Enterprise Architecture and IT Governance
A Risk-Based Approach

by
James R. Getter
United Stares Capitol Police
jim_getter@cap-police.senate.gov

Abstract

The USCP had enormous challenges with its IT Program and support to the internal and external stakeholders of the Department, because of a fragile IT infrastructure. The IT Program was not able to provide the basic assistance to the end-user, adequate reporting to middle and senior management, and lacked training of IT and end-user staff, to venture into the rapidly changing technologies in network management, operating systems, data security, risk management, and systems integration, as well as, the need for innovative data management. The need for these services were exacerbated by increased demands on the IT Services Group and budgetary pressures restricting the resources available to accomplish the mission until an IT Governance structure was adopted and the development and implementation of an Enterprise Architecture with corresponding Risk Management Planning was undertaken.

In order to overcome the inadequacies in the IT program, USCP established several ambitious goals for updating its Strategic Planning Process, developing and implementing an Enterprise Architecture and Risk Management Plan, setting up an IT Governance structure to provide the necessary standards and guidance, as well as the relevance, accessibility, and timeliness of its Information Technology support. The Office of Information Systems, set out to transforming itself into a performance-based organization. The envisioned "to be" system architecture helped USCP focus scarce assets on prioritized application and infrastructure projects to directly support USCP mission requirements, both Operational and Administrative. Additionally an IT Security Program was implemented to include compliance with FISMA [7]; established a Configuration and Change Management Board; instituted Earned Value Management techniques into project management activities, during the system acquisition process.

1. Introduction

The United States Capitol Police (USCP) has a unique mission and operational environment. As an organization of the Legislative Branch of Government, USCP is a law enforcement agency, as well as, a protective agency. Created by Congress in 1828 to secure the United States Capitol Building, the USCP mission has evolved into a dual role as a law enforcement agency serving all the people who work and visit Capitol Hill, and a protection agency charged with providing security for Congressional members.

Background

The United States Capitol Police (USCP) conducted an assessment of its then current and future information technology (IT) requirements in calendar year 2000. The assessment provided a comprehensive analysis of current and future requirements related to data and information, defined the functions of applications to meet functional requirements, developed an overall system's design using the results of the functional requirements analysis, and identified risks.

The "as-is" system had a custom-built business process applications, (i.e., the Capitol Police System (CPS)) and had not kept pace with changing business needs; and, the base infrastructure system was not robust enough to support the necessary communications and interoperability requirements. Additionally, internal and external customers identified areas in the "as-is" architecture needing improvement through business process re-engineering. Bottom line, the USCP identified the need to develop a new and comprehensive enterprise architecture which was presented to the Department for consideration with the following assumptions: The "to-be" enterprise architecture must be far reaching enough to achieve the information

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

1530-1605/07 $20.00 © 2007 IEEE

technology vision outlined in the USCP Strategic Plan. Care must be taken to ensure that what is put into place was robust enough to last for at least the length of the strategic plan, (i.e., five years 2004 – 2008). Implementing a shortsighted architecture with limited growth potential would provide for unreasonable risk by the internal and external stakeholders. Additional extensive enhancements and investments were necessary in the Network infrastructure to keep pace with the future growth of the organization.

The risk of successfully implementing this course of action was highly dependent upon the availability of stakeholders support. Without this support, the risk of not achieving the goals of the Strategic Plan and supporting enterprise architecture were greatly increased. With appropriate leadership support, the risk could be significantly reduced. USCP leadership, with its internal and external stakeholders, stepped up to the plate to make the IT Modernization effort a reality, and insisted upon unqualified support from all sectors of the USCP. It required commitment of the organization's most critical resources – manpower, time, and dollars.

2. Enterprise Framework

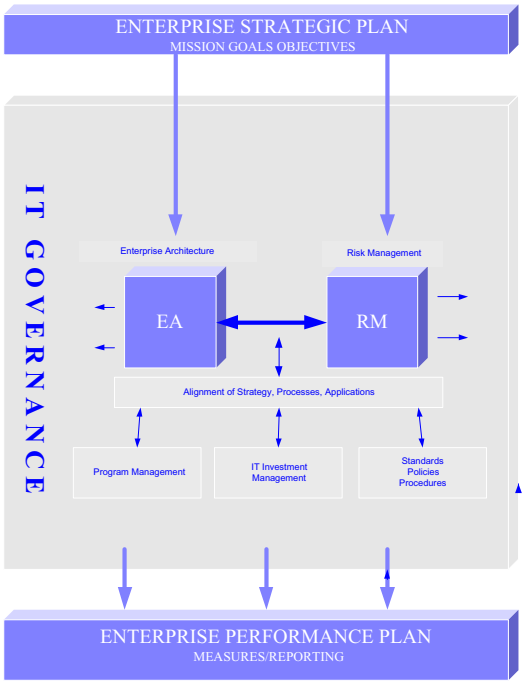


Figure 1. Enterprise framework

2.1. Strategic Plan

Figure 1, illustrates the related processes that are part of USCP's Enterprise Framework begins with the Strategic Plan, the roadmap for the activities USCP performs and the resources the Department requests each year. The Strategic Plan lays out the mission and what it is to be accomplished. The Plan also quantifies what success looks like for these accomplishments. Although The Strategic Plan is a five - year running view, there may be and are events and other factors that impact USCP's mission and activities, sometimes in a relatively sudden fashion. The Strategic Plan is a living document that is a current description of its mission, goals, and objectives and for this reason is refreshed annually.

2.2. Risk Management Plan

Risk Management Planning process identifies, analyzes, plans, tracks, and monitors those conditions considered risks, which may have a negative or positive impact on the program. In the context of the Enterprise Framework, the Risk Management process encompassed the whole enterprise. The IT Governance and associated processes are considered by the Department as risk mitigating processes. With the Governance structure and associated activities outlined in this paper, the risk for a successful Enterprise Architecture implementation was greatly decreased.

2.3. Enterprise Architecture

The EA gives the Department the ability to ensure that its modernization projects are coordinated across the entire USCP enterprise, that they produce an integrated and unified set of systems, and that they are scoped to eliminate duplication of effort. The EA is explicitly driven by USCP's business needs and priorities, and informs and guides the USCP on projects underway and provides a framework of future projects.

3.0. IT Governance

3.1. Alignment of Strategy, Processes, and Applications is a continuing activity that uses the Strategic Plan, mission, goals, and objectives; the EA interrelated architectural views of business functions and processes, data view identifying major types of information, infrastructure view identifying hardware-software, and network technologies required to

manage business applications throughout the enterprise; the Risk Management Plan; Program Management structure; Investment Management; and Standards, Policies, and Procedures.

3.1.1. Program Management

Program Management is the process of managing the program and projects as well as stakeholders expectations, requirements, and objectives. Failure to manage provides untenable risk and most likely has a negative effect on service delivery to the Department. This module of the framework covers the entire life cycle with respect to Initiating, Planning, Controlling, Executing, and Closing Processes based on Project Management Body of Knowledge [1]. This module includes governance structure such as BSMO, IRB, and OIS; processes such as communications and transition planning; and Service Level Agreements with the Department's internal and external customer base.

3.1.2 ITIM

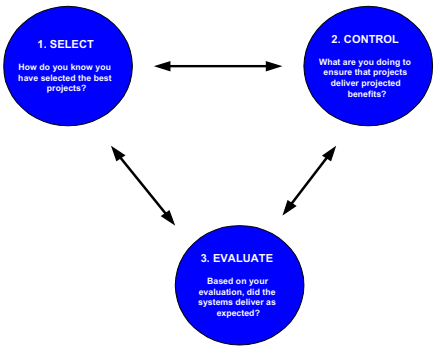


Figure 2. Investment management process

Investment Management is the systematic approach to managing the risks and returns associated with the IT Investment Program, figure 3. The process provides for the continuous selection, control, life-cycle management and evaluation of investments focused on achieving a desired business outcome. Each project is closely managed throughout its life-cycle to ensure that the investment achieves or exceeds the planned benefits proposed. This is accomplished through monitoring of cost, schedule, technical and performance measures while ensuring the project remains in alignment with organization and business goals.

3.1.3. Standards, Policies, Procedures

The Department has produced a set of Policies and Procedures which have been codified through the Department's General orders documentation process. The standards, policies, and procedures are a result of discussions, interviews, and documents reviews of "best practices", "best-in-class" organizations, and guidance from the General Accountability Office. Selected Software Engineering Standards from IEEE, [6] and CMMI [3] were incorporated into the USCP IT Standards for acquisition and systems development.

3.1.4. The Enterprise Performance Plan

provides a measurement system, focusing attention on the Enterprise Strategic Plan's goals and objectives. It assists in measuring productivity and effectiveness of a program. The plan is reviewed on a quarterly basis, and demonstrates how resources are being used, communicates successes, and provides a heads-up for those tasks not meeting the goal, generates information for senior management to assist them in the program management for the Department, and tracks overall progress of the Department toward the strategic plan road-map of where the Department wants to be.

4. Enterprise Strategic Plan

Figure 3. Enterprise strategic plan

The Department's Strategic Plan describes the mission, vision, goals, and objectives for the Departments Bureaus and Offices. The current five-year plan had a major revision in 2004 and is in effect through 2008, with annual updates, [12] &[15]. USCP's environmental assessment included analysis of factors external and internal to USCP, as well as an analysis of opportunities. In developing and maintaining the Strategic Plan, USCP draws on many existing relationships and communication forums with Congressional committee staff

members, Sergeants at Arms Office's for the House and the Senate, and the Architect of the Capitol, to name a few. In addition to on-going discussions, USCP conducted formal discussions with key Congressional staff, the Capitol Police Board, and the US General Accountability Office (GAO). Several themes emerged from these discussions with stakeholders regarding the USCP strategic plan framework and direction.

Stakeholders noted the importance of communications in all aspects of the Department's work. Whether it is communication around a specific emergency incident, regular discussions with congressional stakeholders, or outreach awareness and education programs, structured deliberate communications repeatedly came up as a critical factor in USCP success; balancing openness and accessibility with security; and alignment of the Strategic Plan and its Information Technology support.

The major USCP business processes comprise Law Enforcement (LE) and Administrative processes. The administrative business processes are related to budget, financial, acquisition, asset, human resources, logistics, records, and information management. The LE processes relate to Operations matters and the Department's mission. Information Technology transcends both Administrative and LE processes.

Figure 3, illustrates the USCP Strategic Plan framework. The top of the pyramid includes the Department's various stakeholders: Members of Congress, staff, and the public. We must serve these stakeholders in order to achieve our mission. Serving and satisfying our stakeholders means that we must excel at our operational work. This operational work is captured in three strategic goals: "Assess the Threat," "Prevent," and "Respond." The fourth strategic goal "Support the Mission" addresses how we manage our resources and people to support our operational goals. Within each of the strategic goals, the Department has created specific objectives that address the scope of its work a running five-year period. The objectives are listed under each strategic goal.

5. Risk Management Framework

Figure 3. Risk management framework

USCP has developed a Risk Management Planning Framework [20] comprising multiple processes within the Enterprise Framework (figure 3) to identify, analyze, plan, monitor, control and manage risk. This process is codified in the USCP Polices and Procedures Handbook.

USCP utilized both qualitative and quantitative risk assessments as part of its Risk Management Planning process. In developing its Risk Management Plan for the Enterprise Architecture, USCP used a risk model to identify, analyze, plan, monitor, and control the Program/Project Risks.

Risk Identification was accomplished by subject matter experts listing all potential risks (uncertain event or condition). The original list of potential risks was reduced by 44 %, or 29 risks. Twenty-nine risks considered and vetted thru the process were determined to be inconsequential largely because of the IT Governance Structure currently in place. Twenty-one identified and categorized risks were forwarded for further qualitative risk analysis, if necessary a quantitative risk analysis will be accomplished on selected risks.

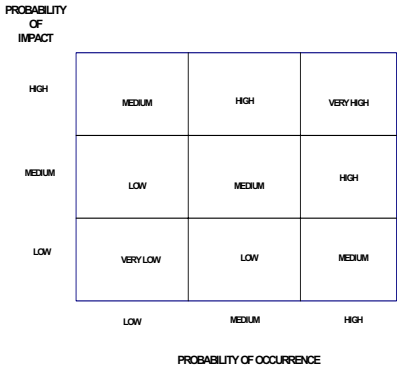
General risk categories used by USCP for risk categorization are listed in the following table 1.

Table 1. Risk categories

CATEGORY	EXAMPLE
Quality or Performance	Platforms, integration
Program Management	PM qualified
Organization	Structure, longevity
External Factors	Stakeholder satisfaction
Internal Factors	Training support, policies
Technical	Functional or Interface complexity, unproven technology

USCP uses a risk matrix detailing probability in percent, impact by category, and a qualitative risk prioritization of Low, Medium, and High, table 2.

Table 2. Risk assessment severity level matrix



Each risk on the risk list was evaluated as to its probability of occurrence and its severity of impact, if it in fact did occur, using the risk matrix in Table 2. The risks along with their cause and effect were then arranged in numeric order, highest to lowest. BSMO then reviewed each risk identified, its cause and effect, and made a determination as to whether the risk would be accepted, mitigated, or transferred. (Acceptance means doing nothing, mitigated is to take some sort of action that lessons the impact, and transference means that the risk has been transferred to someone else (ie. We might subcontract software development, if we had no skilled software engineers available)). Risks were numbered consecutively, and as is the case with the enterprise architecture program the post-script for the risk number is EA. Risks that have been identified are less likely to occur because they have changed from uncertain events or conditions to known events or conditions [10].

Risk Identification and assessment procedures used for Qualitative Risk Analysis were developed using existing documentation, information gathering techniques such as brainstorming, Delphi techniques, interviewing, root cause analysis, SWOT, checklist analysis, assumptions analysis, and diagramming techniques. USCP risk assessment procedures for Quantitative Risk Analysis utilizes interviewing, probability distributions, subject matter experts, sensitivity analysis, expected monetary value, decision tree analyses and modeling, and simulation (ie. Monte Carlo techniques) The USCP uses these assessment procedures during the course of developing, maintaining, and managing its EA risk analysis.

Additional information about each risk is collected to include: risk description, risk owner, last update, risk status, risk exposure, mitigation strategy, cost of mitigation strategy, WBS accounting code, and risk trigger

Monitor and controlling the selected risks starts with the selection of a risk mitigation strategy, developed and an associated cost analysis produced for the mitigation task. The risks were then ranked for exposure and placed in the USCP Risk Tracking System (RTS) to track the risk status for each risk identified (table 3). The tracking status of each EA risk is reported to BSMO on a monthly basis, unless of course, there are compelling reasons for increased status reporting. The USCP tracking system is fielded in MS Access 2000 and is part of the official documentation archived for program planning, project history, and lessons learned, for future reference of program/project activities, as are all program and project activities conducted by the USCP.

The Risk Management Plan is integrated with the Enterprise Architecture, IT Security Plan, Continuity of Operations Plan, the Disaster Recovery Plan, Alternate Computer Facility Operations Plan, and Fiscal Year (FY) Budget formulation planning, for current and out year analysis and input as necessary.

Table 3. Risk rating

RISK ID	RISK NAME	GOVERNANCE ACTIVITY	RISK RATING
EA-GOV-001	Communications Planning	Program Management	Low
EA-GOV-002	Organizational Commitment	Investment Review Board	Low
EA-GOV-003	Risk Mgmt Plan Maintenance	Risk Management	Low
EA-GOV-004	Aligning IT Applications	Aligning of Strategies, Processes, & Applications	Low
EA-GOV-005	Change Control Management	Configuration & Cgange Control Mgmt	Low
EA-GOV-006	Project Management	Program Management	Low
EA-SEC-007	IT Security Program	Standards, Policies, & Procedures	Medium
EA-TRN-008	End-user Trng	Standards, Policies, & Procedures	Low
EA-HRM-	Dependence on Key Personnel	Human Capitol Planning	Medium

009			
EA-NET-010	Network Monitoring	Program Management	Medium
EA-GOV-011	Systems Administration	Standards, Policies, & Procedures	Medium
EA-POL-012	Standardized Platform	Capital Planning & Investment Control	Low
EA-SEC-013	Information Leakage	Security Program	Medium
EA-SEC-014	End-User Computing	Security Program	Low
EA-GOV-015	Service Level Agreement	SLA	Low
EA-GOV-016	IRB Briefing Support	Investment Review Board	Medium
EA-INF-017	Integrating data among systems	Standards, Policies, & Procrdures	Low
EA-POL-018	Documentation Management	Standards, Policies, & Procedures	Low
EA-POL-019	Systems Acceptance	Standards, Policies & Procedures	Low
EA-GOV-020	Rqmnts Fully Understood	Business Case	Low
EA-GOV-021	Stakeholder buy-in	Communications Planning	Medium

6. Enterprise Architecture

To achieve the Department's vision, the USCP initiated a business process re-engineering and Enterprise Architecture (EA) effort. The EA process that the USCP/BSMO is using is based on work done by the US Treasury (*TSIAF 1997*) and advice given in "*The CIO Practical Guide to Enterprise Architecture*", as well as GAO guidance documents including "*A Framework for Assessing and Improving Enterprise Architecture Managemen*t" (Version 1.1, 2003). The USCP follows the GAO Enterprise Architecture Management Maturity Framework (*EAMMF*) for developing and revising its EA.

The USCP Enterprise Architecture is comprised of separately defined but interrelated architectural views. The business view representing the functions and processes that support the operations and administrative functions, and the factors that could cause the business to change; the data view identifies major types of information needed to support the business functions. It identifies and defines the information model, data sets, metadata repositories, their relationships to the business functions and application systems; the application view identifies and describes applications, as well as their relationship to business processes and other applications systems. Major influences include technologies employed and interface requirements; the infrastructure view identifies and describes the hardware, software, and communications network technologies required to manage business applications throughout the enterprise and a performance view

The Enterprise Architecture captures the business and technology components that support the business and operations objectives of the USCP. The document set encompasses the USCP organization, from the Strategic Plan, Mission Statement, and its Goals and Objectives, to business functions and business direction through to the technology needed to support, implement and maintain USCP IT systems. The EA has been adopted using a methodology adopted and adapted by the USCP Business Modernization Office (BSMO).

Based on the Information Technology Assessment [11], updating of the USCP Strategic Plan (USCP Strategic Plan, 2004-2008), goals and objectives, meetings with stakeholders, advice and guidance from the General Accountability Office (GAO Reviews), and Congressional guidance through the budget process, USCP developed a target "to-be" architecture (EA, v 4.0) vision that focuses on delivering integrated, streamlined, business and operations services to its cliental. USCP envisions that its "to-be" architecture will provide accurate and timely access to data and information for all levels of the organization.

The performance view accomplishes the answering of the following questions using artifacts (ie models) and the inter-relationship and correlation of these artifacts, (Are all IT systems supporting business processes? Are the IT goals in line with the Department's strategy? Are the business processes supporting the Department's strategy? If an IT system was changed, what business process would it effect?). Five artifacts were used in the analysis: Organization Decomposition, USCP Strategic Goals and Objectives, IT Goals and Objectives, Major Business Functions and Processes, and existing IT Systems. The IT Governance process identifies major USCP components which support best practices related to performance and program management activities. Clearly USCP top leadership support commitment to change, as identified in the transition plan for the modernization effort; there is continual involvement from senior and mid-level managers, through the Strategic and Performance Planning structure; stakeholders (internal and external) are communicated with periodically, some daily, and feedback through surveys and

data calls is requested to provide for better support and services from the IT organization.

In EA version 4.0 [13], now being revised, estimated to be completed September 2006, the integration of security planning, risk and performance management is a major focus. All federal systems have some level of sensitivity and require protection as part of "best practices" and the Federal Information Systems Management Act (*FISMA, 2004*). The hiring of an Information Security Officer, development and execution of the IT Security Program, promulgation of security policies, procedures, and plans, and the establishment of an IT Security Awareness and Training Program. Additionally a systematic Certification and Accreditation project for all USCP systems was instituted on a three-year cycle. For critical business areas, business process modeling [2] & [9], was completed.

EA provides a clear and comprehensive picture of the structure of an entity, organizational or functional or mission area. EA defines an organization's operations in logical (information flows) as well as technical terms (hardware & software). The EA also describes these perspectives both for the organizations current "as-is" environment and for its target "to-be" environment as well as for a transition plan for moving from the "as-is" to the "to-be" environment. The EA is used to align IT Investments with strategic objectives. The EA is used for strategic program decision making. The EA leverages the "as-is" infrastructure, provides multiple cross-functional users a standardized platform (hdwr/sftwr), and supports better connectivity, user responsiveness, provides for standardized security policies, procedures, and use of "best practices", with accountability, and has internal and external stakeholder interests built-in.

7. IT Governance and Management

IT Governance, "is the administering of IT resources by the processes of strategic planning, prioritization, decision making, and performance measurement".

The Governance structure used by USCP, was developed overtime using "best practices" through an iterative approach. BSMO focuses on the "big picture" needs, keeping the IT and Business alignment of the Enterprise Architecture and vigilant of performance measures projected vs actual measures attained for projects in development. The Investment Review Board (IRB) is made up of Bureau Chiefs and Office Directors. The IRB is the senior executive decision body which drives the Department's Strategic Plan, Enterprise Architecture, and IT Investments Management Program efforts and Risk Management Planning. The IRB recommends the preferred alternative(s) to the Chief of Police, for approval. This IT Governance structure (Figure 1), provides for risk mitigation at the enterprise level. An explanation of each entity follows:

7.1. Alignment of Strategy, Processes, and Applications

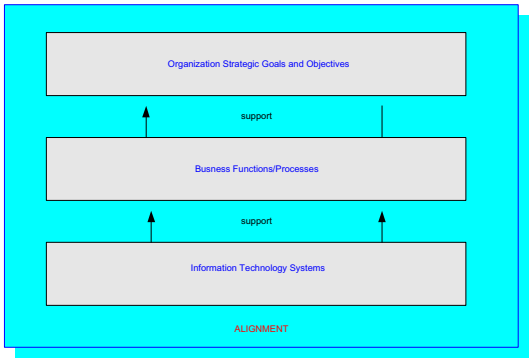


Figure 4. Alignment

Understanding the alignment between the business processes and USCP goals and objectives is critical to evaluating the value of the Department's IT applications and focus of future work efforts. When stakeholders and auditors want/need to understand the alignment between certain organizational elements, they have the ability to pull up the information quickly [17]. This is especially true for those who require strategic visibility into the organization and need to understand how a change to a business process affects the IT and/or how systems development affects business processes. This alignment compliments the USCP's Enterprise Architecture and the USCP's Strategic Plan and provides a focused view into the organization. This alignment analysis provides a textual representation of the alignment between business elements; and provides, through the use of modeling tools, the ability to follow the "business vision" through "business processes", as well as analyzing and simulating changes to the organization.

7.2. Program Management Process

7.2.1. Business Systems Modernization Office (BSMO)

USCP uses the BSMO, co-chaired by the CIO and CFO, as a working group and decision body, for promulgating policy, procedures, strategies, effecting cross-functional business needs and reports to the IRB. BSMO provides technical, functional, managerial, and planning IT support to the USCP in the development and maintenance of the Enterprise Architecture, development and implementation of near and long term Plan to include acquisition and deployment of a "target architecture" related to the enterprise. BSMO provides focus to the Enterprise as a whole, from the developing and updating of the Department Strategic Plan, the integration of the Internal Control Program (*OMB Circular A-123*) to program managing specific projects. It advises the Investment Review Board (IRB), balancing between intermediate and long-term goals and the IT Portfolio [8]. The makeup of BSMO, provides for a strong understanding of the Organization, its mission and culture, and how information technology fits in the Operations of the Department. BSMO is pro-active at building relationships with both internal and external customers, aligning IT investments to business functions, and keeping abreast of new technologies that could possible be incorporated into the Enterprise Architecture. BSMO staffing expands and contracts depending upon the number of subject matter experts and contractor support needed for a given project or program.

7.2.2. Communication Plan

The implementation of the Enterprise Architecture occurred in 2002 with the guidance of the General Accountability Office (GAO). Maintenance of the EA and the Risk Management Plan occurs through the Office of Information Systems, Planning Division with the approval of the Business Systems Modernization Office and the Investment Review Board. To ensure EA and RM implementation, operations and maintenance a success, effective communications with all stakeholders and users is critical between the US Capitol Police, system and network administrators (internal and external) and the end-users. Additionally as established in the EA Program's organization, effective communications between all stakeholders and users, including the IRB, BSMO, the Director, OIS, and all members of the Command Staff, ensures that all parties understand the EA and the RM, its purpose and what it means to the decision making process. The Communications Plan [4]outlines the coordination that will take place among all EA stakeholders to properly communicate events as they unfold. The dissemination of accurate, reliable, and timely information related to the EA and potential risks will determine the outcome of a successful EA. Proper communications begins by knowing the structure of the EA itself and the roles and responsibilities each key player in the process.

7.2.3. Investment Review Board (IRB)

The USCP has formalized its investment review and management process based on "best practices" and legislative requirements by establishing the Investment Review Board (IRB). The IRB consists of Bureau Heads and Office Directors. The Clinger-Cohen Act requires that each agency undertake capital planning and investment control by establishing a "process for maximizing the value and assessing and managing risks of information technology acquisitions". The primary purpose of the IRB is to implement the Investment Management Process that drives budget formulation and execution for investments. All USCP investments are within the purview of the investment management process and administered by the IRB. The IRB focus is on those investments that exceed thresholds established by the IRB. For projects funded on behalf of the USCP, the IRB considers the effect of agreements on project schedules and resources. The IRB determines the business value of entering into any agreement.

7.2.4. Office of Information Systems (OIS)

The Office of Information Systems is responsible for the planning, acquisition, implementation, operation, and management of the USCP automated information systems. Members of OIS assisted in the development of its IT and Departmental Strategic and Performance Plan as well as the Risk Management Plan. OIS also provides executive support to the IRB, including handling the logistics, maintaining and updating he IRB

history file, and serving as the IRB point of contact for Sponsors. The planning and policy component of OIS is staff to the IRB and the contact point for investment issues. OIS is the Department's organizational entity providing IT Operations, Planning, and Networking for the USCP, on a day-to-day basis.

7.2.5. Service Level Agreement

Defined as a formal written agreement made between two parties: the service provider and the service recipient. The SLA itself defines the basis of understanding between parties for delivery of the service itself. The document approximates a formal contract. The contents varies according to the nature of the service. SLAs are most common for provision of IT services and defines specified levels of service. USCP fields SLA's internally with its customer base and externally with service providers.

7.2.6. Transition Plan

The USCP Transition Plan documents the implementation methodology for the BSMO and describes how individual projects will be accomplished and integrated into the overall USCP EA. The Transition Plan provides BSMO a guide to the implementation of the individual projects and their integration as specified by the USCP Enterprise Architecture. This plan is used by the OIS Director and BSMO Chairman to establish and oversight procedures to be followed by BSMO participants in the accomplishment of the program's goals and objectives. This transition plan also assists in the budget formulation for out years related to systems development and operations and maintenance. The plan is used as a program management and communications tool to monitor the governance and implementation of the initiatives.

7.3. Investment Management Process (IMP)

USCP has developed an IT Investment Management Process (IMP) to assist in aligning the Department's portfolio of IT investments with the Department's vision, mission, goals, and objectives to improve the delivery of services to internal and external stakeholders. The IMP outlines a systematic approach to managing the risks and returns associated with IT capital investments. The IMP is an integrated management process providing for the continuous selection, management, and evaluation of investments focused on achieving a desired business outcome. Department leadership, through the IRB and BSMO, closely manage each program/project throughout its life cycle to ensure the investment achieves or exceeds the planned benefits proposed in the business case. IMP Benefits provide for comparative reviews of mgmt process, comparative performance of org units at different maturity levels (look at trends), alignment of investments with target EA, provides organizations ability to take on new initiatives, and redirecting resources to other programs (not just IT, [5].

7.3.1. The Capital Planning and Investment Control Guide (CPIC)

CPIC identifies the processes and activities necessary to ensure that USCP's investments are well through out, cost effective, and support the mission business goals of the organization. CPIC reduces the chances for redundant projects and make it easier to stop work on projects that fall below the approved standard. CPIC provides organizational improvement by a better understanding & mgmt of related risks; ensure investments selected based on merit by well informed decision making body; increases the business value and mission performance of investments. CPIC provides a standard for which the program can be evaluated [19]. To develop this guide, the USCP Office of Information Systems, used guidance from the Office of Management and Budget (*OMB Circular A-130*) and the General Accountability Office (*GAO, ITIM*). This guide is a living document that the Department continuously updates to reflect lessons learned and new government .

7.4. Standards, Policies, and Procedures

The Policy Handbook [18] establishes a policy procedural framework for the Office of Information Systems (OIS) Program within the United States Capitol Police (USCP). The OIS program provides for IT planning, budgeting, organizing, directing, training and controlling information. The program encompasses both information itself and related resources such as personnel, equipment, funds and technology. The Handbook is intended to provide the

Department with a structure for the implementation of policies and regulations issued by the Office of Information Services.

In addition, the Handbook establishes the authorities and responsibilities under which the OIS Program functions at the Department. The Handbook includes OIS policy providing primary documents in a concise and consolidated manner, and detailed procedures and operating guidelines, to include the life cycle management of information activities (i.e., creation, collection, and use); information functions (i.e., automatic data processing, records management, reports management, and telecommunications); the integrated approach to managing information resources (i.e., total systems concept) and the promotion and use of new technologies to improve the effective use and dissemination of information.

Among other things, the Handbook addresses the development and maintenance of an inventory of its information systems and review periodically its information management activities; to ensure that its information systems do not overlap with each other or duplicate the systems of other Departmental programs; and assigns to the designated senior official the responsibility for the conduct of and accountability for any acquisitions made.

7.4.1 Documentation

USCP stores all documentation related to programs and projects on a dedicated drive. MS Office suite is used to capture information . The suite includes MS Project, Visio, MS Access, Excel and MS Word. Additionally, USCP uses Rational Rose for UML, and the Proforma Application for alignment modeling. The USCP **"**police-net**"** (intranet) publishes the IT Standards, Policies and Procedures Handbook, as well as, the Strategic Plan, Performance Plan, and Enterprise Architecture for the Department

8.0 ENTERPRISE PERFORMANCE PLAN

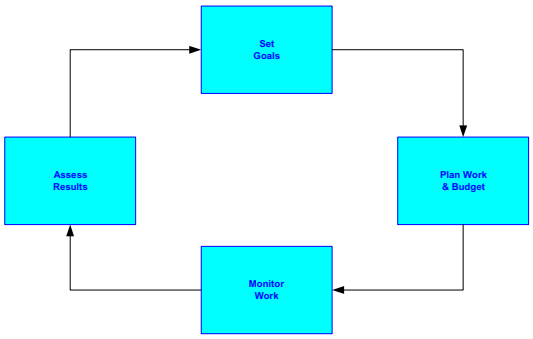


Figure 5. Enterprise performance management framework

The Annual Performance Plan [14] & [16] defines how the USCP pursues the Department's strategic goals and objectives during the fiscal year. It accompanies the 5-year Strategic Plan and fulfills the requirements of the Department's fiscal year 2003 appropriations law, Public Law 108-7. This legislation requires USCP to produce a yearly plan that includes quantifiable performance measures for each objective of the Strategic Plan that applies during the year. These measures assist Congress and USCP determine the success of the Capitol Police in meeting the Department's objectives. In addition to the measures, the annual Performance Plan presents milestones and completion dates for the fiscal year(s) that help USCP and stakeholders track the Department's progress in carrying out work around each strategy. These milestones support operational strategies that contribute to the Department's successful achievement of the objectives outlined in the USCP Strategic Plan. There are 32 performance measures that are used to determine the success of the Capitol Police in meeting the goals and objectives stated in the Strategic Plan.

USCP involved the Command Staff, the Capitol Police Board, and the Congressional Committees. Senior USCP staff met with stakeholders to ensure that USCP was focusing on measures that provide the information needed to make informed decisions about the future of the US Capitol Police. The performance measures have been base-lined, several measures have changed to better reflect the accounting necessary for tracking purposes. The measures illustrate USCP's commitment to continuously improve the Department's operations and procedures. Every improvement made enables the USCP to more effectively protect the Congress, its legislative processes, Members,

employees, visitors, and facilities from crime, disruption, or terrorism.

The Performance Planning effort allows USCP to establish targets and accountability. USCP Operational and Business units track and report the Department's progress quarterly, on reaching the goals and objectives. USCP also incorporates discussion of performance results into the current Department annual report, which is a precursor to the planned production of a full Performance and Accountability Report.

As shown in Figure 5: Enterprise Performance Management Framework, the Department brought together a number of new and existing processes, outputs, and programs into a comprehensive framework for managing USCP's overall performance. The successful implementation of this performance management capability enables the USCP employees to understand how they contribute to the achievement of USCP's goals and objectives; it ensures that the stakeholders understand how USCP serves them; and ultimately, it enables the entire community of the Capitol to be safe from crime, disruption, or terrorism.

8. Conclusions

The Department's Enterprise Framework – using a risk-based approach - provides a process that links technology and business functions, driven by the organizations mission and priorities, holding those accountable to a standard, for producing the necessary performance, to satisfy the internal and external stakeholders.

9. References

[1] A Guide to Project Management Body of Knowledge, Third Edition, (PMBOK Guide), 2004 Project Mgmt Institute, Inc. 388pp.

[2] A UML-driven Enterprise Architecture Case Study, Frank Armour, Steve Kaisler, Jim Getter, and Doug Pippin, IEEE HICCS'36 Conference, Hawaii, January 2003.

[3] Capability Maturity Model Integration, Carnegie-Mellon University, Software Engineering Institute.

[4] Enterprise Architecture Communication Plan, USCP, Revised June 2006.

[5] GAO IT Investment Mgmt (ITIM) Framework for Assess & Improving Process Maturity, (GAO-04-394G, Mar 2004, ver 1.1)

[6] Institute of Electrical and Electronic Engineers, Software Engineering Standards Collection, August 2003.

[7] Federal Information Security Management Act, 2002.

[8] Management of Enterprise Administrative Systems Implementation at US Capitol Police, Michael Valivullah, Jim Getter, Frank Armour, Steve Kaisler, INCOSE Conference, Washington, DC, July 2003.

[9] Modeling Enterprise IT Architectural Views with UML and IBM Rational Rose, Frank Armour, Steve Kaisler, Jim Getter, Rational Users Conference, Orlando, Florida, August 2003.

[10] Risk Management, Rita Mulcahy, RMC Pubs, Inc*., 2003*, 336p.

[11] Technology Assessment US Capitol Police, JB&A, December 2000

[12] USCP Strategic Plan, U.S. Capitol Police, August 2003, 38 pp.

[13] USCP Enterprise Architecture, Version 3, U.S. Capitol Police, October 2004, 850pp.

[14] USCP Performance Plan, U.S. Capitol Police, October 200, 52pp.

[15] USCP IT Strategic Plan, U.S. Capitol Police, April 2004, 15pp.

[16] USCP IT Performance Plan, U.S. Capitol Police, October 2004,33pp.

[17] USCP IT Alignment Study, U.S. Capitol Police, 54pp.

[18] USCP IT Polices and Procedural Handbook, US Capitol Police, April 2002, 413pp.

[19] USCP Capital Planning & Investment Control Guide, April 2004, 85pp.

[20] USCP, Risk Management Plan, revised June 2006.