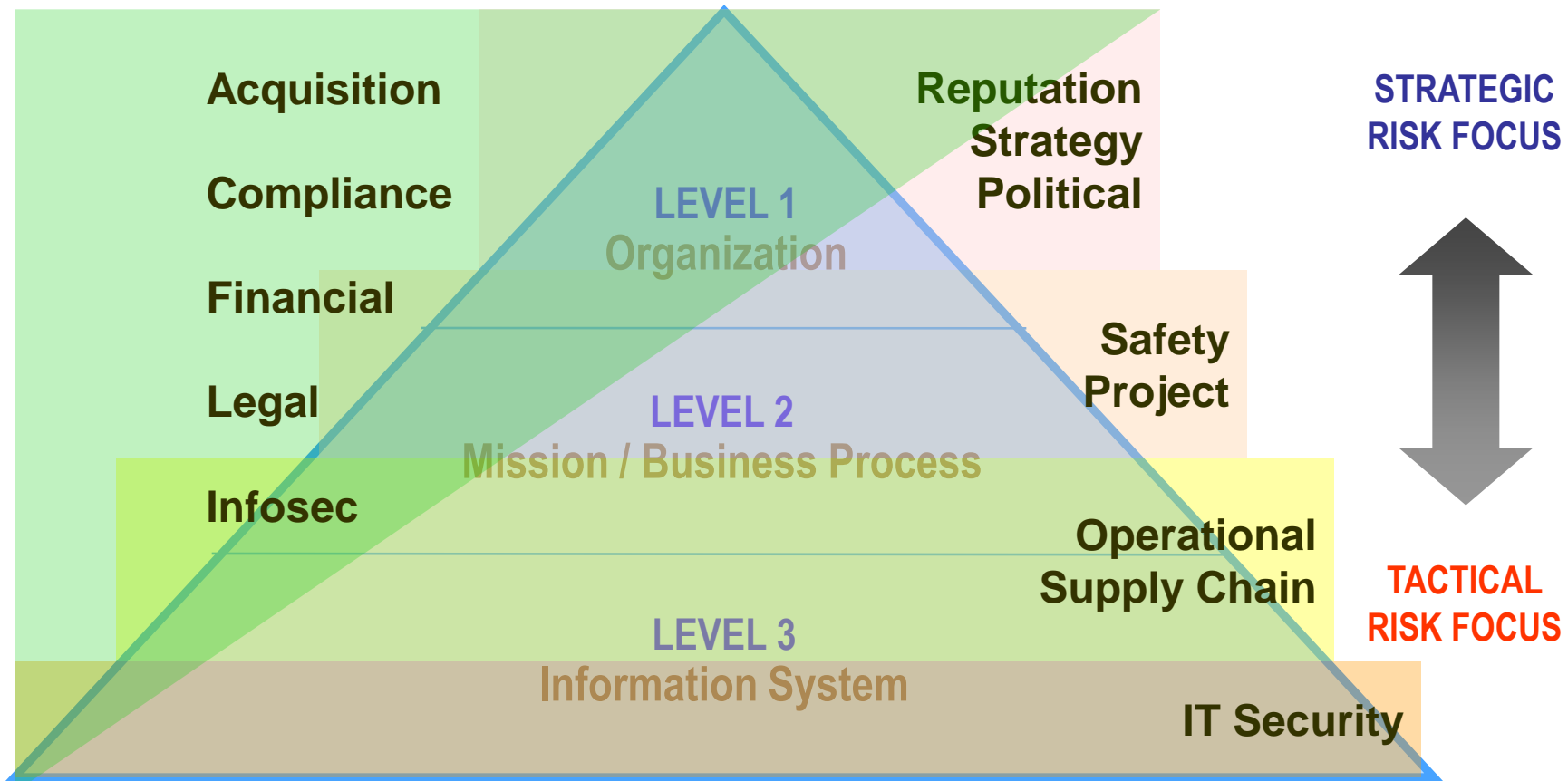
LEVEL 2
Mission / Business Process

LEVEL 3
Information System

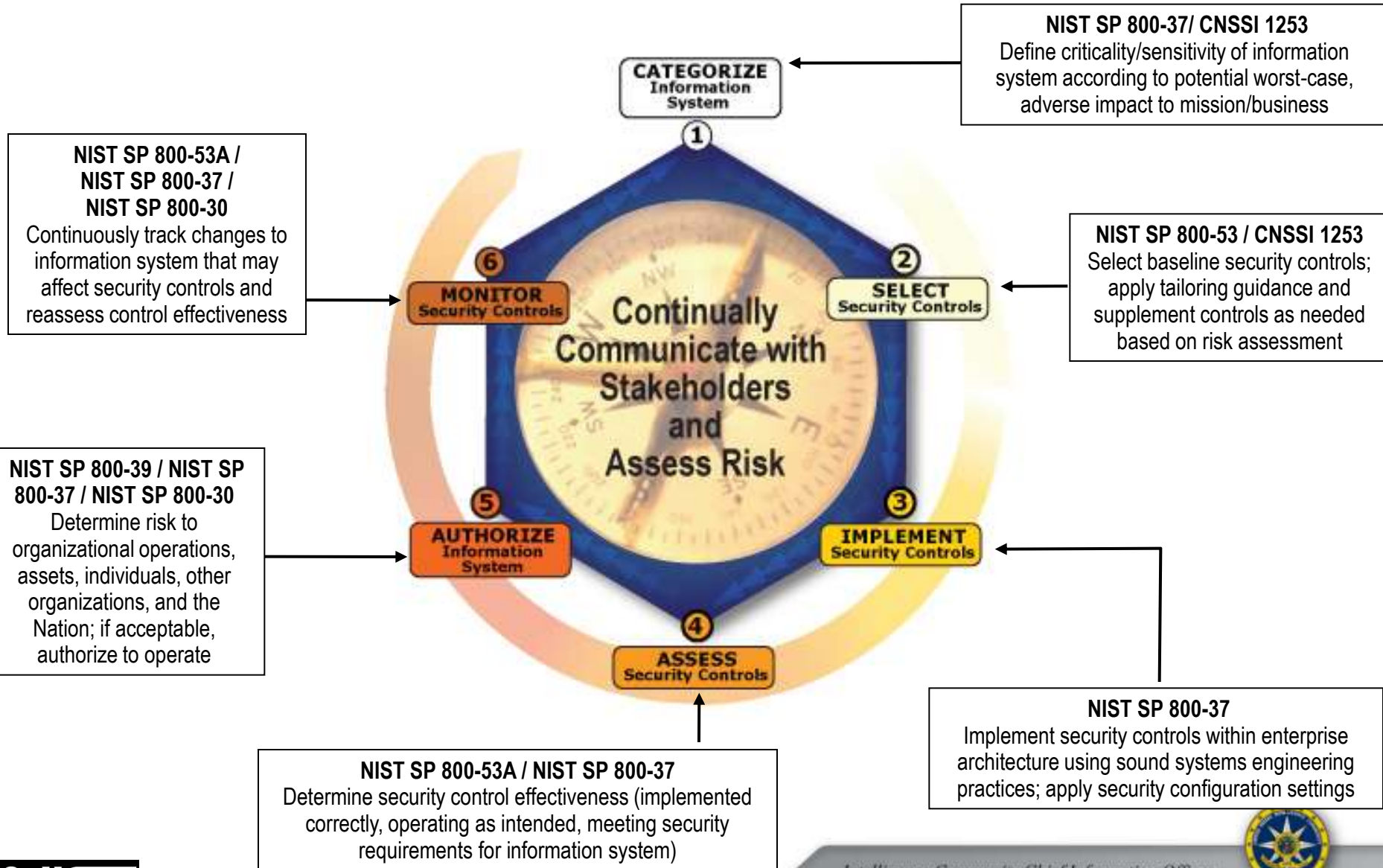
- Linkage to SDLC
- Information System Categorization
- Selection of Security Controls
- Security Control Allocation and Implementation
- Security Control Assessment
- Risk Acceptance
- Continuous Monitoring



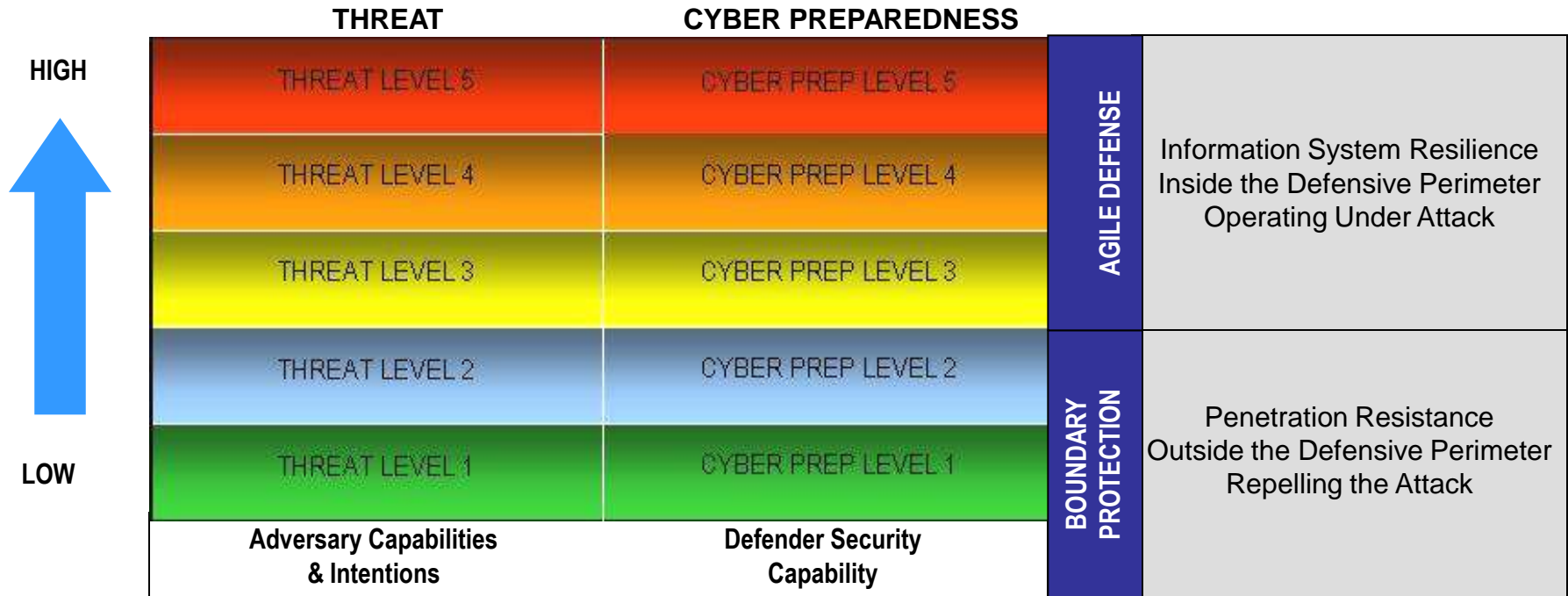
Risks Exist Across Hierarchy



Risk Management Framework



Cyber Preparedness



An increasingly sophisticated and motivated threat requires increasing preparedness...



Understanding Risk Tolerance

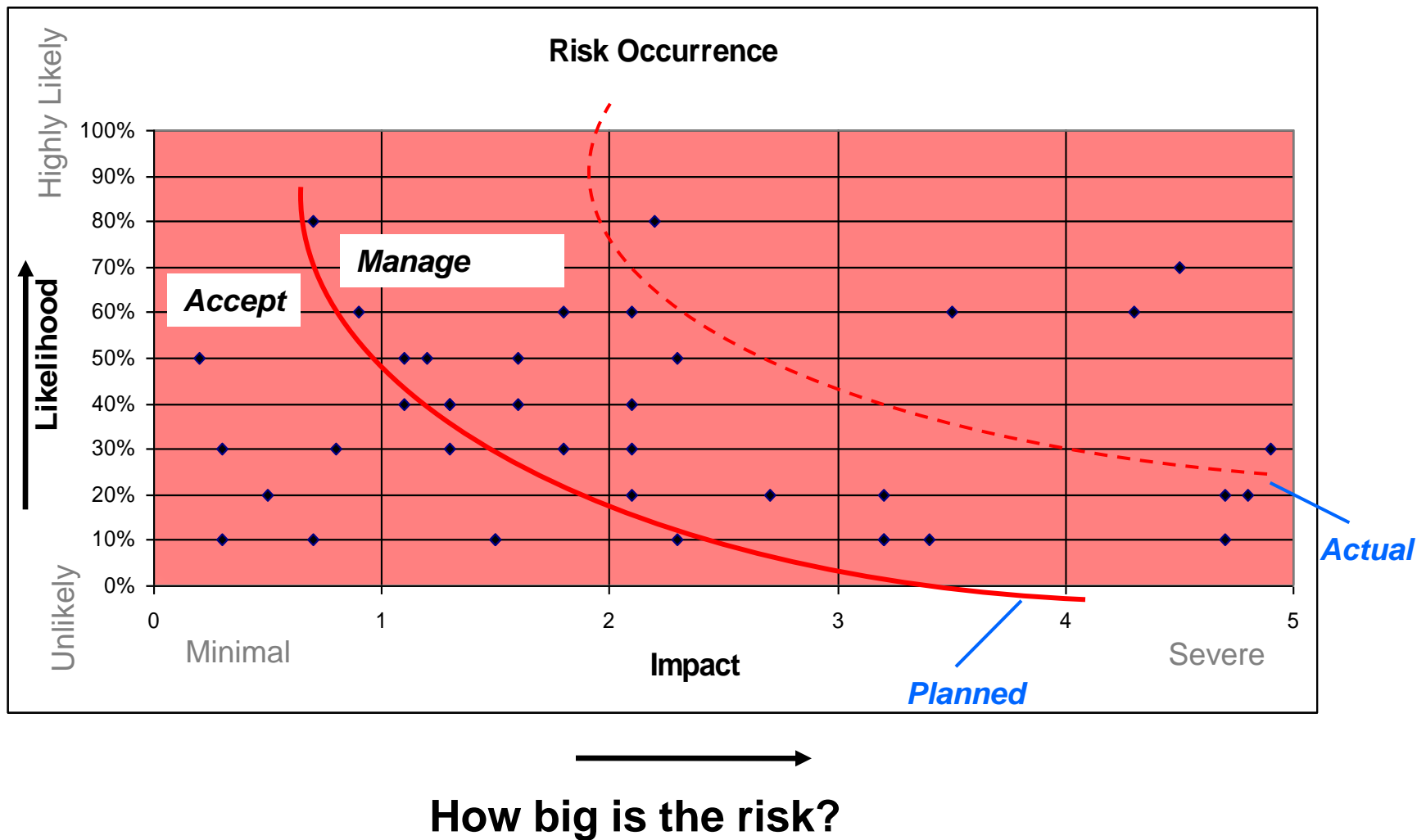
- ***Organizational risk tolerance is the degree of risk that an organization is willing to accept***
 - Consistent with strategic planning objectives
 - Set within the context of the mission
 - Can shape depth / range of security controls selection

- **Establish priorities for best use of limited resources and minimal exposure based on:**
 - Range of risk types an organization faces
 - Degree of interconnection across the enterprise
 - Determination of the types of risk that require immediate action
 - Past occurrence of risk and how things were managed

- **Establishing risk tolerance not an exact science**



Organizational Risk Tolerance Example



Decision Making and Risk

- **Risk response options**
 - **Accept risk**
 - **Operational risk reduction** or mitigation via mgmt and operational security control and/or compensating controls
 - **Technical risk reduction** or mitigation through corrective action and/or compensating technical controls
 - **Contractual risk transfer** (outsource)
 - **Transfer** of risk to a 3rd party (e.g., insurance)
 - **Reject risk** (without pursuing mitigation)

- **Not all options are available at all times**



Risk Executive Function (REF)

- Organizations have flexibility in determining the specific structure and assignment of the risk executive function: person, office, or governance board
- Provides an *organization-wide perspective* on all sources of risk
- Helps the organization understand the relationships between risks, including mission, information technology, budget, and security
- Identifies overall risk posture based on aggregated risks
- Helps to ensure consistency in organizational approach to accepting risks
- Promotes cooperation and collaboration among mission and business leaders and authorizing officials
- Acts as an advisor to the Authorizing Official (AO), but does NOT make authorization decisions



Authorizing Official

- **Authorizing Officials are responsible for making the final decision of *whether or not to authorize a system to operate***

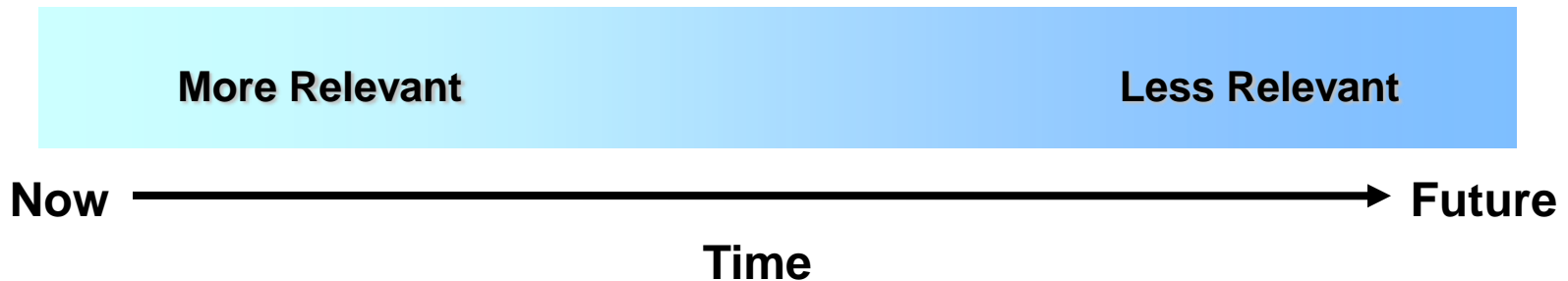
- **Their decision takes into account:**
 - Content of the authorization package
 - System Security Plan (SSP)
 - Security Assessment Report (SAR)
 - Plan of Actions & Milestones (POAM)
 - Risk Executive (Function) inputs, including
 - Mission and business requirements
 - Organizational risk tolerance, risk strategy
 - Other organizational risks not directly associated with the information system

- **Determines risk acceptability**
 - ***Acceptable*** - Issues an authorization to operate (ATO) for a specified period of time
 - ***Unacceptable*** - Does not issue an ATO or halts activity on an information system currently in operation



Risk / Time Relationship

Risk or the perception of risk is significantly influenced by the concept of time



The further out the timeframe, the greater the frequency of questions of relevance



“It must be safe to tell the truth”



*Ed Catmull, “How Pixar Fosters Collective Creativity,”
Harvard Business Review, September 2008*



Case Study Exercise PART A: The Really Awesome Database (RAD) System

- **Instructions for Part A:**
 - Partner with the person next to you
 - Review case study materials, including: instructions, system security plan, security assessment report, and plan of actions and milestones
 - Develop responses to case questions (*see next slide*) and document any assumptions on the template provided
 - Be prepared to share your case findings with the class
 - You have 20 minutes to read the materials and work with your partner



Case Study Exercise: PART A Debrief

- **Would you approve the system for operation based on the information available?**
 - If YES, are there specific terms and conditions surrounding the authorization? What is the authorization termination date?
 - If NO, what are the reasons why?
- **What assumptions did you make that influenced your decision?**



Case Study Exercise: RAD System PART B

- **Instructions for Part B:**
 - With your learning partner, review the instructions and risk executive meeting notes
 - Develop responses to case questions (*see next slide*) and document any assumptions on the template provided
 - Be prepared to share your case findings with the class
 - You have 15 minutes to read the materials, and work with your partner



Case Study Exercise: PART B Debrief

- **Did the additional information from the Risk Executive cause you to change your authorization decision? Please explain why or why not.**
- **If your authorization decision changed, please explain how (e.g., terms and conditions, authorization termination date)?**



Summary

- **You should take away from this presentation**
 - An understanding of what is meant by an organizational perspective on risk, and why it is important to information security
 - An understanding of risk tolerance and its role in decision-making
 - An understanding of the role of the REF
 - A feel for how the REF's perspective on risk can influence an authorizing decision

- **An enterprise-wide view of risk management**
 - Requires a holistic approach
 - Takes into account strategic goals and the relationship between mission & business processes and the supporting information systems
 - Brings together best collective judgments to provide adequate security and risk mitigation



Contact Information

- **NIST Information Technology Laboratory**
 - Project Leader: Dr. Ron Ross, (301) 975-5390
 - Website: www.nist.gov

- **IC CIO C&A Transformation**
 - Program Manager: Roger Caslow, 703-983-3340
 - Senior Risk Advisor: Jennifer Fabius Greene, 703-983-3449
 - Intelink-U: <https://www.intelink.gov/ICTG/ca.intel>
 - Intelink-TS: http://www.intelink.ic.gov/ICTG/ppd_ca.intel

