U.S. Department of the Interior

Interior Enterprise Architecture

Conceptual Architecture

Principles

January 4, 2002

Introduction and Background

The Clinger-Cohen Act of 1996 requires the heads of Federal agencies to link information technology (IT) investments to agency accomplishments, and to establish a process to select, manage and control these agency investments. To meet this requirement, the Office of the Chief Information Officer (OCIO) is leading the effort to create an Interior-wide enterprise architecture. Enterprise architecture is an integrated framework and governance process for managing and evolving IT while meeting strategic and information resource management goals.

To be successful, the architecture must be derived from business requirements and be understood and supported by IT senior management and the heads of the Bureaus. Information technology does not exist for its own purposes; rather it exists to support the needs of business users. Accordingly, the first major product of the architecture process is the IEA Common Requirements Vision (CRV), published on October 15, 2001. This vision document is intended to ensure that Interior's IT products and services are aligned with the business community's strategic direction. It preceded creation of this document, the IEA Conceptual Architecture Principles (CAP), a logically consistent set of principles that are derived from the business requirements and will be used to guide the engineering of the organization's information systems and technology infrastructure. In essence, the architecture is the DNA necessary for successful growth and development of information technology throughout Interior.

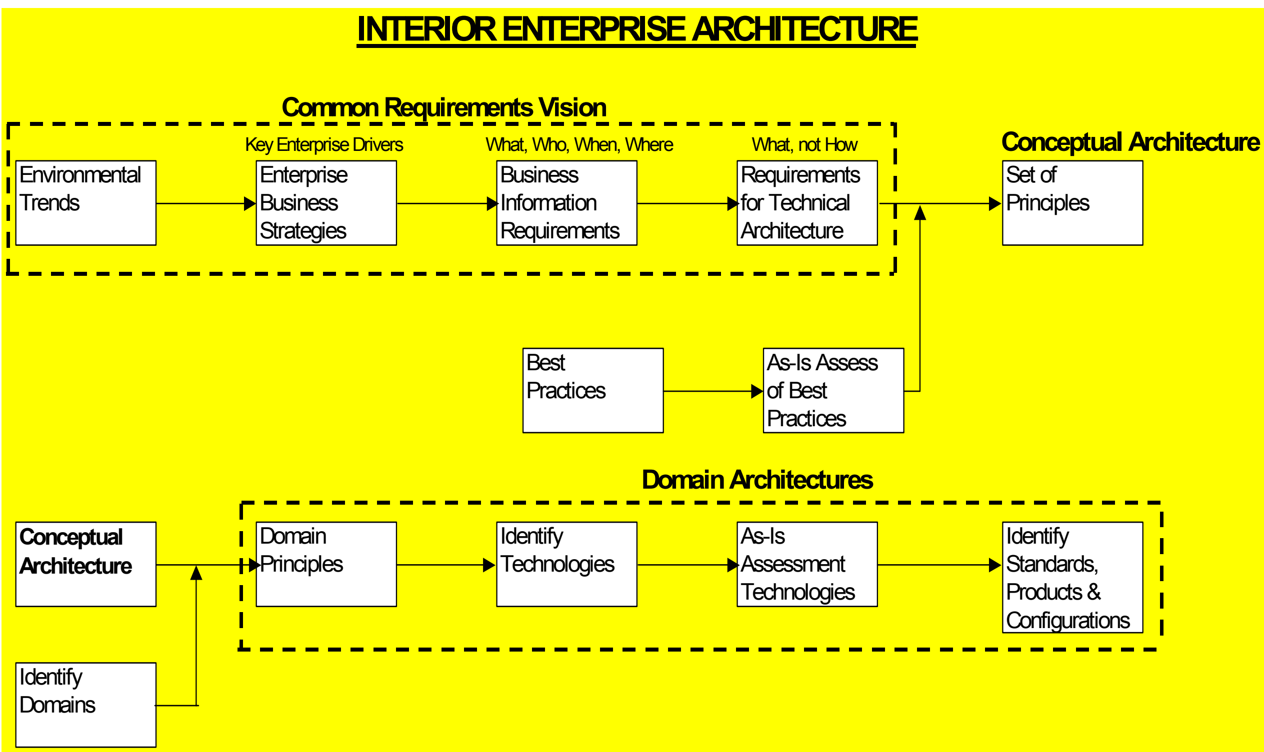
The Interior Architecture Program employs a federated approach to architecture development, focusing exclusively on business processes common to two or more Bureaus or Offices. This approach enables Interior to focus on crosscutting needs while recognizing the responsibility of Bureaus and Offices to manage business processes unique to their individual environments. The Interior Enterprise Architecture will provide the framework needed to ensure Bureau and Office architectures are aligned with Interior as a whole.

Current Approach

The current effort to develop a high-level Interior Enterprise Architecture (IEA) will be accomplished in eight phases. They are:

1. Architecture Management and Governance
2. Common Requirements Vision
3. Conceptual Architecture Principles
4. Domain Architectures
5. Current Technical Infrastructure Documentation
6. Gap Analysis
7. Migration Planning
8. Implementation Planning

Below is a simplified graphic of a portion of the META Group, Inc. Enterprise Architecture Strategies (EAS) process to create the CRV, the CAP, and the next phase of the IEA, development of Domain Architectures.



Once the high-level effort is complete, work will begin on development of the next level iteration of the IEA. Architecture is never "done" -- it continually evolves through refining and updating, increasing the level of detail, and enhancing the architecture governance processes. This ongoing process increasingly evolves the blueprint used by management to make informed IT investment and design decisions.

Introduction to Conceptual Architecture Principles

The Interior Enterprise Architecture (IEA) Conceptual Architecture Principles (CAP) represents core business and technical guidelines upon which all Interior-wide technical domain architectures will be based. These principles guide the implementation of technology to meet Interior-wide requirements as well as guide decision-making to maximize business benefit and the adaptability of the IT environment.

IEA CAP must be incorporated into information technology planning and solution design activities by the bureaus and their IT contractors. Guided by industry and government best practices, the principles are articulated in basic business language understood by all those involved in the IT decision-making process.

IEA CAP plays a pivotal role in obtaining the results and actions desired, stemming from the values of an organization. Upon reading a principle, a common reaction is that "this is all motherhood and apple pie." Although a principle may seem self-evident, that does not mean that the principle is actually observed within Interior today.

Adopting the set of principles should initiate a change process in information and technology-related policies and procedures to bring them into conformance with IEA. Violations of principles in an environment employing enterprise architecture generally lead to operational problems and inhibit the ability of the organization to fulfill its mission. For the purposes of the Interior Enterprise Architecture, the principles will:

- Provide a firm foundation for making architecture and planning decisions,
- Frame policies, procedures and standards, and
- Lead the way to resolving technology conflicts.

The set of principles stands as a guide for accomplishing technology alignment with business requirements. Business issues of importance to the leadership of Interior, such as the need for Interior systems and technology to function in a manner that provides for adequate security, confidentiality and privacy of Interior data, is reflected in Principles 5 and 9, among others.

The 14 principles are divided into two categories: Business Oriented (7) and Technology Oriented (7). The principles are stated, but more importantly, the rationale for each principle and the implications of their adoption are delineated. Decisions made regarding domain architecture technologies, standards, products and configurations will be traceable to these principles.

Criteria for Effective Principles

There are five (5) criteria that distinguish effective principles. They are:

Criteria	**Explanation**
Understandable	The underlying tenets of the principles can be quickly grasped and understood by individuals throughout the enterprise. The intention of the principle is clear and unambiguous so that violations, whether intentional or not, are minimized.
Robust	Enforceable policies and standards can be created from the principles. There are no "easy out" exception clauses or expressions. Each set of principles should be sufficiently definitive and precise for deciding a wide range of potentially controversial situations.
Complete	Every potentially important principle governing the management of information and technology for the enterprise has been defined. The principles are applicable to every perceived situation.
Consistent	Every word in a principle statement should be carefully chosen to ensure consistent interpretation. There may be times, however, when strict adherence to one principle may require a loose interpretation of another principle. For example, access to information may be weighed against ease of use, and the need to provide for security, confidentiality and privacy will take precedence over the sharing of data with others. There must be a balance of interpretations of the principles. Principles should not be contradictory to the point where adhering to one principle would violate the spirit of another.
Stable	Principles should have a "timeless" quality about them, and be able to transcend all foreseeable changes that could occur. The principles for information and technology management need not be changed to keep pace with technology advances.

Conceptual Architecture Principles

Summary of Principles

Principle 1: Information is valued as an Interior asset to accelerate sound decision-making, improve management, and increase accountability.

Principle 2: Data and information must be managed and maintained as a stewardship responsibility to support the mission of the department.

Principle 3: Systems must be designed, acquired, developed, or enhanced such that data and processes can be effectively shared across Interior and with our partners.

Principle 4: In considering system requirements (e.g., new functionality), we should look to reuse existing components before we buy. If no components exist, purchased solutions (e.g., COTS or GOTS) should be explored before we build.

Principle 5: IT systems should be implemented in adherence with security, confidentiality and privacy policies to assure proper safeguards and limitations for information availability and access.

Principle 6: An assessment of business continuation and recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design, testing and maintenance will take place.

Principle 7: A basic set of information services will be provided to all employees.

Principle 8: We must implement an Interior-wide "interoperable network" performing as if it were a virtual, Interior-wide Local Area Network.

Principle 9: Easy and timely access to data and information is the rule rather than the exception, without security and privacy being compromised.

Principle 10: Business processes will be analyzed, simplified or otherwise redesigned in preparation for and during information systems enhancements, development, and implementation.

Principle 11: Interior will adopt a total cost of ownership model for IT systems that includes life-cycle considerations like the costs of development, implementation/ transition, training, support, disaster recovery, and retirement as well as the impacts of flexibility, scalability, ease of use and reduction of integration complexity.

Principle 12: IT solutions will use industry-proven and "state-of-the-art" mainstream technologies.

Principle 13: Priority will be given to products adhering to industry standards and open architecture.

Principle 14: The planning and management of the Interior Enterprise Architecture will follow a unified "federated" model. It will include sufficient support and review structures to ensure that the integrity of the architecture is maintained as systems are acquired, developed and enhanced.

Conceptual Architecture Principles

Business Oriented

Principle 1: Information is an Interior asset.

Information is valued as an Interior asset to accelerate decision-making, improve management, and increase accountability.

Rationale:
- The value of information is not realized if it is held in isolated pockets.
- Information must be shared to maximize effective decision-making across lines of business and with partners.
- Information is necessary for decision making to support accelerated business process cycles.
- Increased access leads to improved integrity and relevance of data.

Implications:
- Supporting policies regarding security, privacy, confidentiality, information sharing, information integrity, utility and data relevance must be developed and implemented.
- Need to promote interoperable information management, such as data warehouses and data access methods that facilitate information availability for decision-making.
- Data warehouses, metadata and data accesses may need to be developed to facilitate information availability for decision-making.
- Information needs to be structured for easy access and management, timely availability, and use.
- Metadata (information about the data, such as source, units of measurement, and collection methods) will need to be developed and made available.

Principle 2: Data and Information Stewardship

Data and information must be managed and maintained as a stewardship responsibility to support the mission of Interior.

Rationale:
- Data is a resource important to the accomplishment of Interior's work. In its broadest sense, it is information including items like electronic and paper records, emails, film, etc. Like natural resources, data needs stewards who are responsible for its valuation, preservation, security, access and utilization across Interior and with the public.
- Data stewards will promote common business rules, which would facilitate information sharing and improve data integrity.

Implications:

- Recognition that business area personnel need to be responsible for stewardship of the data and the commitment of the resources necessary to make stewardship happen.
- Stewardship includes responsibility for clarification of the data's meaning, content, and reuse.
- Stewardship includes responsibility for managing data's consistency, timeliness, accuracy and completeness.
- The scope of stewardship must be very sensitive to the sources and uses of the information, ensuring security, confidentiality and privacy are protected.
- Need to develop a data stewardship program that will transcend many organizational boundaries (e.g., no current rewards for cross-bureau cooperation) and include various levels of stewardship while leveraging and adhering to Federal data programs and standards (e.g., FGDC, NIST).
- Recognition of the need to manage "meta" data; that is data "about" the data.

Principle 3: Integration/ Interoperability

Systems must be designed, acquired, developed, or enhanced such that data and processes can be effectively shared, for appropriate purposes, across Interior and with our partners.

Rationale:

- Increased efficiency will better serve our customers (e.g., the public, employees, etc.).
- Redundant systems cause higher support costs.
- Ensures more accurate information.
- Shared data and processes lead to better decision-making and accountability.

Implication:

- Over-integration can lead to difficult data management and inefficient processes.
- Every systems analyst needs to consider enterprise wide impacts when designing enhancing, acquiring or extending the scope or use of applications.
- We will need new tools that enable data sharing and the training for their proper use.
- Will need a method for identifying data and processes that need integration, when integration should take place, the degree of integration versus interoperability, who should have access to the data, and cost justification for integration.
- Will need common data standards and consistent data management processes across Interior.

Principle 4: Reuse before you buy and buy before you build.

In considering system requirements (e.g., new functionality), we should look to reuse existing components before we buy. If no components exist, purchased solutions (e.g., COTS or GOTS) should be explored before we build.

Rationale:

- Complies with OMB Circular A-130, the Privacy Act of 1974, and the Government Information Systems Reform Act.
- The more you're "like" everyone else (e.g., same standard, same systems), the easier it is to share with others.
- System development is not a primary mission of Interior.

Implications:

- Need to identify and maintain "reusable" components.
- Good system specifications will be needed early in the planning cycle to evaluate alternatives.
- Business processes may need to be "changed" but not compromised to ensure compliance with Interior and Federal standards, to accommodate reuse or purchased solutions.
- In-depth knowledge of system functions may be outside of the organization, potentially increasing issues of risk and cost.
- Requirement for greater sensitivity to the possibility of losing mission responsibility when using outside resources.
- System design will migrate to "open" standards.

Principle 5: Ensure Security, Confidentiality and Privacy

IT systems should be designed and implemented in accordance with security, confidentiality and privacy legislation and policies to assure appropriate information availability.

Rationale:

- Helps safeguard confidential and proprietary information.
- Enhances public trust.
- Enhances the proper stewardship over information.
- Enhances the integrity of the information.
- Complies with the Computer Security Act, the Privacy Act of 1974, and OMB Circular A-130.

Implications:

- Need to identify, publish and keep the applicable policies and attendant interpretations current.
- Need for education on issues of privacy, security, and confidentiality to become routine part of normal business processes.
- Need to make the security, confidentiality and privacy requirements clear to designers, developers, and operations personnel.

Principle 6: Continuity of Operations Planning

An assessment of business continuation and recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design, testing and maintenance will take place.

Rationale:

- Customers and partners have heightened awareness of the need for systems availability
- Any significant visible loss of system availability and stability could negatively impact our mission and legal responsibilities.
- Application systems and data are valuable organization assets that must be protected.

Implications:

- Operation and systems plans will need to be categorized according to business recovery needs (e.g., short term essential and long term essential).
- Alternate information resource capabilities need to be in place.
- Systems should be designed with appropriate level of fault tolerance and recovery in mind.
- Plans for work site recovery will need to be in place.
- Life cycle and other costs may increase.
- Continuity of Operations Planning (COOP)/ Continuity of Business Operations (COBO) will require periodic testing and revision.
- Plans for records recovery and alternate data capture mechanisms/processes need to be in place.
- Appropriate personnel certifications need to be available and in place.

Principle 7: Basic Services

A basic set of information services will be provided to all employees.

Rationale:

- Consistent IT capability provides the basis for larger business initiatives and greater access to information.
- Potentially reduces total cost of ownership.
- Provides basis for improved communication.

Implications:

- Basic services definition needs to be created and regularly reviewed and updated (e.g., email, voicemail, e-Forms, internet access).
- May increase initial costs for deploying personnel.
- More training will need to be provided to the entire organization for any addition to or modification of the basic services.
- May require 24x7 operation and associated personnel availability and costs.

Technology Oriented

Principle 8: Enterprise Network as "Virtual" LAN

We must implement an Interior-wide "interoperable network"; performing as if it were a virtual, Interior-wide Local Area Network.

Rationale:

- Networks are the essential enabling technology for client/server, Internet, and collaborative computing (e.g., emails, file transfers, secure teleconferencing, workflow).
- Knowledge workers' have increasing need for access to information across Interior; this access must appear seamless.
- Lack of a robust network architecture will impact the success of distributed applications.
- Expands the vision of organizations by reaching out to customers and suppliers.

Implications:

- Requires higher speed and higher bandwidth networks.
- Will need the interconnection of distributed LANs.
- Need to create connections between legacy systems, client/server and Internet applications.
- Need to implement a robust, interoperable directory services capability.
- Need to define guidelines around "who pays", "who uses", "who gets", and "who coordinates" these interoperable networks.
- Policies and protocols on sharing and exchanging information with third parties need to be addressed (e.g., restricted sub-nets will need to be supported).
- Need to accommodate remote locations with limited communications options.

Principle 9: Information Access

Easy and timely access to data and information is the rule rather than the exception without security and privacy being compromised.

Rationale:

- Productivity, decision-making, and customer service all benefit from easy, direct, and timely availability of information.
- In accordance with the Paperwork Reduction Act (PRA, PL 104-13), employees and the public should have efficient, effective, and economical access to Government information.
- Information should be attainable in the appropriate place, time, format and context.
- The Rehabilitation Act of 1998 requires executive agencies to develop, acquire and use information technology that is accessible to individuals with disabilities.
- Under E-FOIA bureaus and offices are required to make records that are frequently requested under the FOIA available for public inspection. Further, records created on or after November 1, 1996 must be available via the Internet or other electronic means.

- The Government Paperwork Elimination Act requires agencies to incorporate privacy protections when developing electronic processes.
- Beyond the legal requirements, easy and timely access to data and information makes sound business sense.

Implications:

- For unclassified information, the right to know should be presumed unless policy or law specify otherwise; however, for information like "pre-decisional information", access would still be controlled.
- The business necessity of sharing information must be established.
- Technology must be deployed to distribute and allow access to information.
- Classification of information must be clearly stated and the rules well defined.
- Secure information must not be accidentally released.
- A variety of public and private access methods for public information in accordance with E-FOIA will need to be provided.
- Information must be available in formats accessible to those with sensory disabilities in accordance with Section 508.
- Designation of sensitivity must be clearly stated.

Principle 10: Reengineer First

Business processes will be analyzed, simplified or otherwise redesigned in preparation for and during information systems enhancements, development, and implementation.

Rationale:

- Work processes should be streamlined, efficient, and cost-effective.
- Work processes, activities, and associated business rules will be well understood and documented.
- Enables E-Government initiatives.
- Potentially reduces the total cost of ownership.
- Provides better customer service.
- Required by Clinger-Cohen and A-130 before an IT investment can be made, and promotes compliance with the Government Performance and Results Act.

Implications:

- Need agreed upon business process re-engineering scope and results to enable continual improvement through analyzing, simplifying and redesigning work processes.
- New technology will be applied in conjunction with business process review.
- Business processes must be optimized to align with business drivers.
- Additional time and resources will have to be invested in business analysis early in the systems life cycle.
- Organizational change may be required to implement reengineered business processes.
- Requires all organizational levels, especially senior leadership to sponsor and support reengineering efforts.

Principle 11: Total Cost of Ownership

Interior will adopt a total cost of ownership model for IT systems that includes life-cycle considerations like the costs of development, implementation/transition, support, disaster recovery, and retirement as well as the impacts of flexibility, scalability, ease of use and reduction of integration complexity.

Rationale:
- Leads to better-informed decisions through an improved understanding of trade offs.
- Enables improved planning and budget decision-making.

Implications:
- Need to develop a total cost of ownership model and educate system sponsors and decision-makers about how to use it.
- Leads to coordinated system replacements, enhancements and retirements.
- Need to apply TCO to portfolio management and records management.
- Need to provide tools for collection of the actual total cost of ownership.

Principle 12: Mainstream Technologies

IT solutions will use industry-proven and "state-of-the-art" mainstream technologies.

Rationale:
- Avoids dependence on weak vendors.
- Ensures robust product support.
- Enables greater use of commercial-off-the-shelf solutions.
- Complies with OMB Circular A-130, which requires the application of up-to-date information technology to take advantage of opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

Implications:
- Need to establish criteria for vendor selection and performance measurement.
- Need to establish the criteria to identify the weak vendors and poor technology solutions in compliance with Federal government contracting policy and procedures.
- Requires the technology portfolio to migrate away from existing weak products or products that are reaching obsolescence.
- We may be slow to adopt new technologies.
- The exploration of new technology will be managed and investigation results shared.

Principle 13: Industry Standards

Extra value will be given to products adhering to industry standards and open architecture.

Rationale:
- Required to support data and process interoperability.

- Reduces risks.
- Reduces dependence on single vendor.
- Enables greater use of commercial-off-the-shelf solutions.
- Allows flexibility and adaptability in product enhancement, extensibility, and replacement.

Implications:

- Need effective management process to identify and assess industry standards and share standards information across Interior.
- Participation in the development of open standards is needed.
- Training and education is required to promote the use of "open standards."

Principle 14: Architecture Management

The planning and management of the Interior Enterprise Architecture will follow a unified "federated" model. It will include sufficient support and review structures to ensure that the integrity of the architecture is maintained as systems are acquired, developed and enhanced. ·

Rationale:

- Clinger-Cohen Act of 1996
- There will be a single Interior-wide technical architecture, supported by Bureau architectures. At the very least, there will be diversity among:
  - Priorities/Tradeoffs
  - Principles
  - Product Standards
  - Configurations
- Enables bureaus to maintain their diversity and uniqueness, yet enables process interoperability, information sharing, and the potential for driving down costs.

Implications:

- To realize the benefits of a standards-based Interior-wide architecture, all information technology investments must be reviewed through the IT Capital Planning and Investment Control process to ensure compliance with the established architecture.
- For maximum impact, review should begin as early in the solution planning process as possible.
- Since it is a federated model, which defines the principles and standards for the subset of the bureau architectures that is shared across Interior, the processes, procedures and guidelines for integrating the various bureau architectures will need to be created.
- A unified approach will assist in accomplishing the required cultural change.
- Governance will be improved through use of consistent, defined processes.
- A structured project level review process will be needed to ensure that information systems comply with the architecture and related standards.
- Processes incorporating the principles of this architecture must be developed for all application acquisition, development, design, major enhancement and management activities.

- This compliance process must allow for the introduction of new technology and standards.
- Architecture principles should be used as evaluation criteria for acquiring as well as major enhancements and development of new systems.
- Interior Department and bureau leadership and staff must accept and adhere to a unified architecture standard to ensure success.