THEME 3

Systems of informational security

Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

CAPITAL PLANNING AND INVESTMENT CONTROL

Increased competition for limited federal budgets and resources requires that agencies allocate available funding toward their highest-priority information security investments to afford the agency and its systems and data, the appropriate degree of security for their needs.

This goal can be achieved through a formal enterprise **capital planning and investment control** (CPIC) process designed to facilitate and control the expenditure of agency funds.

The Federal Information Security Management Act (FISMA) and other existing federal regulations charge federal agencies with integrating information security activities and the capital planning and investment control process. The practices discussed in this chapter are designed to help security practitioners and managers identify funding needs to secure systems and provide strategies for obtaining the necessary funding.

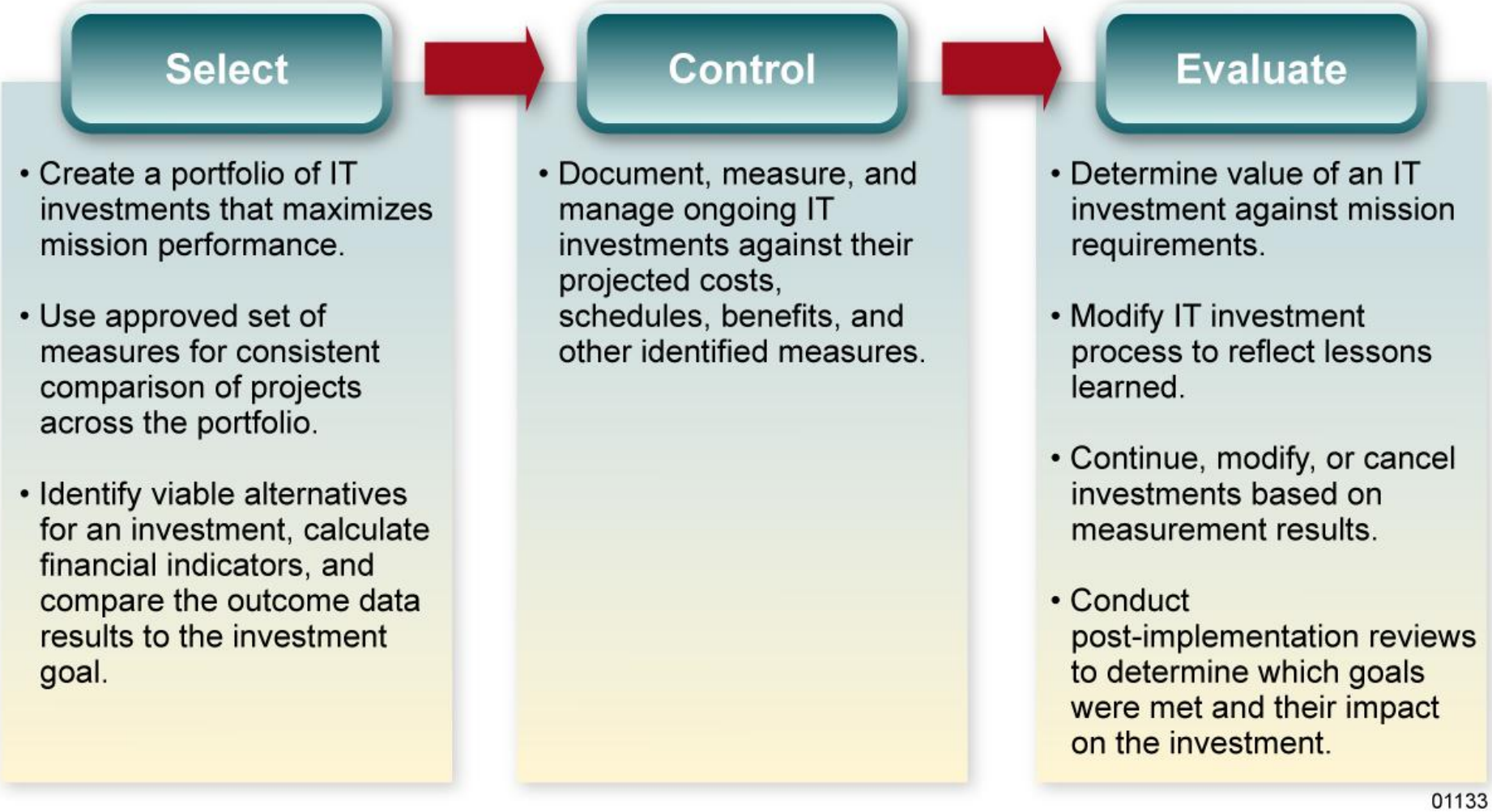
LEGISLATIVE OVERVIEW

Implementation of information security within the federal government is guided by a combination of legislation, rules and regulations, and agency-specific policies. FISMA is the overarching information security legislation for federal information systems.

Signed into law in 2002, FISMA:

- Charges the Office of Management and Budget (OMB) and NIST to develop security standards and identify tolerable security risk levels;
- Makes NIST standards compulsory for all agencies; FISMA eliminated an agency's ability to obtain waivers on NIST standards.
- NIST SP 800-53 identifies a set of minimum security controls applicable to information systems based on FIPS 199 categorization (low, moderate, high).
- OMB Circular A-11 directs agencies to complete Exhibit 300s and an Exhibit 53.
- FISMA Report is an annual report to OMB detailing the agency's security posture and any areas of weakness.35
- Plan of Action and Milestones (POA&M) documents each agency security weakness, associated corrective action, and the corrective action cost.

LEGISLATIVE OVERVIEW



LEGISLATIVE OVERVIEW

The Select phase refers to activities involved with assessing and prioritizing current and proposed IT projects based on mission needs and improvement priorities, and then creates a portfolio of IT projects to address these needs and priorities. Typical Select phase activities include screening new projects; analyzing and ranking all projects based on benefit, cost, and risk criteria; selecting a portfolio of projects; and establishing project review schedules.

The Control phase refers to activities designated to monitor the investment during its operational phase to determine whether the investment is within the cost and schedule milestones established at the beginning of the investment life cycle. Typical processes involved in the Control phase include using a set of performance measures to monitor the developmental progress for each IT project to enable early problem identification and resolution.

The Evaluate phase refers to determining the efficacy of the investment, answering the question, “Did the investment achieve the desired results and performance goals identified during the Select phase?”

INTEGRATING INFORMATION SECURITY INTO THE CPIC PROCESS

INTEGRATING INFORMATION SECURITY INTO THE CPIC PROCESS

1) **Identify the Baseline**: use information security metrics or other available data to baseline the current security posture.

2) **Identify Prioritization Requirements**: evaluate security posture against legislative and chief information officer (CIO)-articulated requirements and agency mission.

3) **Conduct Enterprise-Level Prioritization**: prioritize potential enterprise-level information security investments against the mission and the financial impact of implementing appropriate security controls.

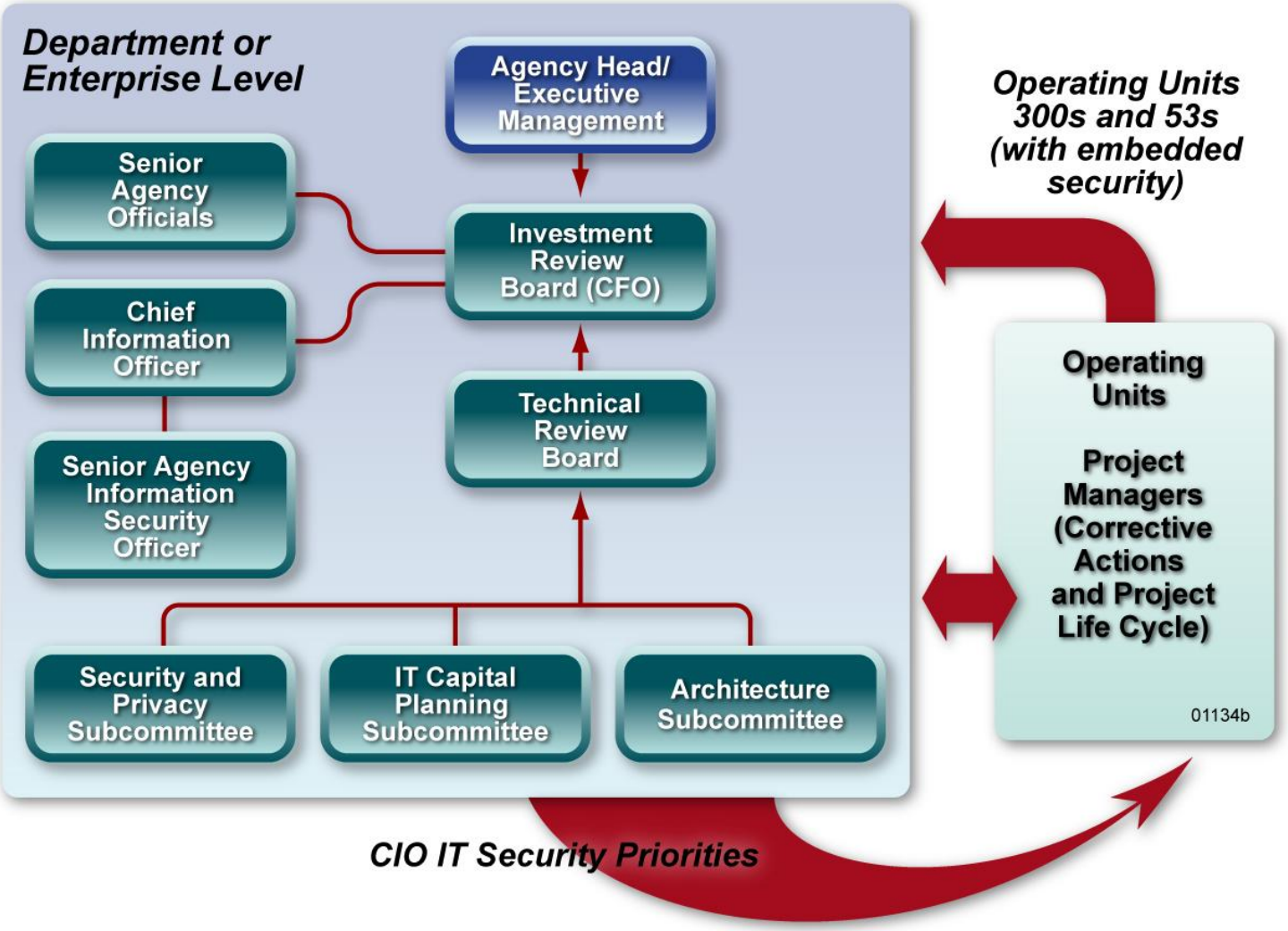
4) **Conduct System-Level Prioritization**: prioritize potential system-level corrective actions against system category and corrective action impact.

5) **Develop Supporting Materials**: for enterprise-level investments, develop concept paper, business case analysis, and Exhibit 300. For system-level investments, adjust Exhibit 300 to request additional funding to mitigate prioritized weaknesses.

6) **Implement Investment Review Board (IRB) and Portfolio Management**: prioritize agency-wide business cases against requirements and CIO priorities and determine investment portfolio.

7) **Submit Exhibit 300s, Exhibit 53, and Conduct Program Management**: ensure approved 300s become part of the agency's Exhibit 53; ensure investments are managed through their life cycle.

CAPITAL PLANNING AND INVESTMENT CONTROL ROLES AND RESPONSIBILITIES



CAPITAL PLANNING AND INVESTMENT CONTROL ROLES AND RESPONSIBILITIES

Integrating information security into the CPIC process requires input and collaboration across operating units and lines of business throughout the life cycle of technology investments.

While specific practices for investment management can differ at the operating- unit level because of varying mission scopes, the process generally mirrors the process at the departmental level. The CIO formulates and articulates information security priorities to the organization to be considered within the context of all agency investments. Priorities may be based on agency mission and executive branch guidance such as the President's Management Agenda (PMA), OMB guidance, or other external/internal priorities. Examples of security priorities include certifying and accrediting all systems or implementing public key infrastructure (PKI) throughout the enterprise. It is important to note that OMB/executive branch guidance or laws should be ranked highest among these priorities.

CAPITAL PLANNING AND INVESTMENT CONTROL ROLES AND RESPONSIBILITIES

Once operating units finalize their IT portfolios and budget requests for the budget year, they forward their requests to the agency-level decision makers. At the agency level, several committees evaluate IT portfolios from the operating units as referenced in Figure 5-3, culminating in a review by the IRB. The IRB then decides on an agency-level IT portfolio and forwards recommendations to the agency head for review. Once the agency-level IT portfolio is approved by the agency head, the necessary Exhibit 300s and Exhibit 53 are forwarded to OMB for funding consideration.

Many different stakeholders, from information security, capital planning, and executive leadership areas, have key roles and make decisions on integrating information security into the CPIC process with the ultimate goal of forming a well-balanced IT portfolio. Involvement at the enterprise and operating-unit levels throughout the process allows agencies to ensure that CPIC and information security goals and objectives are met.

CAPITAL PLANNING AND INVESTMENT CONTROL ROLES AND RESPONSIBILITIES

CPIC Steps	Identify Baseline	Identify Priority Requirements	Enterprise-Level Prioritization	System-Level Prioritization	Develop Supporting Materials	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, Architecture, and Security and Privacy Subcommittees	●	●	●	●	●	●	●
Operating Units	●		▲	▲	▲		▲

01139c

Legend: Approves = ★ Leads = ▲ Supports = ●

IDENTIFY BASELINE

The first step in integrating information security and the CPIC process is to assess the security baseline. The security baseline provides a snapshot of the agency's compliance with baseline security requirements (BLSRs) and is instrumental in identifying information security strengths and weaknesses. The result of a security baseline analysis enables agency executives to evaluate their information security posture and identify areas for improvement. Agencies can identify their baselines for enterprise-level and system-level investments. System-level investments are those security investments designed to strengthen a discrete system's security posture, such as strengthening password controls or testing a contingency plan for a particular system. Enterprise-level investments are those security investments that are ubiquitous across the agency and will improve the overall agency's security posture, such as the acquisition of an enterprise-wide firewall or intrusion detection system (IDS).

NIST SP 800-55, Security Metrics Guide for Information Technology Systems, provides guidance on developing and implementing an information security metrics program. Metrics can provide baseline compliance percentages that indicate the existence of adequate security controls, highlight current weaknesses, and identify gaps between actual and desired implementation status of information security controls.

IDENTIFY PRIORITIZATION CRITERIA

Available funding does not always allow all security needs identified in the baseline assessment to be addressed immediately. Therefore, requirements must be prioritized to address the most pressing security investment needs first. Specific prioritization criteria will vary from agency to agency depending on specific agency mission and goals and applicable legislation and regulations. Examples of information security priorities include:

- Complying with statutory requirements in Clinger-Cohen Act, FISMA, and OMB Circular A-130 guidance;
- Implementing a risk-based security program (FISMA, Executive Orders, and supporting NIST standards and guidance); for example, implementing the security controls outlined in NIST SP 800-53;
- Safeguarding national and agency mission-critical assets (Homeland Security Presidential Directives);
- Improving information security program status; and
- Completing a security certification and accreditation of all systems in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

A variety of taxonomies can be used to organize prioritization criteria, including FIPS 200 security control families or other agency-specific categories.

CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

Once agency management and stakeholders agree on the prioritization of investments, the agency can begin the prioritizing process by rank-ordering requirements against the prioritization criteria. The objective of this activity is to fund first the most critical security investment. The next layer of funding should then be applied to the next critical security investment and so forth, until the security budget is entirely expended, or priorities met, whichever comes first.

Before conducting corrective action prioritization, the agency should allocate the funding necessary to mitigate significant deficiencies and other needs that obviously require attention. These initiatives should then be removed from the prioritization process to avoid duplication of effort.

After identifying the security baseline and prioritization criteria, an agency can prioritize corrective actions at two levels:

1) **System-level prioritization**: prioritize corrective actions to address system-level security weaknesses and vulnerabilities found during the baseline assessment against the predefined prioritization criteria. This prioritization is performed at the operating unit level by system owners and program managers.
2) **Enterprise-level prioritization**: prioritize enterprise-wide security corrective actions identified during the baseline assessment based on predefined prioritization criteria. This prioritization is performed at the enterprise level by agency information security stakeholders.

CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

Inputs	Source	Data Accessibility
System-Level Information		
System categorization	System security certification and accreditation, security plan or categorization according to NIST SP 800-60 and Federal Information Processing Standard (FIPS) 199.	Security certification and accreditation, security plans, and NIST SP 800-60/NIST FIPS 199 categorizations are required for all agency systems. Required data is easily extractable from appropriate documentation.
Security compliance	System-level information security metrics or an aggregation of information security compliance percentages from, risk assessments, security certification and accreditation, or other sources, organized according to the prioritization criteria categories	Risk Assessments, and security certification and accreditation activities are required for all agencies. Required data can be easily aggregated in the required form.
Corrective action cost	System POA&M	POA&M is a required activity for all agencies. Required data can be easily aggregated in the required form.

CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

Inputs	Source	Data Accessibility
Enterprise-Level Information		
Stakeholder rankings of enterprise-wide initiatives	Prioritization sessions with agency information security stakeholders	New activity – requires collaboration among agency information security stakeholders.
Enterprise-wide initiative information security status	Enterprise-level information security metrics or an aggregation of information security compliance percentages from risk assessments, security certification and accreditation, or other sources, organized according to the prioritization criteria categories	Risk assessments and security certification and accreditation activities are required for all agencies. Required data can be easily aggregated in the required form.
Cost of implementing remaining required security controls for enterprise-wide initiatives	Program POA&M	POA&M is a required activity for all agencies. Required data can be easily aggregated in the required form.

CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

Some of the data inputs need to be manipulated further to support the corrective action prioritization process:

- **Compliance gap:** the difference between the desired and actual compliance with the security requirements. For example, if an information system has completed 80 percent of security certification and accreditation activities, that investment would have a security certification and accreditation compliance gap of 20 percent. (The actual compliance of 80 percent is subtracted from the desired compliance of 100 percent to yield a 20 percent compliance gap.) The smaller the compliance gap, the more compliant the system or enterprise control.
- **Corrective action impact:** the ratio of compliance gap to corrective action cost. The corrective action impact is calculated by dividing the compliance gap percentage by the cost to implement the corresponding corrective action(s). This ratio provides a proportion of result to cost. The higher the impact proportion, the more "bang for the buck" the corrective action will provide. The resulting proportion is multiplied by 100,000 to facilitate further calculations.

$$\left(\frac{\text{Corrective Action Security Compliance Gap \%}}{\text{Corrective Action Cost}}\right) \times 100{,}000$$

01529

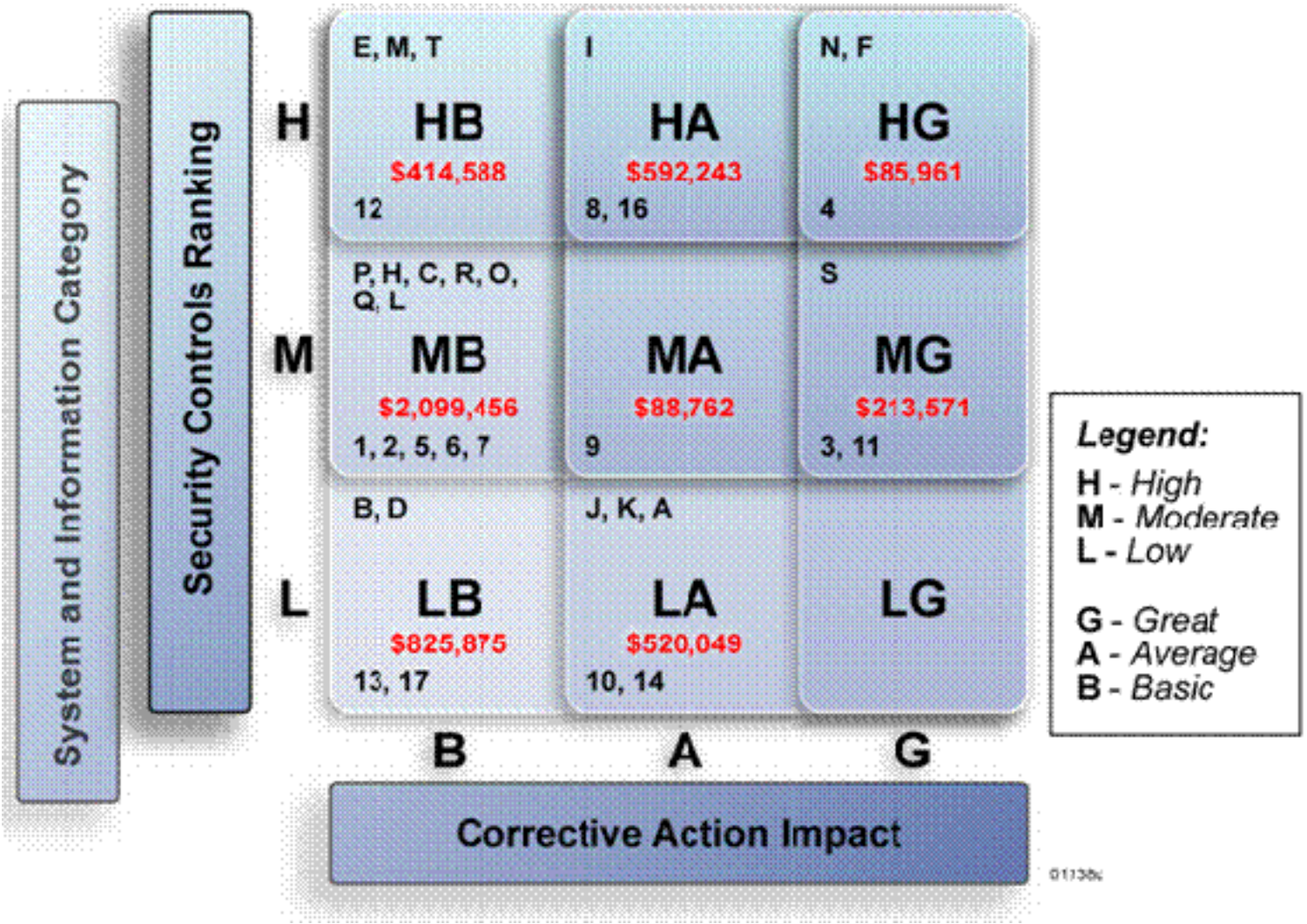
CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

After assembling process inputs, conduct the following four steps to complete the prioritization process:

1) Rank-order prioritized corrective action categories according to selected prioritization criteria in order of importance to the agency;
2) Rank-order agency systems according to system category;
3) Calculate the security compliance gaps at the enterprise and investment levels; and
4) Calculate the corrective action impact at the enterprise and investment levels.

Both enterprise- and system-level prioritization should be performed and then overlapped to ensure that appropriate agency priorities receive funding commensurate with their risk levels. Prioritization may be facilitated using a spreadsheet or a more sophisticated automation tool. Visualization of the prioritization may be used to facilitate the decision-making process.

CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION



CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

The dollar figures in figure represent the total cost to implement all corrective actions within that cell. For example, looking at cell HG, it would cost the agency $85,961 to implement corrective actions for systems “N” and “F” and topic area “4.” After plotting all of its systems, the agency should perform executive validation of the placement of the various systems to ensure that stakeholders’ priorities are met.

Organization information security stakeholders should review the prioritization results to ensure that the prioritization is appropriate and given the opportunity to reprioritize their inputs if the results of the process are found to be unsatisfactory. Assuming the agency stakeholders agree that all prioritized corrective actions are appropriate, as displayed in Figure 5-6, the analysis can proceed accordingly. As indicated by the axes, the implementation of corrective actions should begin with cell HG and proceed diagonally down to cell LB to ensure that the agency implements the most cost-effective, high-impact corrective actions.

CONDUCT SYSTEM- AND ENTERPRISE-LEVEL PRIORITIZATION

To continue with the example, assume the notional agency has a $2,000,000 budget to implement information security corrective actions. As figure demonstrates, adding the three highest priority cells together (HG, HA, and MG) brings a total of $891,775, which is nearly half of the corrective action budget. The agency would then move to the next tier of prioritization, or cells HB, MA, and LG. Totaling these cells yields a total of $503,350, which combined with the previous total from HG, HA, and MG, yields a running total of $1,395,125. With $604,875 remaining in the corrective action budget, the agency would proceed with prioritization into cells MB and LA. Totaling those two cells yields $2,619,505.

Clearly, this total exceeds the remaining corrective action budget, so stakeholders will have to decide on how to allocate the remaining dollars. Should stakeholders determine that the corrective action impact order (G, A, B) is the driving factor, the corrective actions in cell LA will be implemented. If the stakeholders determine that the system and security control category (H, M, L) is the driving factor, the corrective actions from cell MB will be implemented until the remaining $604,875 is expended.

DEVELOP SUPPORTING MATERIALS

Once prioritizing against requirements is completed, operating units are poised to select their investments for the budget year and begin the process of requesting funding from OMB for the next year to implement the corrective actions and security controls.

The Exhibit 300 is the capture mechanism for all of the analyses and activities required for full internal review (e.g., IRB, CIO). More importantly, Exhibit 300 is the document that OMB uses to assess investments and ultimately make funding decisions, and therefore should be leveraged by agencies to clearly demonstrate the need for life cycle and annual funding requests. The Exhibit 300 is completed for new IT investments and is resubmitted annually for mixed life-cycle and steady-state investments.

Operating units should evaluate their prioritized corrective actions and security controls identified during the prioritization process and determine whether the outputs need to be incorporated into an existing investment's Exhibit 300 or whether they will need to create an independent Exhibit 300 for a new investment.

RB AND PORTFOLIO MANAGEMENT

The IRB reviews and selects investments for the agency portfolio based on the Exhibit 300s forwarded by the operating units. Like the prioritization that occurs at the operating-unit level, the IRB typically uses strategic selection criteria to rank-order the investment pool and usually makes decisions based on agency mission and goals, not just on cost. While security is not the typical driving force behind portfolio management, it is a critical element in the investment strategy because it serves as a qualifier for receiving funding and as a business enabler for those functions which support the agency's mission. After prioritizing and approving select Exhibit 300s, the IRB creates an investment portfolio request for review by OMB.

THANKS FOR ATTENTION