Integrating IT Security into Capital Planning and Investment Process

Workshop

National Institute of Standards and Technology

Schedule

8:30AM - 9:00AM	Arrival and Registration
9:00AM - 9:10AM	Introduction
9:10AM - 10:30AM	FY03 FISMA Reporting Instructions and Plans of Action and Milestones Guidance
10:30AM - 10:45AM	Break
10:45AM - 11:05AM	Requirements Overview
11:05AM - 11:30AM	Security Investment Life-cycle Planning
11:30PM - 1:00PM	Lunch
1:00PM - 1:10PM	Questions from Morning Session
1:10PM - 2:10PM	Security Investment Life-cycle Planning
2:10PM - 2:20PM	Questions from Afternoon Session
2:20PM - 3:05PM	Breakout Session
3:05PM - 3:50PM	Outbrief of Breakout Session
3:50PM - 4:00PM	Wrap Up

NIST National Institute of Standards and Technology

Introduction

NIST
National Institute of Standards and Technology

Information Technology (IT) Security Capital Planning and Investment Control (CPIC) Training

Audience: Federal IT personnel responsible for investment request development and approval

- IT managers and security professionals
- Security program managers
- Investment Review Board (IRB) participants

Goal:

- Demystify CPIC process for federal IT security officials
- Provide a roadmap for the federal IT personnel on how to integrate IT security into CPIC process
- Solicit feedback

Duration: 6 hours

NIST National Institute of Standards and Technology

Objectives

After completing this workshop, you will be able to:

- Identify relevant Office of Management and Budget (OMB) and other guidance that applies to governing Federal Government IT security investment decisions
- Explain how current security requirements relate and support the IT CPIC process
- Describe the CPIC process phases: select, control, evaluate
- Identify CPIC-related roles and responsibilities
- Explain best practices IT security management process and why it is important for making sound IT security investment decisions
- Have an understanding of how to develop security requirements and appropriate supporting documentation for IT acquisition
- Identify steps and materials required to complete sound business case in support of investment requests
- Have an understanding of implementation issues associated with incorporating IT security into CPIC process

NIST National Institute of Standards and Technology

FY03 FISMA Reporting Instructions and Plans of Action and Milestones Guidance

Requirements Overview

In this section, you will:

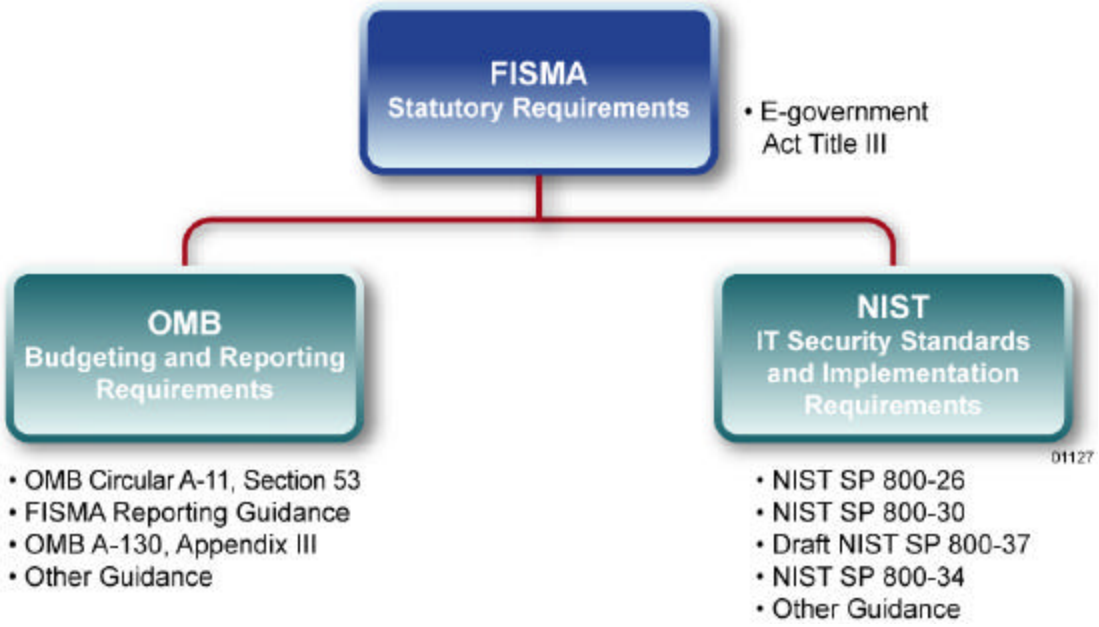
- Learn about OMB, NIST, and other guidance that applies to governing Federal Government IT security investment decisions
- Identify relationship between current security requirements and IT CPIC requirements
- Learn the steps of the CPIC process
- Learn about the basics of risk management and its importance
- Identify different types of investment risks in addition to security risks

NIST
National Institute of Standards and Technology

Current Requirements

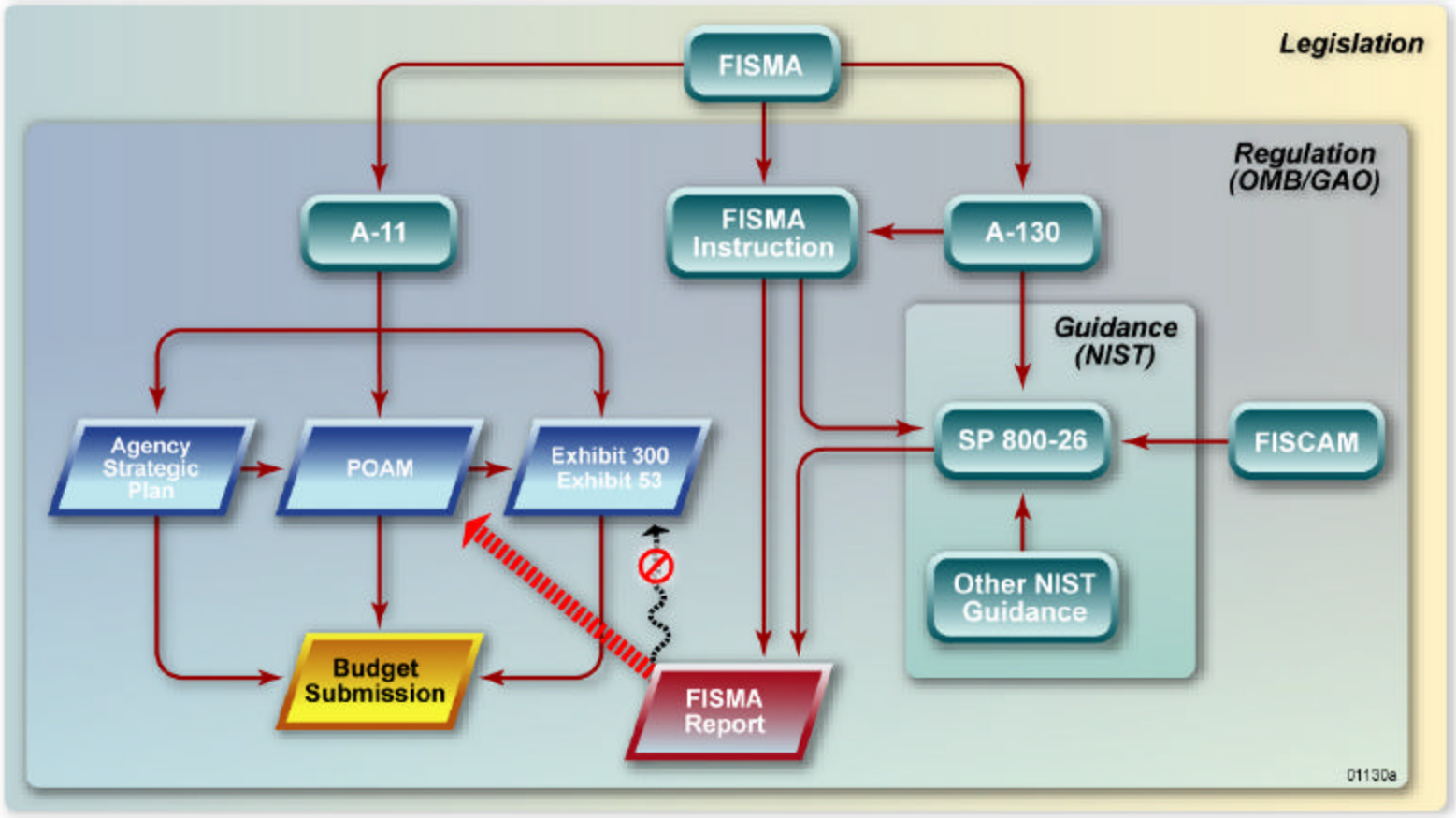
Federal Information Security Management Act (FISMA) requires integration of IT security into capital planning

- OMB provides capital planning and FISMA reporting requirements
- NIST publishes guidance on security implementation



Relationship Between IT Security and Capital Planning Guidance

- Combination of FISMA legislation, OMB requirements, and NIST **guidance** point at the common goal of using strategic planning and sound business decisions to plan security-related investments



Overview of OMB A-11 IT Security-Related Requirements

- Report on IT by submitting Exhibit 53
- Link IT investments to the President's Management Agenda
- Ensure that Exhibit 53 is complete by filling out all parts
  - IT systems by mission area
  - IT infrastructure and office automation
  - Enterprise architecture and planning
  - Grants management
- All parts use a number of common elements, one of which is **Percentage IT Security:** percentage of the total investment for a budget year associated with IT security for a specific project:
  - Direct costs of providing IT security for the specific IT investment (does not include Inspector General [IG] activities)
  - Products, procedures, and personnel that have an incidental or integral component, a quantifiable benefit for the specific IT investment
  - Allocated security control costs for networks that provide some or all necessary security controls for associated applications

NIST National Institute of Standards and Technology

Direct Costs of Providing IT Security for the Specific IT Investment

- Risk assessment
- Security planning and policy
- Certification and accreditation
- Specific management, operational, and technical security controls
- Authentication or cryptographic applications
- Education, awareness, and training
- System reviews/evaluations (including system security test and evaluation [ST&E])
- Oversight or compliance inspections
- Development or maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment
- Contingency planning and testing
- Physical and environmental controls for hardware and software
- Auditing and monitoring
- Computer security investigations and forensics
- Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations

See the handout with detailed crosswalk to the NIST SP 800-26 topic areas and specific NIST guidance documents that describe implementation of these items

Products, Procedures, and Personnel with a Security-Related Component

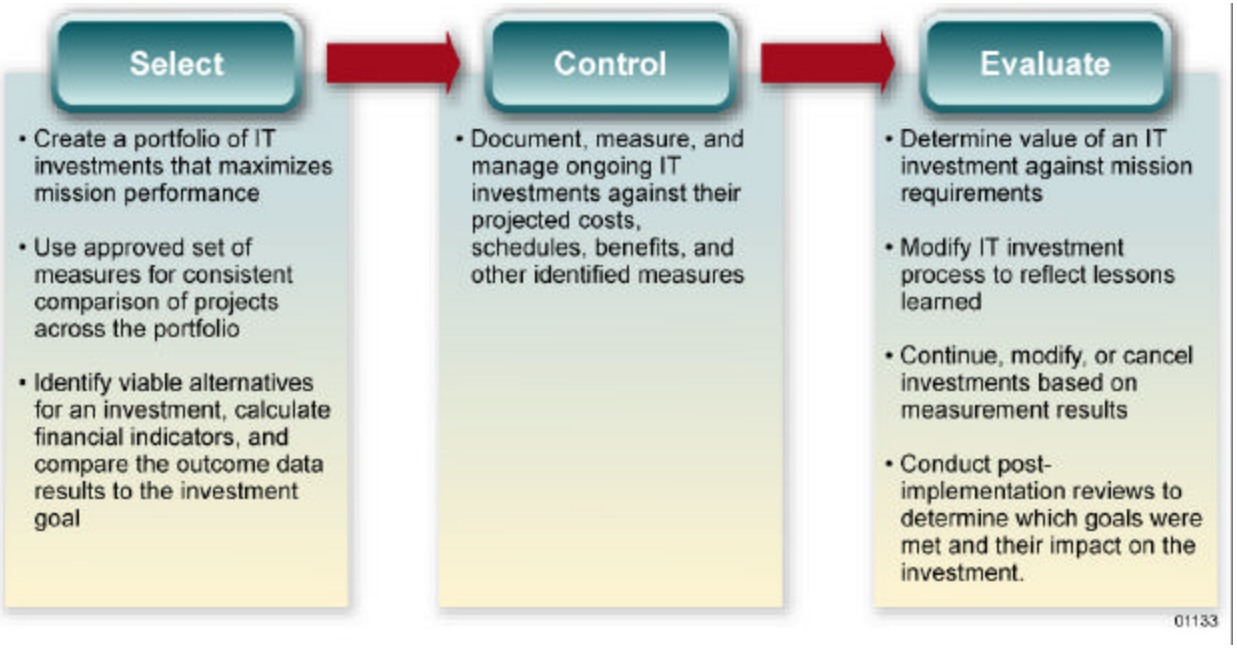
- Configuration or change management control
- Personnel security
- Physical security
- Operations security
- Privacy training
- Program/system evaluations whose primary purpose is other than security
- System administrator functions
- System upgrades with new features that obviate the need for other stand-alone security controls

See the handout with detailed crosswalk to the NIST SP 800-26 topic areas and specific NIST guidance documents that describe implementation of these items

NIST National Institute of Standards and Technology

Investment Management Life Cycle

- Specific practices and decisions occur during each phase of the Select-Control-Evaluate life cycle to optimally manage IT investments



NIST National Institute of Standards and Technology

Why is Risk Management Important?

Without a strong and consistently applied risk management process, project managers are more likely to:

- Assign inadequate resources to mitigate or resolve major risks
- Make key decisions without adequate information
- Have little insight into potential problems
- Repeat mistakes that plagued earlier projects
- Devote resources to rework rather than problem avoidance
- Fail to deliver a compliant product or service on time and within budget

NIST
National Institute of Standards and Technology

A Best-Practices Approach to Risk Management

These program elements are structured to ensure that risk management is practiced in a consistent, coordinated, and controlled manner throughout the life cycle of a project

NIST National Institute of Standards and Technology

Types of Investment Risk

Comprehensive risk assessments effectively apply a risk management process that integrates the skills, knowledge, and experience of a variety of specialists and the customer. OMB has identified eight categories of risk:

- Project Resources/Financial
- Technical/Technology
- Business/Operational
- Organizational and Change Management
- Data/Information
- **Security**
- Strategic
- Privacy

In addition to the eight OMB-defined areas of risk, a comprehensive risk assessment should include the assessment of each of the following categories:

- Product Risk Assessment
- Process Risk Assessment
- **Threat and Requirements Risk Assessment**
- Cost Risk Assessment
- Quantified Schedule Risk Assessment

All risks, including security, contribute to the calculation of risk-adjusted cost, now required to be reported

See the handout that lists definitions of each type of investment risk

Integration of Security into the Capital Planning and Investment Control Process

Subsections

- Security-related CPIC roles and responsibilities
- Development of budget submission from security point of view
- Implementation issues

NIST
National Institute of Standards and Technology

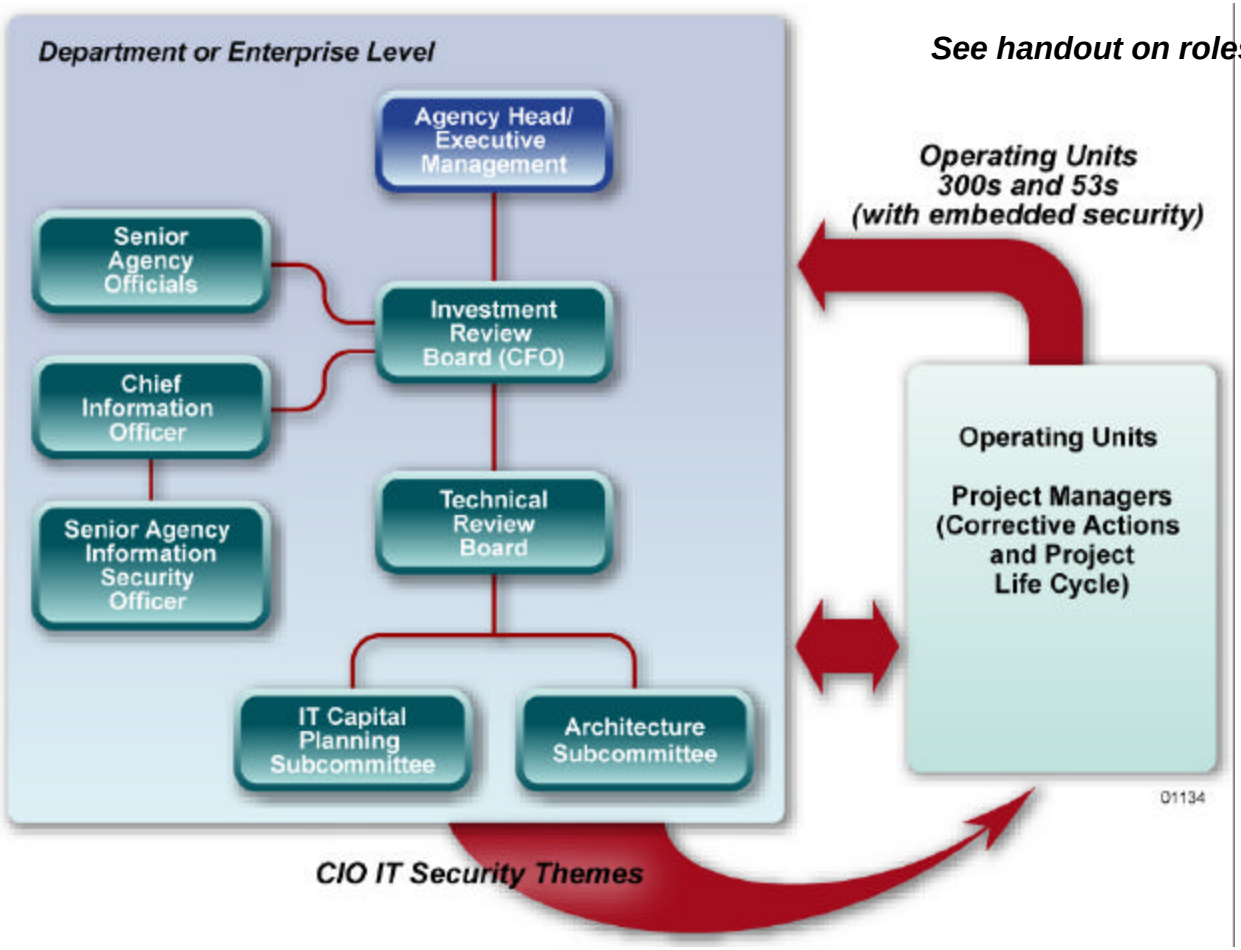
Security-Related CPIC Roles and Responsibilities

In this section, you will:

- Learn roles and responsibilities of agency officials regarding integrating IT security into the IT CPIC process

IT Management Hierarchical Diagram

Components of IT management oversee the operating units to ensure that the IT investment pool consists of a strategic mix of investments, enabling achievement of agency mission goals and objectives



See handout on roles and responsibilities

Development of Budget Submission From Security Point of View

NIST National Institute of Standards and Technology

In this section, you will:

- Identify key milestones and activities of the IT CPIC process
- Learn best practices for prioritizing IT security corrective actions for implementation
- Gain an understanding of how to develop security requirements and appropriate supporting documentation for IT acquisition
- Identify steps and materials required to complete a sound business case in support of investment requests

NIST National Institute of Standards and Technology

Integration of Security into the CPIC Process

- Use information security metrics to determine security baseline
- In the absence of information security metrics, use available data to determine security baseline
- Evaluate current security posture against requirements
- Identify Chief Information Officer (CIO)-articulated IT security themes that align with mission goals
- Prioritize initiatives around requirements to align with mission goals
- Develop concept paper, business case analysis (BCA), other supporting materials, and Exhibit 300 for prioritized initiatives
- Submit business cases to the IRB
- Prioritize agency-wide business cases against CIO themes
- Determine investment portfolio
- Approved Exhibit 300s become part of the agency's Exhibit 53s
- Manage investments throughout life cycle

NIST National Institute of Standards and Technology

Integrating Security into Each Step of the CPIC Process: CPIC View

Critical IT security analysis and decisions occur throughout the CPIC process

	Select	Control	Evaluate
Identify Baseline	Agency-specific and federally mandated security requirements are identified. Metrics are used to determine agency's compliance with requirements	Project managers monitor investment performance against baseline to ensure no new corrective actions are necessary to mitigate security compliance gaps	Post Implementation Reviews are conducted to determine whether the investment has achieved its desired results Metrics are used to evaluate investment performance against the baseline
Identify Prioritization Requirements	Agency CIO or other senior management official articulates IT security themes based on agency mission goals and priorities	Agency CIO or other senior management official articulates IT security themes based on agency mission goals and priorities	
Prioritize Against Themes	Project managers prioritize investments based on CIO - articulated themes and score initiatives against each other on specific risk, financial, technological, management, legislative, and OMB requirements	Project managers monitor initiatives against the changing CIO's IT security themes and performance criteria to determine whether they are achieving anticipated results and if any modifications are necessary	
Develop Supporting Materials	Project managers develop business cases and other supporting materials to support initiatives aligned to agency mission and goals	Project managers ensure their initiatives remain aligned with evolving mission and goals as the initiatives mature	
Perform Portfolio Management - IRB	The IRB reviews completed business cases and selects an appropriate mix of investments for inclusion in the agency's portfolio. IRB can use prioritized corrective actions as a selection criterion. Successfully scored initiatives are added to the OMB investment pool, pending funding approval from OMB	The IRB reassesses initiatives that have undergone major modifications and monitors costs and security performance	
Develop Exhibit 53s, 300s, Program Management	Project managers prepare and submit Exhibit 300 and Exhibit 53 budget request/justification materials and submit the documentation to OMB for review and funding approval	Project managers review and update Exhibit 300s annually to reflect changes in the investment	01146

NIST National Institute of Standards and Technology

Integrating Security into Each Step of the CPIC Process: Security View

Security drivers impact decision making and guide strategy throughout the select-control-evaluate investment life cycle

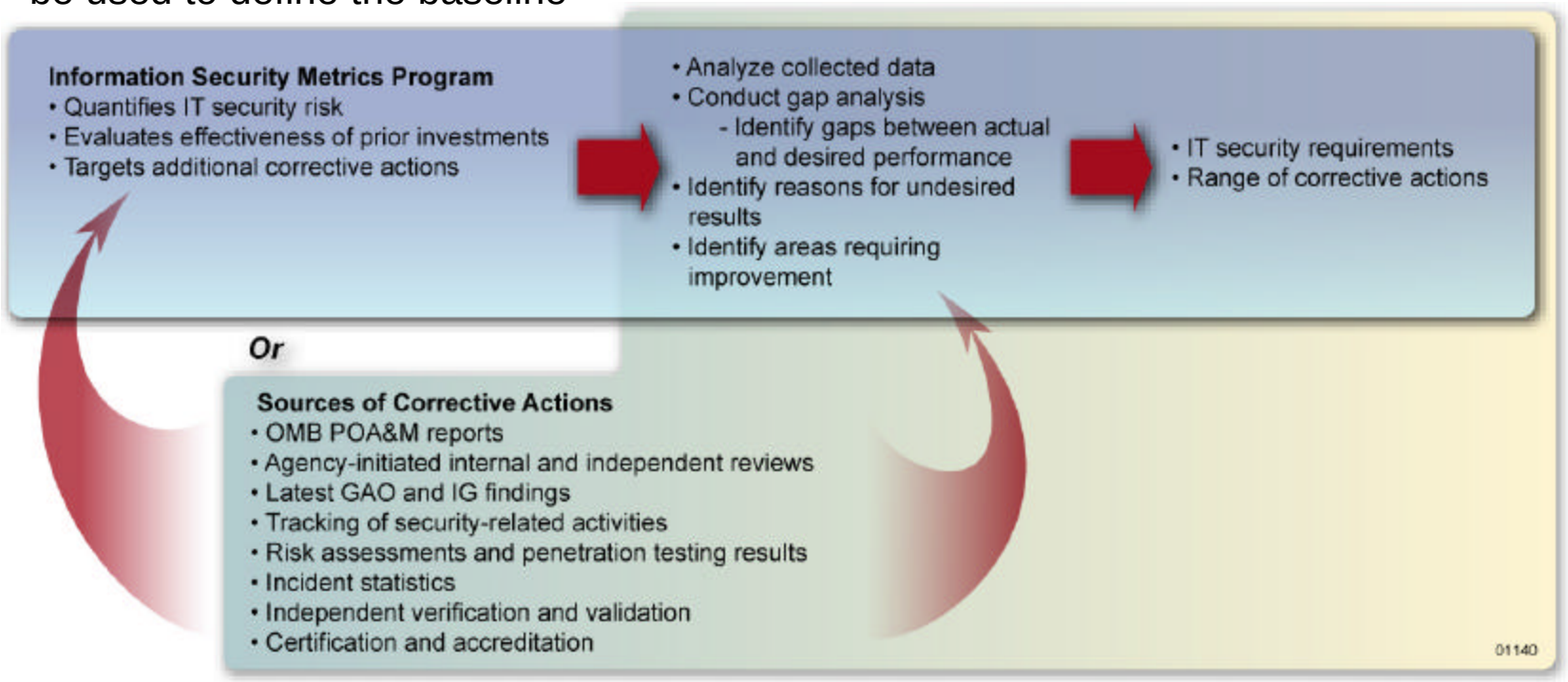
	Select	*Control*	*Evaluate*
Initiation	• Data Sensitivity Analysis • Privacy Impact Assessment		
Development or Acquisition	• Risk Assessment • System Security Plan • POA&M	• Security Controls • Contingency Planning • Security Test and Evaluation • Certification	
Implementation		• Approval/Authorization to Operate	
Operations and Maintenance		• Continuous Monitoring • Use Metrics	• Periodic Reviews • Annual Self-assessment • Recertification
Disposition			• Removal from Operational Status • Media Sanitization

01147

NIST National Institute of Standards and Technology

Identify Baseline

- Existing information security metrics program provides the best way to define the baseline
- Information security metrics program uses existing data sources to create a quantifiable picture of security posture throughout an organization
- In absence of an information security metrics program, the same data sources can be used to define the baseline



NIST National Institute of Standards and Technology

Identify Prioritization Criteria

- Available funding usually does not cover all requirements resulting from the security baseline needs assessment
- Requirements must be prioritized to address the most pressing security investment needs first — by statute, risk is a primary driver
- Corrective actions should be prioritized to ensure the most effective use of resources
- Requirements should be prioritized based on specific criteria articulated by the agency CIO or other senior management official that allows IT security investments to be rank ordered:
  - Federal government priorities
    - ✓ President's management agenda
    - ✓ Federal enterprise architecture requirements
    - ✓ E-government scorecard
    - ✓ Compliance with rules and regulations — Clinger-Cohen, Presidential Decision Directives (PDD), FISMA, HIPAA
    - ✓ NIST standards and guidance
  - Agency mission and goals that align with specific agency concerns and its risk profile
  - Government and agency initiatives, for example
    - ✓ Electronic tax filing, E-Clearance, E-Grants
    - ✓ Operating units within agencies will develop their IT security investments in alignment with the CIO- articulated IT security themes

IT Security Themes Discussion

Security themes embody an agency's approach to IT security, which can be used to drive cultural change and prioritize security activities

- Use qualitative and quantitative criteria
- Themes should evolve over time, reflecting the changing maturity level of the security program, the security culture, and the environment (technology and threats)

Examples of themes are:

- Complying with statutory requirements in Clinger-Cohen, FISMA, and guidance in OMB A-130
- Implementing a risk-based security program (FISMA and Executive Orders)
- Safeguarding National and Department mission-critical assets (PDD-63 and Executive Order 13231)
- Achieving Federal Information Technology Security Assessment Framework (FITSAF) maturity level 4 (or 5) security program
- Completing certification and accreditation of all systems in accordance with NIST guidance and standards

What are other relevant themes?

- _____
- _____
- _____

NIST National Institute of Standards and Technology

Prioritization Criteria Examples

- Strategic view
  - Linkage with a government-wide initiative
  - Impact on agency goals
  - Impact on E-government scorecard improvement to result from activity
  - Mission criticality

- IT Security view
  - Support of agency mission: system and information sensitivity
  - Security controls:
    - ✓ NIST SP 800-26 topic areas or critical elements
    - ✓ Management, operational, and technical controls
    - ✓ Similar agency-specific framework
  - Results
    - ✓ Improvement in compliance with regulations
    - ✓ Reduced cost of implementation
    - ✓ Acceptance of residual risk
  - Impact
    - ✓ Magnitude of impact on the overall departmental security posture
    - ✓ Cost effectiveness of the action (“bang for the buck”)

We will concentrate on prioritizing corrective actions within the scope of security

NIST National Institute of Standards and Technology

Prioritize Against Requirements: Overview

- Corrective actions should be prioritized based on the identified criteria to ensure the most effective use of resources
  - Prioritize system-level corrective actions based on root causes of problems
  - Prioritize enterprise-wide security control-level corrective actions based on root causes of problems
- Prioritization should be performed at the operating unit level and at the CIO level
- Specific prioritization process should provide the opportunity for “management override” of priorities
- Partial automation of calculations and rankings should be considered to reduce administrative burden and the chance of human error
- Metrics should be used to inject greater objectivity into the process
- Ranking quantitative and qualitative information into high, medium, and basic categories helps summarize results of prioritization

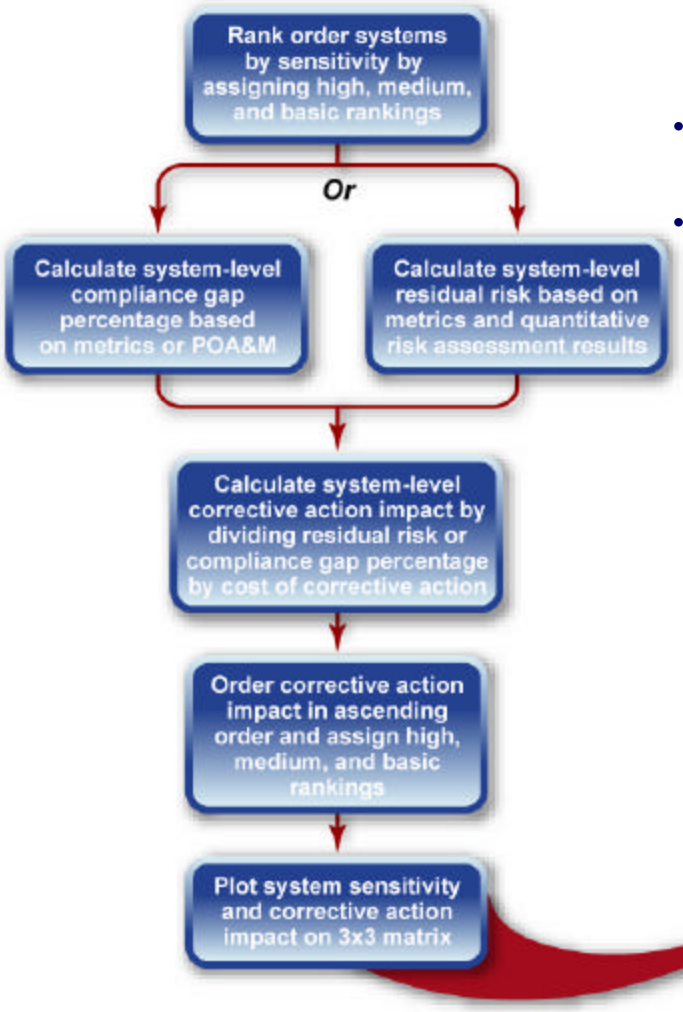
NIST National Institute of Standards and Technology

Notional Corrective Action Prioritization Inputs

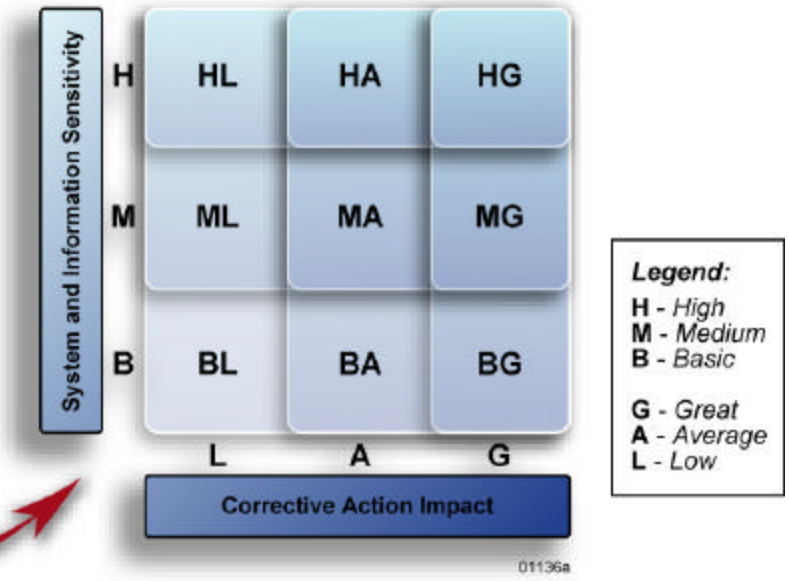
ID	NIST SP 800-26 Topic Area (TA)	Importance Ranking	Corrective Action Compliance From POAM			Average Across Department	Security Compliance Gap %	Corrective Action Cost	Corrective Action Impact	Category
			System X	System Y	System Z					
	Formula=	From Step 1				(A+B+C)/3=	(100%-D)=	(POAM)=	(E/F)x100,000=	
	Column=	AA	A	B	C	D	E	F	G	H
RM	Risk Management		90%	80%	65%	78%	22%	$168,335		
RS	Review of Security Controls		75%	90%	10%	58%	42%	$179,139		
LC	Life Cycle		25%	12%	15%	17%	83%	$117,789		
AP	Authorize Processing		5%	10%	5%	7%	93%	$237,350		
SP	System Security Plan		100%	95%	90%	95%	5%	$196,143		
PS	Personnel Security		90%	90%	100%	93%	7%	$82,263		
PH	Physical Security		75%	75%	75%	75%	25%	$88,762		
PI	Production, Input/ Output Controls		25%	30%	10%	22%	78%	$457,120		
CP	Contingency Planning		15%	25%	50%	30%	70%	$482,347		
HS	Hardware and Systems Software Maintenance		25%	25%	25%	25%	75%	$450,959		
DI	Data Integrity		50%	10%	0%	20%	80%	$328,506		
DC	Documentation		75%	100%	50%	75%	25%	$144,755		
SA	Security Awareness, Training, and Education		50%	0%	100%	50%	50%	$133,898		
IR	Incident Response Capability		50%	25%	30%	35%	65%	$81,161		
ID	Identification and Authentication		50%	25%	60%	45%	55%	$441,880		
LA	Logical Access Controls		25%	10%	75%	37%	63%	$248,154		
AT	Audit Trails		0%	100%	75%	58%	42%	$94,326		

NIST National Institute of Standards and Technology

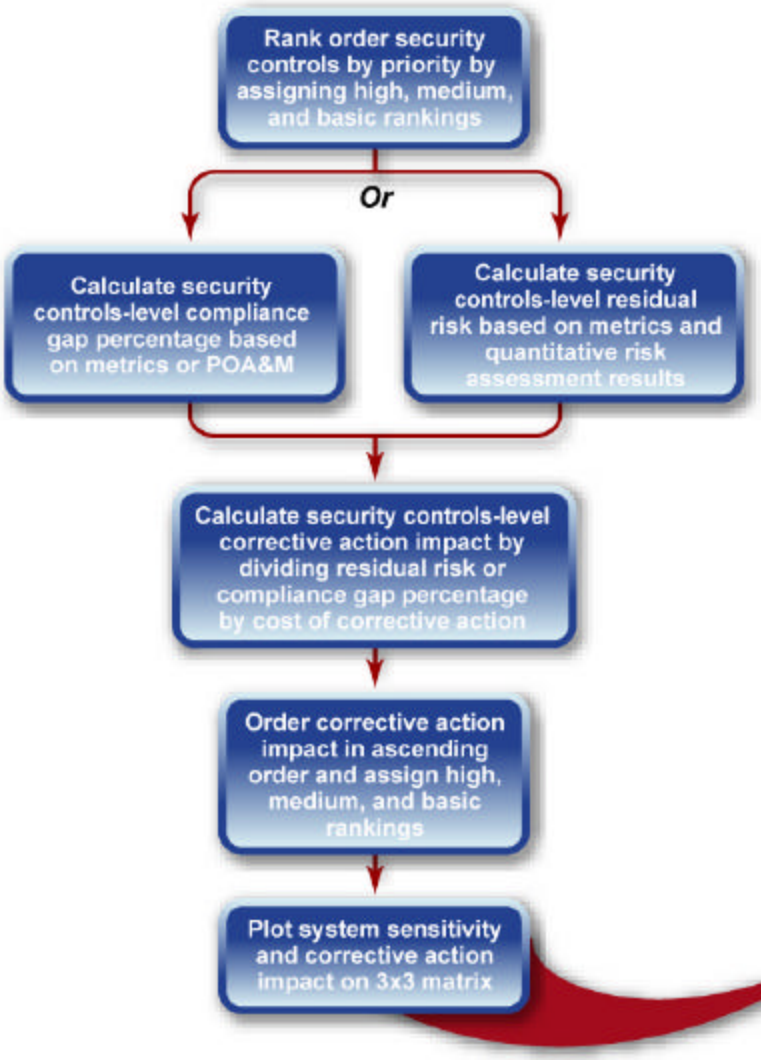
Prioritize Against Requirements: Prioritizing System-Level Corrective Actions



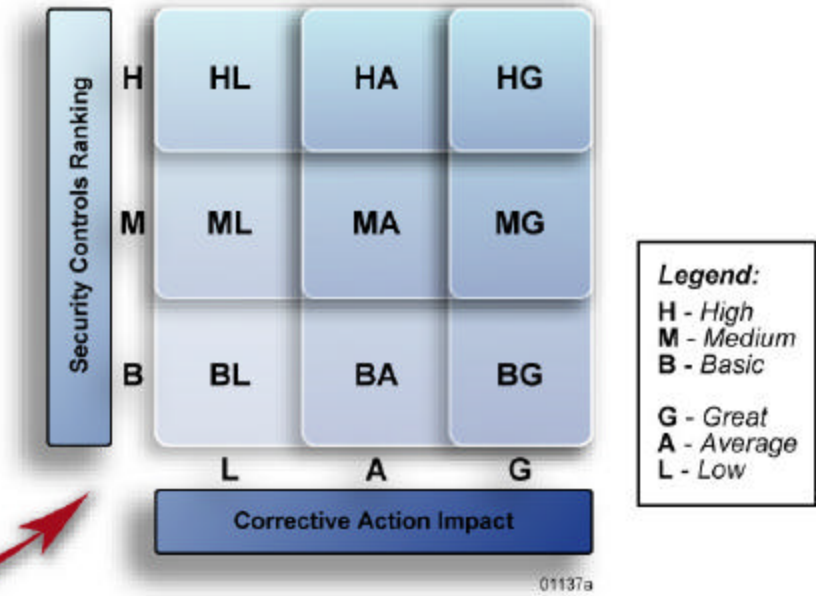
- System-level compliance gap percentage = 100% (full compliance) – Percentage compliance with policy as determined by the metrics program for each individual system
- Compliance percentage gap or residual risk should be calculated for each system
- Corrective action impact = (compliance gap percentage for each system)/ (cost of all corrective actions for each system)



Prioritize Against Requirements: Prioritizing Enterprise-Wide Security Controls-Level Corrective Actions



- Security controls-level compliance gap percentage = 100% (full compliance) — Percentage compliance with policy as determined by the metrics program for each security control throughout agency or agency component
- Compliance percentage gap or residual risk should be calculated for each security control category
- Corrective action impact = (compliance gap percentage for each security control)/(cost of all corrective actions for each security control)

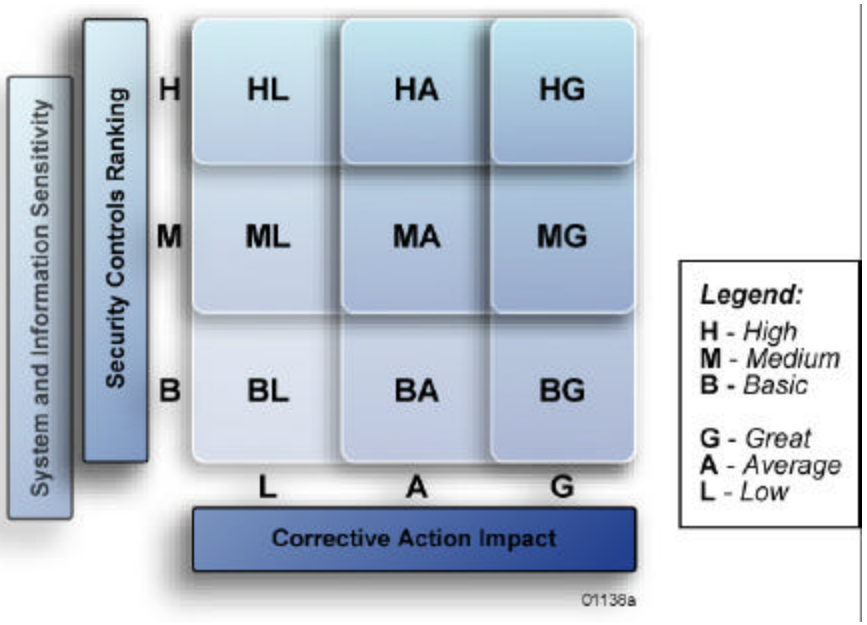


Prioritize Against Requirements: Putting It Together

To further increase efficiency of applied resources, system, and security control matrixes should be overlapped:

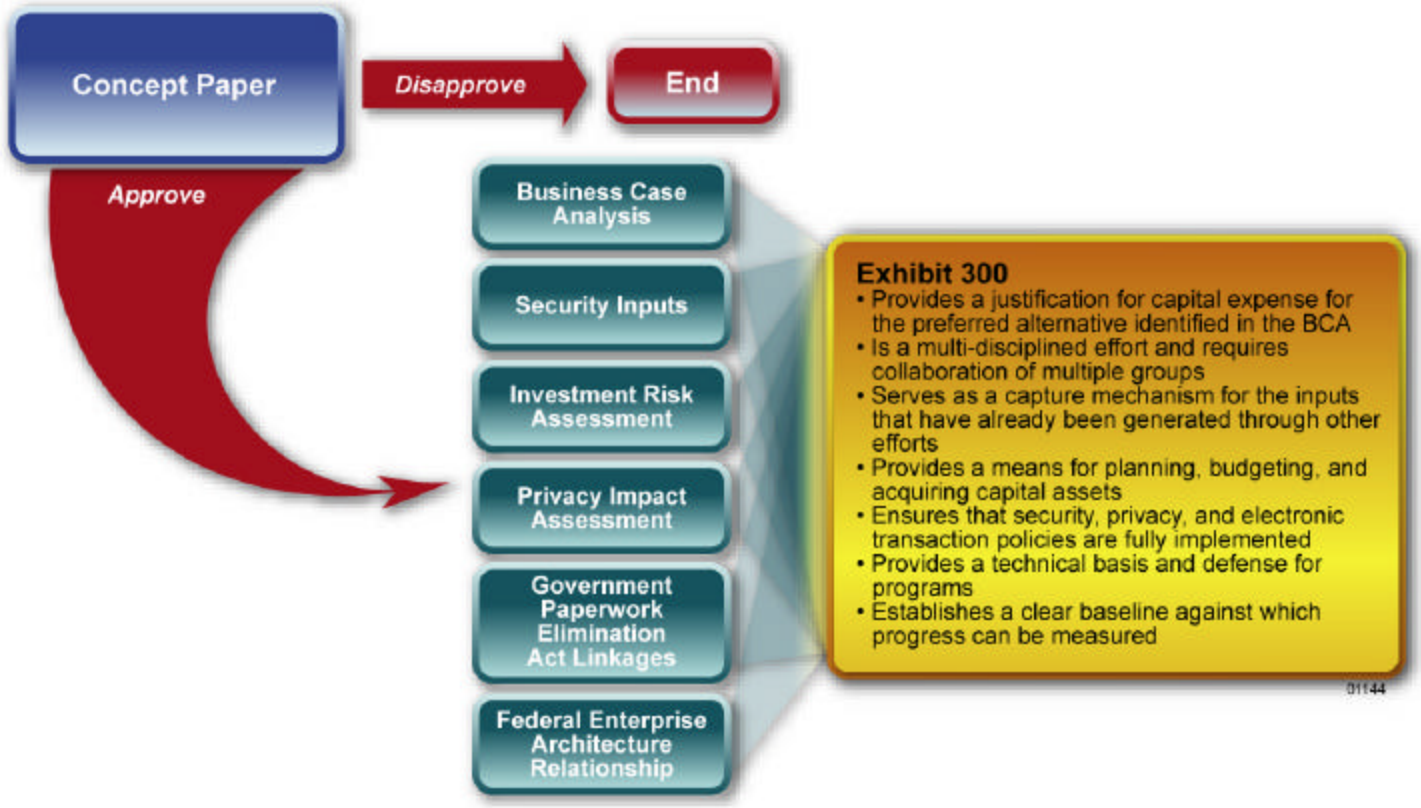
- Identify systems and security controls that fall in the High/Great quadrant
- Those investments that fall in the High/Great quadrants are high-priority investments, while investments that fall into the Basic/Low quadrant are low-priority investments
- Depending on the availability of resources, an agency can implement those investments that fall in the quadrants below and to the left of the High/Great quadrant

The result is a rank-ordered list of cost-effective investments that align with security priorities of the agency



Develop Supporting Materials

Exhibit 300 is a multidisciplined effort that combines inputs generated through other analyses into a comprehensive justification for capital expense for the investment identified in the concept paper



NIST National Institute of Standards and Technology

Alternatives Analysis is a Key Step in Making Good Business Decisions

- OMB A-11 states that every system investment justification (OMB Exhibit 300) must include a minimum of ***three*** alternatives

- The term 'alternative' means:
  - A way of meeting the mission need or providing the functionality needed to accomplish mission/goals (e.g., sometimes a mission need can be met with a new IT system; sometimes by changing business processes)
  - Alternative description that should demonstrate why the selected investment provides the most effective (cost- and performance-wise) manner of meeting the associated mission need (versus different investments or process changes)

- Exhibit 300 guidance requires that a description be provided of the alternatives considered for a project and the results of the feasibility/performance/benefits analysis, including financial and non-financial benefits (such as value to users, citizens, and customers)

NIST National Institute of Standards and Technology

What are Some Examples of Credible Alternatives?

- **Status Quo**
  Status quo, or an explanation of the current method of meeting the mission need, should always be one of the alternatives. Explain the limitations and/or adverse effects on performance associated with the current status. Presumably, an investment would be needed because the current way of meeting the mission need is inadequate.

- **Outsourcing**
  Analyze and document benefits, risks, and costs of outsourcing the function.

- **Government-Owned and -Operated**
  Analyze and document benefits, risks, and costs of maintaining the function within and ownership of assets by the government.

- **Process/Organizational Changes Only**
  This alternative could include a reorganization in the agency or division or the reengineering of a particular business process that helps an organization meet a mission need. Analyze and document benefits, risks, and costs of restructuring processes or functions within the agency versus meeting the mission need with the investment.

- **Information Technology/System Only**
  Investing in a system or IT asset without any underlying organizational changes.

An alternative could also be a mixture of these solutions

NIST National Institute of Standards and Technology

IRB and Portfolio Management

The IRB reviews and selects investments based on business cases forwarded by operating units

- The IRB typically bases investment selection decisions on relation to agency mission and goals, not just on cost
- The IRB will use strategic selection criteria to rank order investment proposals at the department/agency level
- Security typically is not the driving force behind portfolio management, but it is strategically important for the investment strategy because it serves as a qualifier for receiving security funding and a business enabler for those functions that cannot be performed without appropriate security controls

Exhibits 53, 300, and Program Management

Following the IRB's selection of initiatives for the agency's investment pool, the Exhibit 300s are forwarded to OMB to secure funding.

- Exhibit 53 – approved Exhibit 300s become part of Agency Exhibit 53, which contains life-cycle cost estimates for the the agency's IT portfolio

- During the control phase of the investment life cycle, the Exhibit 300 is reassessed annually and modified as necessary to reflect any life-cycle cost estimate updates, security requirements changes, and other items

Roles for Integrating Security into Capital Planning

The roles and responsibilities of the IT management hierarchy and the operating units throughout the CPIC process allow agencies to ensure that both financial and IT security goals and objectives are met

CPIC Steps	Identify Baseline	Identify Priority Requirements	Priority Against Themes	Develop Business Case	Portfolio Management	Develop 53s and 300s
Agency Head		★			★	★
CIO, Senior Agency Information Security Officer, and Senior Agency Officials	▲	▲	▲	●	▲	▲
Investment Review Board	★	●	★	★	★	★
Technical Review Board		●	●	●	●	●
Capital Planning and Architecture Subcommittees	●	●	●	●	●	●
Operating Units	●		▲	▲		▲

01139

Legend: Approves = ★ Leads = ▲ Supports = ●

NIST National Institute of Standards and Technology

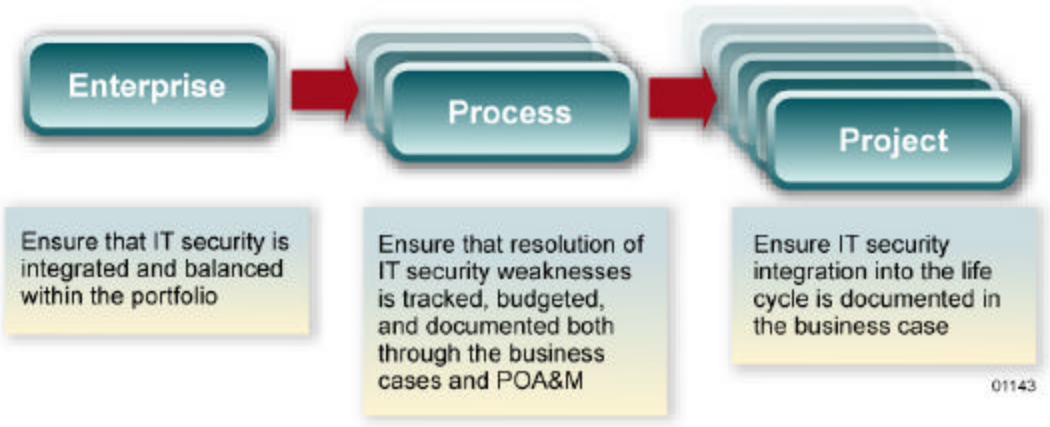
Implementation Issues

In this section, you will:

- Learn about the iterative nature of security integration into the CPIC process
- Identify issues of security decision-making thresholds and legacy system security funding
- Understand how security activities overlap with CPIC activities for multiple budget years throughout a single fiscal year

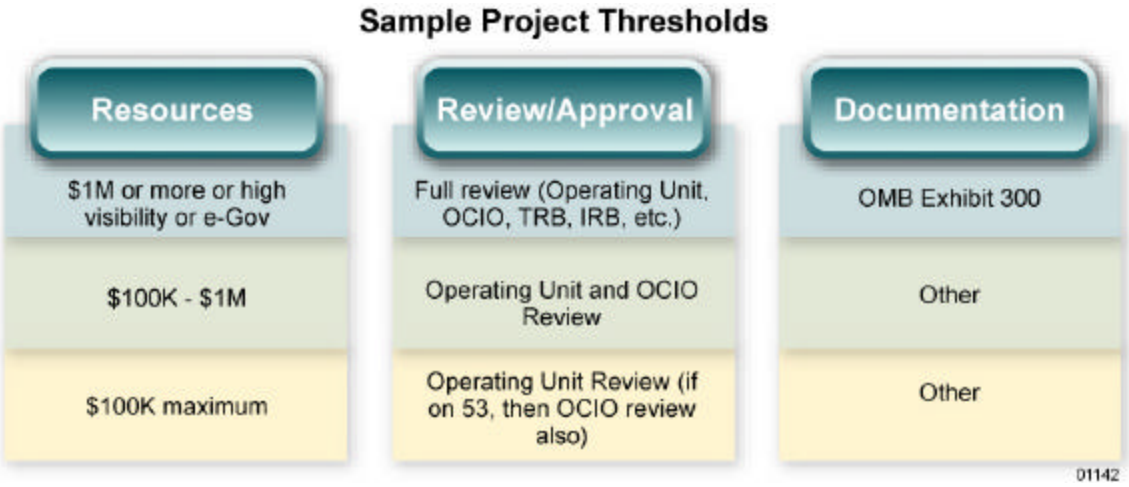
Integration of Security into the CPIC Process Occurs at Multiple Levels of the Organization

Similar processes, which continue to evolve, may be implemented at enterprise and operating unit levels



IT Security Decision-Making Thresholds

Formality of security budget documentation and review is governed by a series of thresholds



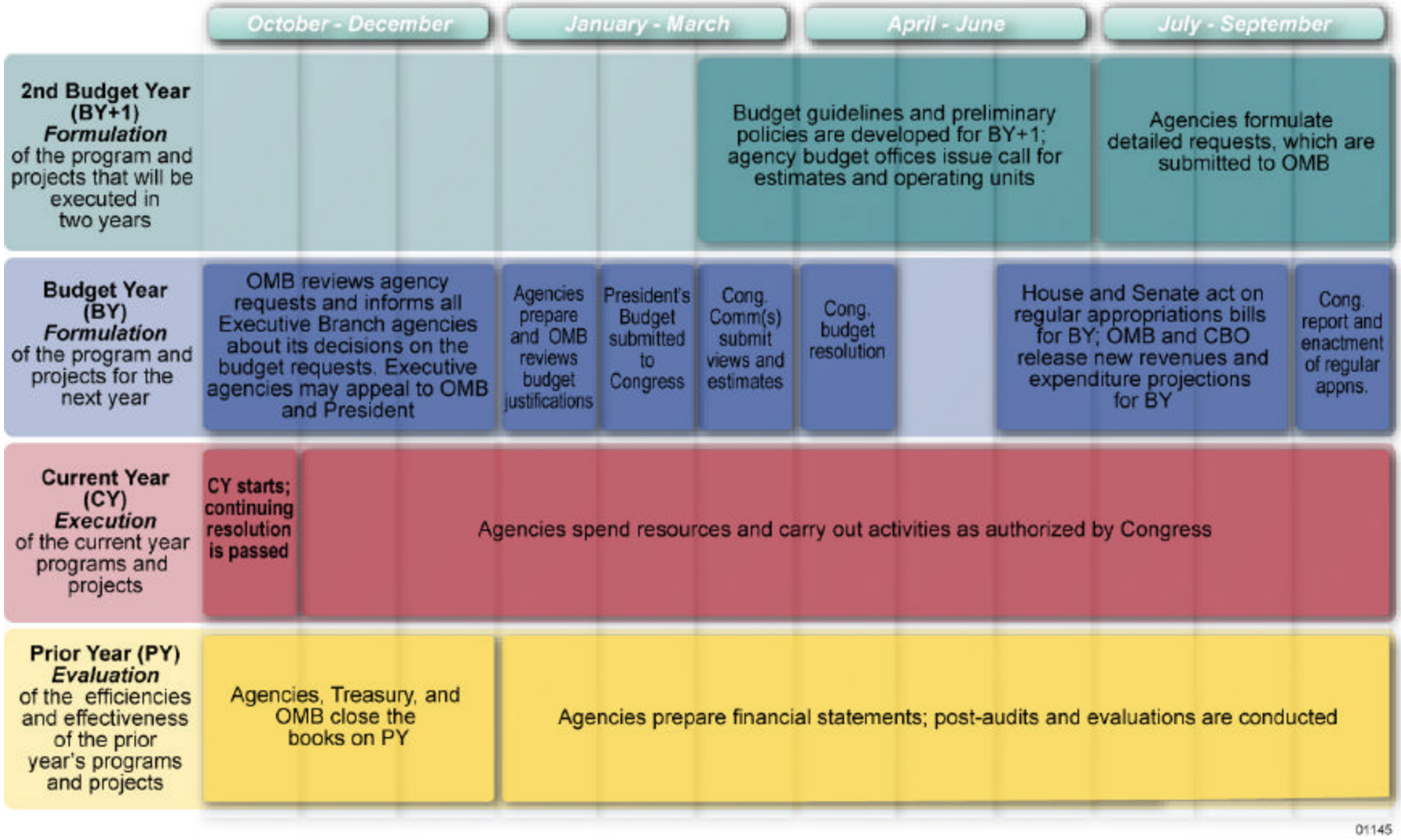
Legacy Systems — A Very Significant Issue

- Legacy systems may rank low from a prioritization standpoint because they:
  - Include existing systems with historically potentially low development/procurement and corrective action costs
  - Accept residual risk
  - Fall into B/L quadrant (lower left area) both from a system and corrective action perspective
  - Are perceived to be of a limited life span
  - Are often well into the IT life cycle and typically at the operating and maintenance or disposition stages
- However, these systems are currently functional and cannot be taken off-line for long periods of time without significant mission impact. They appear (currently and historically) to be working well.
- Typically IT security issues associated with legacy systems include:
  - Lack of current security documentation such as security plans and risk analyses
  - Insufficient management, technical, or operational controls such as certification and accreditation
- Agencies must ensure that sufficient funds are budgeted for and that security is sufficiently integrated into these systems

NIST National Institute of Standards and Technology

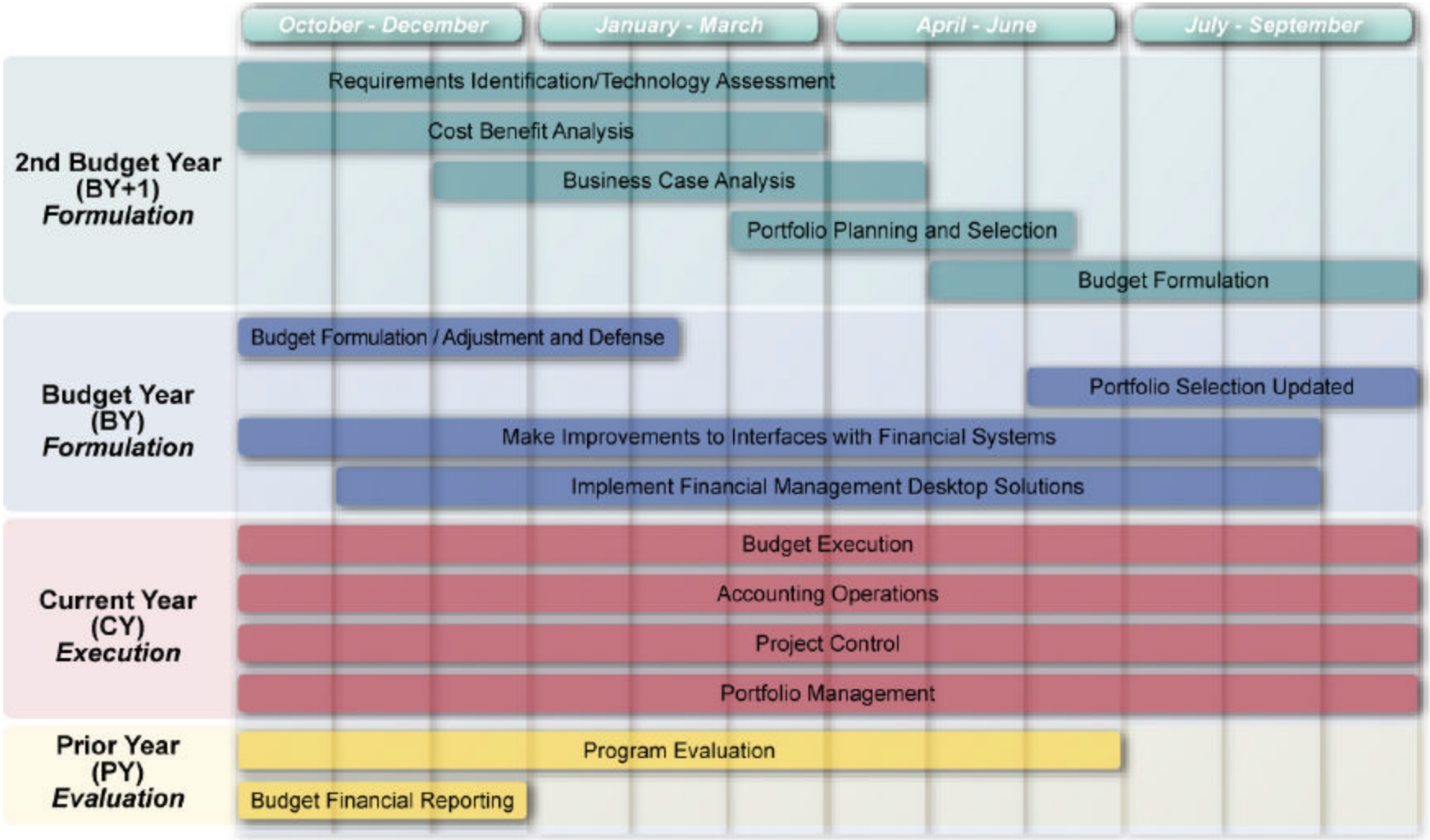
CPIC Process Timeline: High Level Picture

Prior year, current year, and budget year determinations depend on when the President receives the annual budget



CPIC Process Timeline: Department-Level Activities

With multiple events of the budget process occurring within each fiscal year, it is imperative that agencies employ disciplined CPIC processes and controls to streamline activities



Summary

- Well-articulated security requirements increase the probability of acquiring required funding
- Security funding must be spent against highest priority security assets and needs at the department level to improve department's overall risk posture
- Use of standardized methodology facilitates consistent prioritization and decision making
- Management will determine how the presented models and methodologies may be integrated into the existing processes and the thresholds for decision making
- Special emphasis on ensuring sufficient security funding for legacy systems is required since these systems transmit, process, and store sensitive information while often falling below the thresholds for the formal budgeting process
- Continually assessing the risk and prioritizing the funding is key to the implementation of cost-effective security solutions

NIST National Institute of Standards and Technology

Breakout Session

NIST National Institute of Standards and Technology

Breakout Session

Goal: The breakout session will prioritize a POA&M.

Duration: 45 minutes

Method:

- Divide into groups of 7 to 8 people
- Review the POA&M with costs, material weaknesses, and notional budget ceiling
  - Prioritize the POA&M based on provided prioritization criteria
  - Complete the POA&M prioritization matrixes

Follow up: Each group will have 4 minutes to present its outbrief:

- In the manner of an IRB briefing
- To the audience acting as the IRB

NIST National Institute of Standards and Technology

Case Study Description

The mission of the Department of Magic and Wizardry is to fulfill citizens' wishes. It has several operating divisions to support the mission with regional headquarters and offices across the nation and at international locations. The Department is a part of the E-Government initiative. The Department is using NIST SP 800-26 topic areas to categorize its corrective actions[1] and has a budget of $1 million for corrective actions.

Department of Magic and Wizardry **themes** are:

- Complying with statutory requirements
- Mitigating legacy risk and correcting weaknesses
- Achieving certification and accreditation of all systems
- Implementing national standards and guidance

[1]*Note: This is only an example for the purpose of this exercise. This case study is not real.*

Breakout Session

The breakout session will prioritize the POA&M using criteria developed from:

- Themes
- Rank ordering NIST SP 800-26 topic area corrective actions in relationship to themes
- Rank ordering system sensitivity in relationship to themes
- Prioritizing Department-level and System-level corrective actions
- Creating a joint, updateable plan for prioritized corrective action implementation in mitigating risks

A Corrective Action Prioritization Cookbook

Department-Level Prioritization

- Step 1 – Rank order NIST 800-26 topic areas using high, medium, and basic labels
- Step 2 – Input data from POA&M, which lists NIST 800-26 topic areas
- Step 3 – Compute corrective action impact for each topic area
- Step 4 – Determine great, average, and low categories of corrective action impact
- Step 5 –Apply topic area rankings (Step 1) to corrective action impact categories (Step 4) and enter into 3x3 matrix

System-Level Prioritization

- Step 6 – Rank order sensitivity of systems using high, medium, and basic labels
- Step 7 – Input POA&M system data, compute corrective action impact, and sort order of corrective action impact
- Step 8 – Determine great, average, and low categories of corrective action impact
- Step 9 – Apply system rankings (Step 6) to corrective action impact (Step 8) and enter into 3x3 matrix

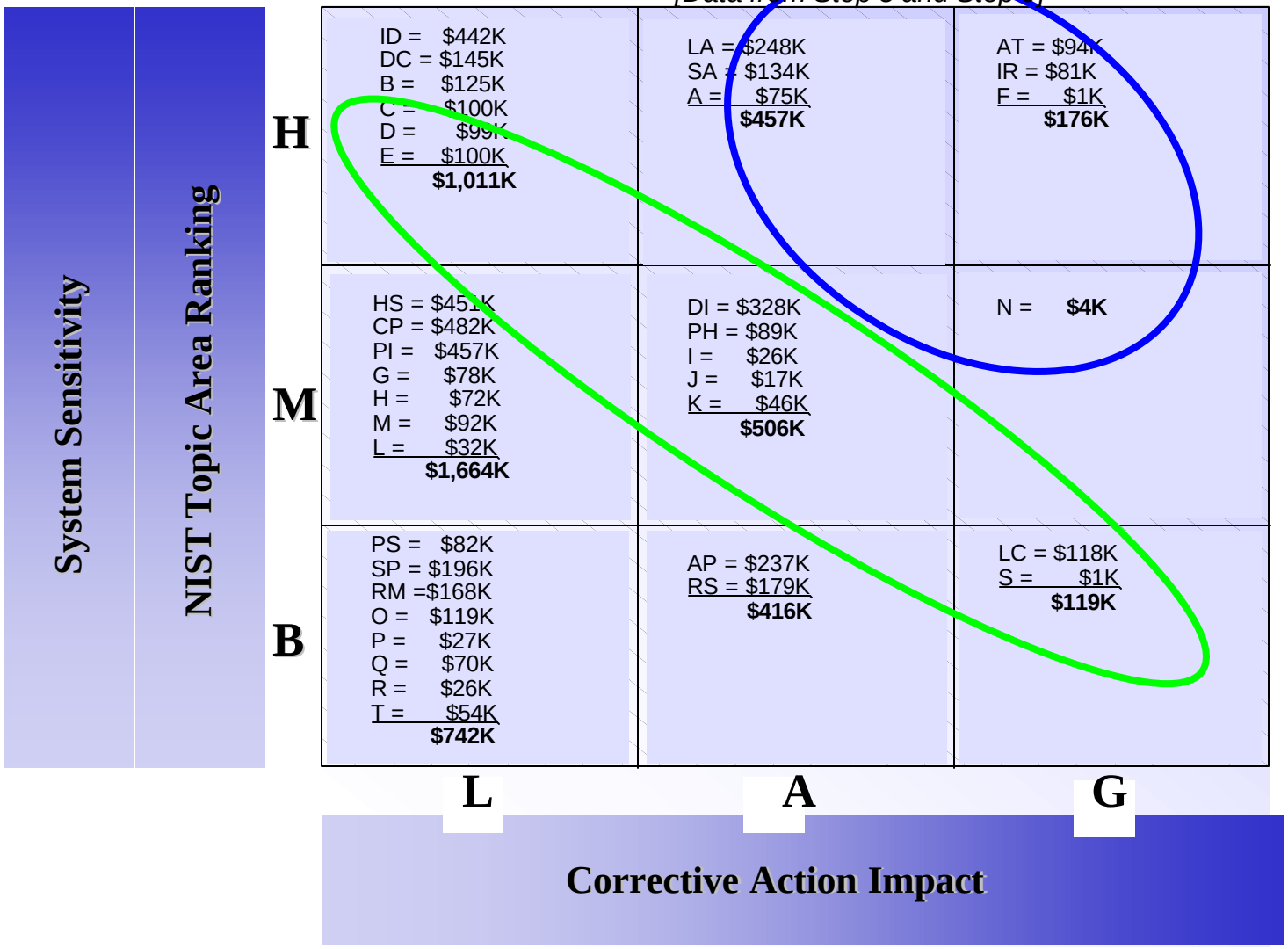
Joint Prioritization

- Step 10 – Overlay Department and System matrixes (Steps 5 and 9)
- Step 11 – Implement matrix from upper-right to lower-left within security budget allocations

NIST National Institute of Standards and Technology

Worksheet Example Z

Step 10: *Corrective Action Prioritization*
[Data from Step 5 and Step 9]



Combine matrixes from Worksheets U and X

Legend:

H – *High*
M – *Medium*
B – *Basic*

G – *Great*
A – *Average*
L – *Low*

Corrective Action Prioritization – Step 1

Department-Level Corrective Action Prioritization

Step 1 – **Topic Area Prioritization**

Department executives and stakeholders should rank the 17 NIST topic areas in order of importance using **H** for high, **M** for medium, and **B** for basic

Categorize the following list while referencing the themes:

Identifier		Identifier	
__ (RM)	Risk Management	__ (DI)	Data Integrity
__ (RS)	Review of Security Controls	__ (DC)	Documentation
__ (LC)	Life Cycle	__ (CP)	Contingency Planning
__ (AP)	Authorize Processing	__ (IR)	Incident Response Capability
__ (SP)	System Security Plan	__ (ID)	Identification and Authentication
__ (PS)	Personnel Security	__ (LA)	Logical Access Controls
__ (PH)	Physical Security	__ (AT)	Audit Trails
__ (HS)	Hardware and Systems Software Maintenance	__ (SA)	Security Awareness, Training, and Education
__ (PI)	Production, Input/ Output Controls		

Agencies are encouraged to use this sample prioritization approach or use their own approach

Corrective Action Prioritization – Step 2

Department-Level Corrective Action Prioritization

Step 2 – Enter data from POAM into columns A through F

*Note: Figure 1 columns A through F are **complete***

	NIST SP 800-26 Topic Area (TA)	Importance Ranking	Corrective Action Compliance From POAM			Average Across Department	Security Compliance Gap %	Corrective Action Cost	Corrective Action Impact	Category
			System X	System Y	System Z					
ID	Formula=	From Step 1				(A+B+C)/3=	(100%-D)=	(POAM)=	(E/F)x100,000=	
	Column=	AA	A	B	C	D	E	F	G	H
RM	Risk Management		90%	80%	65%	78%	22%	$168,335		
RS	Review of Security Controls		75%	90%	10%	58%	42%	$179,139		
LC	Life Cycle		25%	12%	15%	17%	83%	$117,789		
AP	Authorize Processing		5%	10%	5%	7%	93%	$237,350		
SP	System Security Plan		100%	95%	90%	95%	5%	$196,143		
PS	Personnel Security		90%	90%	100%	93%	7%	$82,263		
PH	Physical Security		75%	75%	75%	75%	25%	$88,762		
PI	Production, Input/ Output Controls		25%	30%	10%	22%	78%	$457,120		
CP	Contingency Planning		15%	25%	50%	30%	70%	$482,347		
HS	Hardware and Systems Software Maintenance		25%	25%	25%	25%	75%	$450,959		
DI	Data Integrity		50%	10%	0%	20%	80%	$328,506		
DC	Documentation		75%	100%	50%	75%	25%	$144,755		
SA	Security Awareness, Training, and Education		50%	0%	100%	50%	50%	$133,898		
IR	Incident Response Capability		50%	25%	30%	35%	65%	$81,161		
ID	Identification and Authentication		50%	25%	60%	45%	55%	$441,880		
LA	Logical Access Controls		25%	10%	75%	37%	63%	$248,154		
AT	Audit Trails		0%	100%	75%	58%	42%	$94,326		

Figure 1: *Department-Level Corrective Action Impact Analysis, unsorted*

Corrective Action Prioritization – Step 3

Department-Level Corrective Action Prioritization

Step 3 – Compute the corrective action impact for each topic area, enter the data in column G of Figure 1, and sort the corrective actions in order using column G. Use the formula below:

(Column E/ Column F)x100,000 = corrective action impact = Column G

Enter importance ranking from Step 1 into Column AA

*Note: Figure 2 columns A-G are **complete***

	NIST SP 800-26 Topic Area (TA)	Importance Ranking	Corrective Action Compliance From POAM			Average Across Department	Security Compliance Gap %	Corrective Action Cost	Corrective Action Impact	Category
			System X	System Y	System Z					
ID	Formula=	From Step 1				(A+B+C)/3=	(100%-D)=	(POAM)=	(E/F)x100,000=	
	Column=	AA	A	B	C	D	E	F	G	H
IR	Incident Response Capability		50%	25%	30%	35%	65%	$81,161	0.80	G
LC	Life Cycle		25%	12%	15%	17%	83%	$117,789	0.70	G
AT	Audit Trails		0%	100%	75%	58%	42%	$94,326	0.44	G
AP	Authorize Processing		5%	10%	5%	7%	93%	$237,350	0.39	A
SA	Security Awareness, Training, and Education		50%	0%	100%	50%	50%	$133,898	0.37	A
PH	Physical Security		75%	75%	75%	75%	25%	$88,762	0.28	A
LA	Logical Access Controls		25%	10%	75%	37%	63%	$248,154	0.26	A
DI	Data Integrity		50%	10%	0%	20%	80%	$328,506	0.24	A
RS	Review of Security Controls		75%	90%	10%	58%	42%	$179,139	0.23	A
DC	Documentation		75%	100%	50%	75%	25%	$144,755	0.17	L
PI	Production, Input/ Output Controls		25%	30%	10%	22%	78%	$457,120	0.17	L
HS	Hardware and Systems Software Maintenance		25%	25%	25%	25%	75%	$450,959	0.17	L
CP	Contingency Planning		15%	25%	50%	30%	70%	$482,347	0.15	L
RM	Risk Management		90%	80%	65%	78%	22%	$168,335	0.13	L
ID	Identification and Authentication		50%	25%	60%	45%	55%	$441,880	0.12	L
PS	Personnel Security		90%	90%	100%	93%	7%	$82,263	0.08	L
SP	System Security Plan		100%	95%	90%	95%	5%	$196,143	0.03	L

Figure 2: *Department-Level Corrective Action Impact Analysis, sorted*

Corrective Action Prioritization – Step 4

Department-Level Corrective Action Prioritization

Step 4 - Determine the boundaries of the three categories – great, average, and low – from Column G (corrective action impact) of Figure 2 to facilitate prioritization of the corrective actions. The criteria for the boundaries will vary by stakeholder priority, Department goals, and other factors.

*Note: Figure 3 category boundaries were **completed** by a previous decision-making group for the purpose of this exercise and added to Figure 2, Column H*

Category	NIST SP 800-26 topic areas corrective actions from Figure 2	
Great (>.40)	•Incident Response Capability •Life Cycle	•Audit Trails
Average (.20 to .40)	•Authorize Processing •Security Awareness, Training, and Education •Physical Security	•Logical Access Controls •Data Integrity •Review of Security Controls
Low (<.20)	•Documentation •Production, Input/Output Controls •Hardware and Systems Software Maintenance •Contingency Planning	•Risk Management •Identification and Authentication •Personnel Security •System Security Plan

Figure 3: *Sample Department-Level Corrective Action Boundaries*

Corrective Action Prioritization – Step 5

Department-Level Corrective Action Prioritization

Step 5 – Apply topic area rankings (Step 1) to corrective action impact categories (Step 4) and enter into 3x3 matrix.

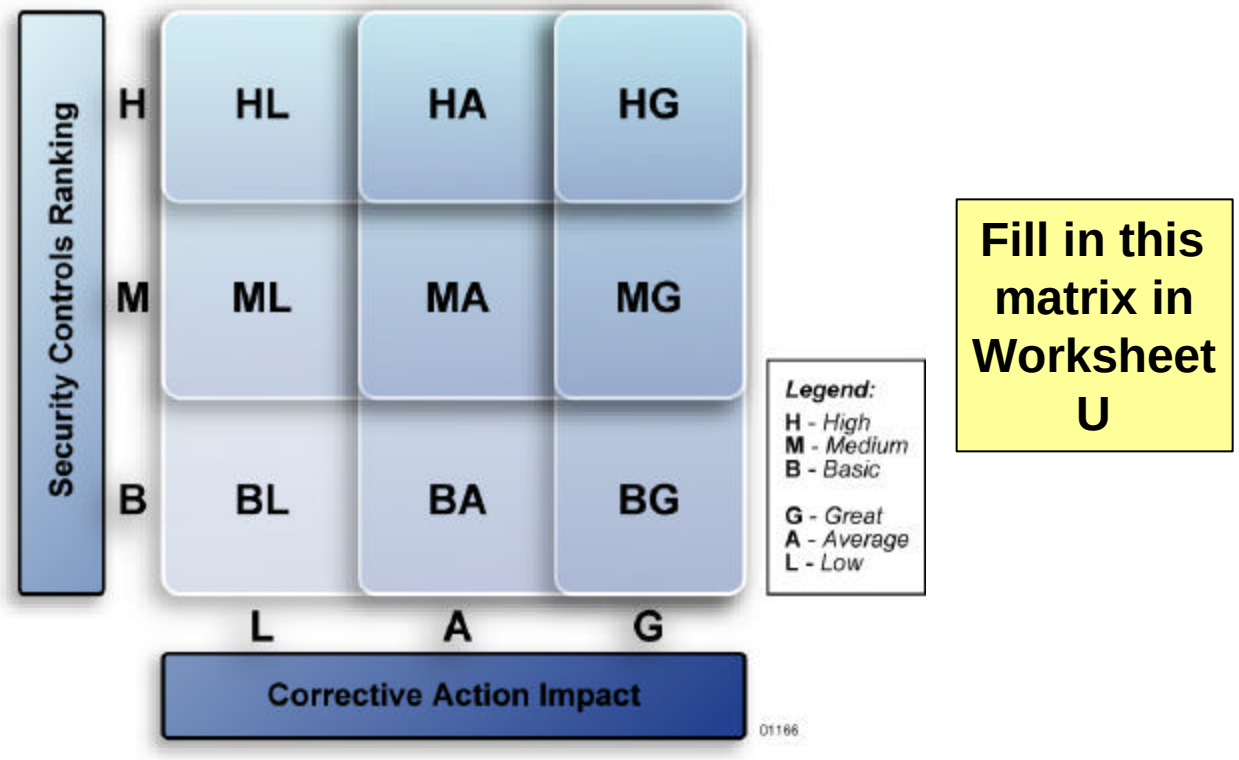


Figure 4: *Department-Level (Topic Area) Corrective Action Priority Analysis*

Corrective Action Prioritization – Step 6

System-Level Corrective Action Prioritization

Step 6 – Rank System Sensitivity

If fiscal constraints prevent the deployment of all identified corrective actions across the Department that fall within the appropriate rectangles in Figure 4, a system prioritization can be used to identify high-priority systems to target during corrective action implementation.

Department executives and stakeholders should rank the 20 systems in order of sensitivity using **H** for high, **M** for medium, and **B** for basic, similar to Step 1.

Rank order the following list while referencing the themes:

__ System A (HR)
__ System B (WzR)
__ System C (payroll)
__ System D (travel)
__ System E (e-wish)
__ System F (e-track)
__ System G (procurement)
__ System H (H-supply chain)
__ System I (Wz-supply chain)
__ System J (wish planning)
__ System K (leave/benefits)
__ System L (magic research)
__ System M (wish resources)
__ System N (wish reclamation)
__ System O (magic husbandry)
__ System P (anti-virus)
__ System Q (PKI)
__ System R (Intrusion DS)
__ System S (Wz continuing ed)
__ System T (Wz academy enrollment/grades)

Worksheet Appendix A

The following is a brief description of the systems for the Department of Magic and Wizardry

- **System A (HR)** – Human Resources system
- **System B (WzR)** – Wizard Resources system, similar to human resources system but specific to wizards. Very old legacy system.
- **System C (payroll)** – Pays employees
- **System D (travel)** – Schedules and registers travel needs
- **System E (e-wish)** – Online system for citizen wish ordering
- **System F (e-track)** – Online system for citizen wish order tracking
- **System G (procurement)** – Supports contracts management for the Department
- **System H (H-supply chain)** – Provides ordering and monitoring capability of inventories from suppliers for human requirements
- **System I (Wz-supply chain)** – Provides ordering and monitoring capability of inventories from suppliers for wizard requirements
- **System J (wish planning)** – Forecasts future impact of implementing wishes to determine potential risks
- **System K (leave/ benefits)** – Supports management of leave/ benefits for employees
- **System L (magic research)** – Provides management capability of research and grant progress/ milestones for funding
- **System M (wish resources)** – Provides management capability of national wish resources
- **System N (wish reclamation)** – Provides tracking of unused wishes and subsequent reclamation of unused wishes
- **System O (magic husbandry)** – Provides management capability of the production of magic inherent plants and animals
- **System P (anti-virus)** – Provides anti-virus software and automatic updates of anti-virus definitions to platforms
- **System Q (PKI)** – Provides Public Key Infrastructure to support encryption of data
- **System R (Intrusion DS)** – Provides intrusion detection system of potential cyber attacks
- **System S (Wz continuing ed)** – Provides management capability of wizardry continuing education requirements and credits
- **System T (Wz academy enrollment/ grades)** – Provides online enrollment to wizard academy and classes, and provides input and viewing of course grades

NIST National Institute of Standards and Technology

Corrective Action Prioritization – Step 7

System-Level Corrective Action Prioritization

Step 7 – Impact Analysis

(a) Enter data from POA&M into columns A & B and compute Column C

(b) Sort Column C, placing the largest number on the top of the list

(c) Enter the sensitivity ranking from Step 6 into Column AA

Note: Figure 5 columns A, B, and C are ***complete***

Impact Analysis					
System Name	Sensitivity Ranking	Security Compliance Gap %	Corrective Action Cost	Corrective Action Impact	Category
Formula=	From Stp 6	(POAM)=	(POAM)=	(A/B)x100,000=	
Column=	AA	A	B	C	D
N		85%	$3,800	22.37	G
S		16%	$1,456	10.99	G
F		10%	$1,000	10.00	G
J		88%	$17,431	5.05	A
I		89%	$26,387	3.37	A
K		95%	$45,566	2.08	A
A		90%	$75,000	1.20	A
P		24%	$27,248	0.88	L
H		59%	$71,860	0.82	L
C		75%	$100,000	0.75	L
E		50%	$100,000	0.50	L
G		38%	$77,954	0.49	L
B		60%	$125,000	0.48	L
D		45%	$99,000	0.45	L
M		40%	$92,423	0.43	L
T		22%	$53,830	0.41	L
R		3%	$26,442	0.11	L
O		14%	$119,060	0.12	L
Q		5%	$69,627	0.07	L
L		1%	$31,627	0.03	L

Figure 5: *System-Level Impact Analysis*

Corrective Action Prioritization – Step 8

System-Level Corrective Action Prioritization

Step 8 – Similar to Step 4, determine the boundaries of the three categories – great, average, and low – from Column C (corrective action impact) of Figure 5 to facilitate prioritization of the corrective actions. The criteria for the boundaries will vary by stakeholder priority, Department goals, and other factors.

*Note: Figure 6 category boundaries were **completed** by a previous decision-making group for the purpose of this exercise and added to Figure 5, Column D*

Category	Department System List from Figure 5	
Great (>10)	•System N •System S	•System F
Average (1 - 9)	•System J •System I	•System K •System A
Low (<1)	•System P •System H •System C •System E •System G •System B •System D	•System M •System T •System R •System O •System Q •System L

Figure 6: *Sample System-Level Corrective Action Boundaries*

Corrective Action Prioritization – Step 9

System-Level Corrective Action Prioritization

Step 9 – Apply system rankings (Step 6) to corrective action impact categories (Step 8) and enter into 3x3 matrix.

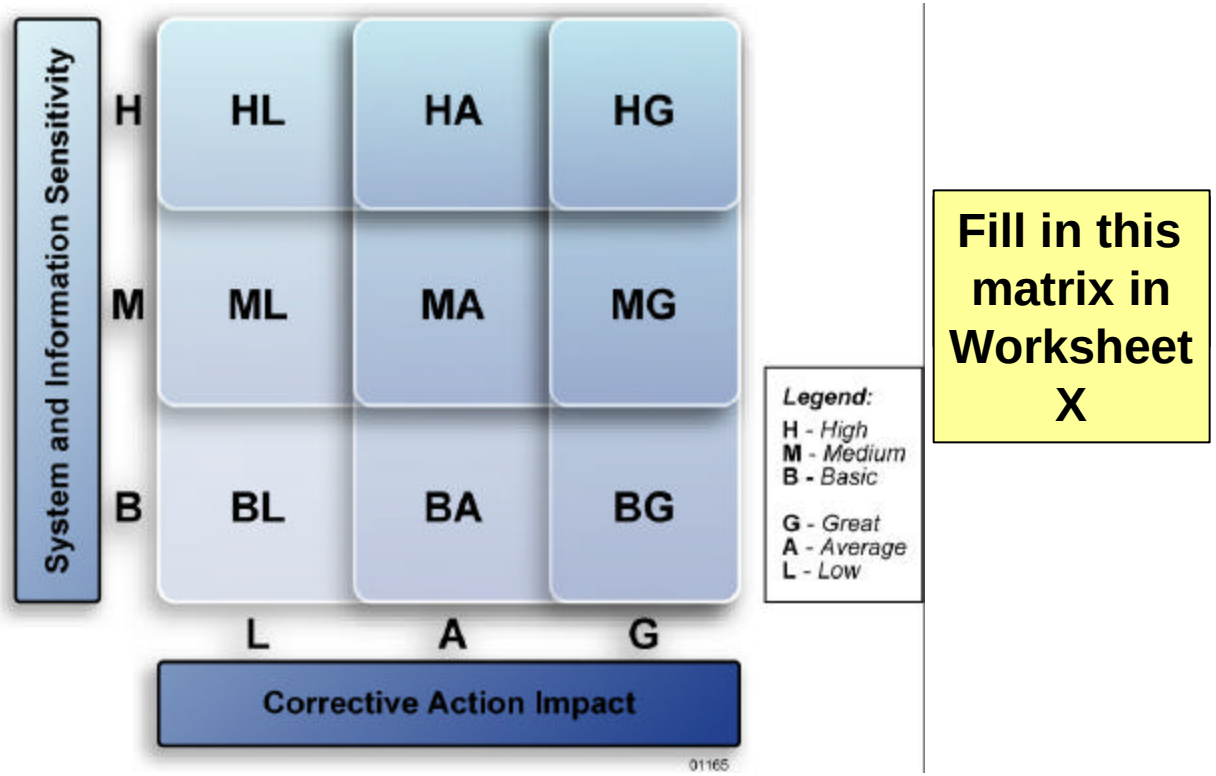


Figure 7: *System-Level Priority Analysis*

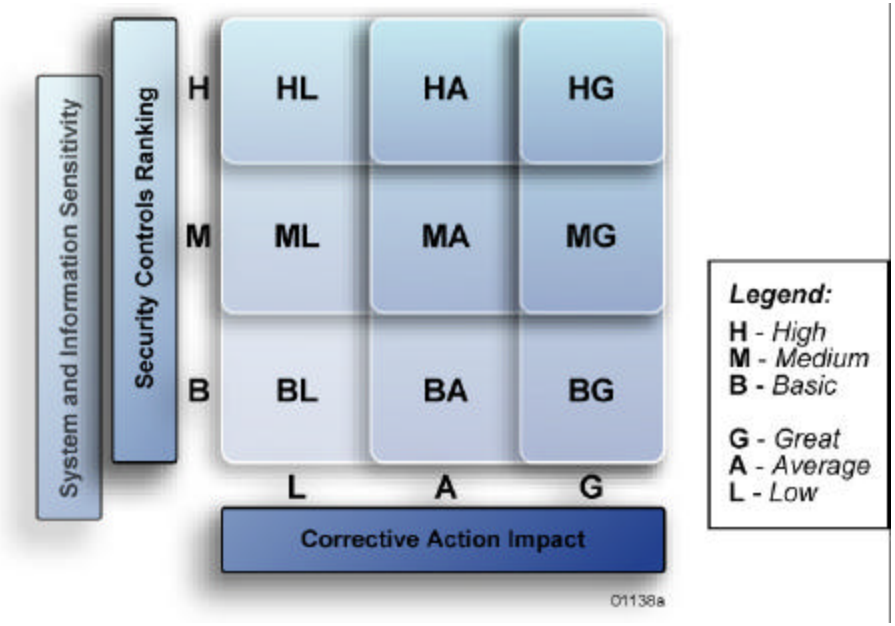
Corrective Action Prioritization – Step 10

Joint Corrective Action Prioritization

Step 10 – The remaining prioritization step combines the results to create a prioritized corrective action implementation plan.

Overlay the Department-level matrix (Figure 4) over the System-level matrix (Figure 7) into Figure 8 below.

For example, if a system was in the ML rectangle in the System-level priority analysis matrix, that system will be placed in the ML rectangle in the Department-level corrective action prioritization analysis.



Fill in this matrix in Worksheet Y

Figure 8: Corrective Action Prioritization

Corrective Action Prioritization – Step 11

Corrective Action Prioritization

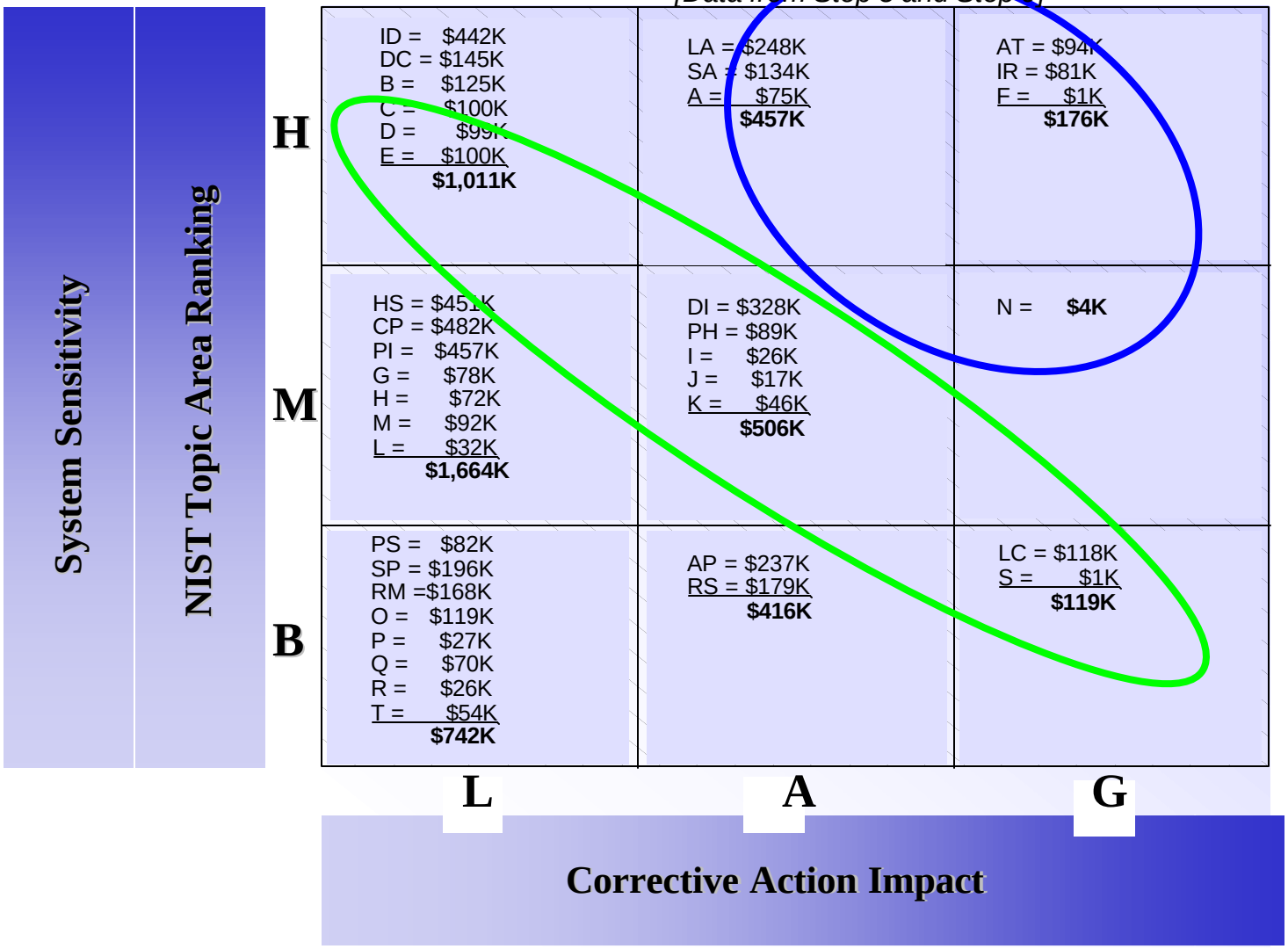
Step 11 – As Figure 8 indicates, the Department's first priority is to implement corrective actions in the HG rectangle.

- Next, the Department will implement corrective actions in either rectangle HA or MG, depending on executive priority
- The Department will continue to implement corrective actions moving from the upper-right rectangle to the lower-left rectangle
- Finally, the extent of the implementation will depend on the security budget allocations the Department receives in the path described
- Regardless of budget constraints, this model provides the Department an easily updateable roadmap for corrective action implementation that would drive the action plan for mitigating risks

NIST National Institute of Standards and Technology

Worksheet Example Z

Step 10: *Corrective Action Prioritization*
[Data from Step 5 and Step 9]



Combine matrixes from Worksheets U and X

Legend:

H – *High*
M – *Medium*
B – *Basic*

G – *Great*
A – *Average*
L – *Low*

Next Steps

- You can immediately apply to what you have learned today
- Notes of the workshop will be published in three weeks
- Integrating IT Security into Capital Planning Guidance first draft will be published in the Spring of 2004
- Please contact Joan Hash if you have any questions at joan.hash@nist.gov, 301-975-3357