Global Principles

BT EA Global Principles

Revision 1.0

01/29/2013

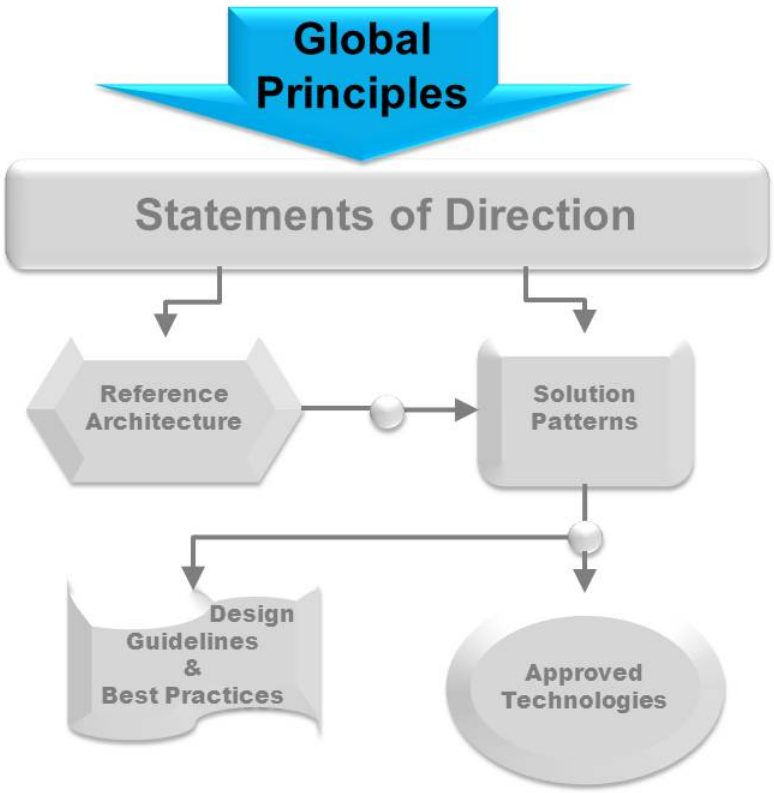

Table of Contents

1.0 Statements

1.1. Business Principles

1.1.1. Principle 1: Primacy of Principles

These principles of information management apply to all organizations within the enterprise.

1.1.2. Principle 2: Maximize Benefit to the Enterprise

Information management decisions are made to provide maximum benefit to the enterprise as a whole.

1.1.3. Principle 3: Information Management is Everybody's Business

All organizations in the enterprise participate in information management decisions needed to accomplish business objectives.

1.1.4. Principle 4: Business Continuity

Enterprise operations are maintained in spite of system interruptions.

1.1.5. Principle 5: Common Use Applications

Development of applications used across the enterprise is preferred over the development of similar or duplicative applications which are only provided to a particular organization.

1.1.6. Principle 6: Compliance with Law

Enterprise information management processes comply with all relevant laws, policies, and regulations.

1.1.7. Principle 7: IT Responsibility

The IT organization is responsible for owning and implementing IT processes and infrastructure that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

1.1.8. Principle 8: Protection of Intellectual Property

The enterprise's Intellectual Property (IP) must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes.

1.2. Data Principles

1.2.1. Principle 9: Data is an Asset

Data is an asset that has value to the enterprise and is managed accordingly.

1.2.2. Principle 10: Data is Shared

Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations.

1.2.3. Principle 11: Data is Accessible

Data is accessible for users to perform their functions.

1.2.4. Principle 12: Data Trustee

Each data element has a trustee accountable for data quality.

1.2.5. Principle 13: Common Vocabulary and Data Definitions

Data is defined consistently throughout the enterprise, and the definitions are understandable and available to all users.

1.2.6. Principle 14: Data Security

Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information.

1.3. Application Principles

1.3.1. Principle 15: Technology Independence

Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.

1.3.2. Principle 16: Ease-of-Use

Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand.

1.4. Technology Principles

1.4.1. Principle 17: Requirements-Based Change

Only in response to business needs are changes to applications and technology made.

1.4.2. Principle 18: Responsive Change Management

Changes to the enterprise information environment are implemented in a timely manner.

1.4.3. Principle 19: Control Technical Diversity

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

1.4.4. Principle 20: Interoperability

Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

2.0 Rationales

2.1. Business Principles

2.1.1. Principle 1: Primacy of Principles

The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organizations abide by the principles.

2.1.2. Principle 2: Maximize Benefit to the Enterprise

This principle embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires information management decisions to adhere to enterprise-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.

2.1.3. Principle 3: Information Management is Everybody's Business

Information users are the key stakeholders, or customers, in the application of technology to address a business need. In order to ensure information management is aligned with the business, all organizations in the enterprise must be involved in all aspects of the information environment. The business experts from across the enterprise and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of IT.

2.1.4. Principle 4: Business Continuity

As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative information delivery mechanisms.

2.1.5. Principle 5: Common Use Applications

Duplicative capability is expensive and proliferates conflicting data.

2.1.6. Principle 6: Compliance with Law

Enterprise policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.

2.1.7. Principle 7: IT Responsibility

Effectively align expectations with capabilities and costs so that all projects are cost-effective. Efficient and effective solutions have reasonable costs and clear benefits.

2.1.8. Principle 8: Protection of Intellectual Property

A major part of an enterprise's IP is hosted in the IT domain.

2.2. Data Principles

2.2.1. Principle 9: Data is an Asset

Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.

2.2.2. Principle 10: Data is Shared

Timely access to accurate data is essential to improving the quality and efficiency of enterprise decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The enterprise holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization.

Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.

2.2.3. Principle 11: Data is Accessible

Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved.

2.2.4. Principle 12: Data Trustee

One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the enterprise. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources.

Note: A trustee is different than a steward - a trustee is responsible for accuracy and currency of the data, while responsibilities of a steward may be broader and include data standardization and definition tasks.

2.2.5. Principle 13: Common Vocabulary and Data Definitions

The data that will be used in the development of applications must have a common definition throughout the Headquarters to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.

2.2.6. Principle 14: Data Security

Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

Existing laws and regulations require the safeguarding of national security and the privacy of data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorized for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.

2.3. Application Principles

2.3.1. Principle 15: Technology Independence

Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves.

Realizing that every decision made with respect to IT makes us dependent on that technology, the intent of this principle is to ensure that Application Software is not dependent on specific hardware and operating systems software.

2.3.2. Principle 16: Ease-of-Use

The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the enterprise's integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low.

2.4. Technology Principles

2.4.1. Principle 17: Requirements-Based Change

This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support - the transaction of business - is the basis for any proposed change. Unintended effects on business due to IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.

2.4.2. Principle 18: Responsive Change Management

If people are to be expected to work within the enterprise information environment, that information environment must be responsive to their needs.

2.4.3. Principle 19: Control Technical Diversity

There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained.

Limiting the number of supported components will simplify maintainability and reduce costs.

The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

2.4.4. Principle 20: Interoperability

Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.

3.0 Implications

3.1. Business Principles

3.1.1. Principle 1: Primacy of Principles

- Without this principle, exclusions, favoritism, and inconsistency would rapidly undermine the management of information.
- Information management initiatives will not begin until they are examined for compliance with the principles.
- A conflict with a principle will be resolved by changing the framework of the initiative.

3.1.2. Principle 2: Maximize Benefit to the Enterprise

- Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage information. Technology alone will not bring about this change.
- Some organizations may have to concede their own preferences for the greater benefit of the entire enterprise.
- Application development priorities must be established by the entire enterprise for the entire enterprise.
- Applications components should be shared across organizational boundaries.
- Information management initiatives should be conducted in accordance with the enterprise plan. Individual organizations should pursue information management initiatives which conform to the blueprints and priorities established by the enterprise. We will change the plan as we need to.
- As needs arise, priorities must be adjusted. A forum with comprehensive enterprise representation should make these decisions.

3.1.3. Principle 3: Information Management is Everybody's Business

- To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment.
- Commitment of resources will be required to implement this principle.

3.1.4. Principle 4: Business Continuity

- Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to assure business function continuity through redundant or alternative capabilities.

- Recoverability, redundancy, and maintainability should be addressed at the time of design.
- Applications must be assessed for criticality and impact on the enterprise mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.

3.1.5. Principle 5: Common Use Applications

- Organizations which depend on a capability which does not serve the entire enterprise must change over to the replacement enterprise-wide capability. This will require establishment of and adherence to a policy requiring this.
- Organizations will not be allowed to develop capabilities for their own use which are similar/duplicative of enterprise-wide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- Data and information used to support enterprise decision-making will be standardized to a much greater extent than previously. This is because the smaller, organizational capabilities which produced different data (which was not shared among other organizations) will be replaced by enterprise-wide capabilities. The impetus for adding to the set of enterprise-wide capabilities may well come from an organization making a convincing case for the value of the data/information previously produced by its organizational capability, but the resulting capability will become part of the enterprise-wide system, and the data it produces will be shared across the enterprise.

3.1.6. Principle 6: Compliance with Law

- The enterprise must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data.
- Education and access to the rules. Efficiency, need, and common sense are not the only drivers. Changes in the law and changes in regulations may drive changes in our processes or applications.

3.1.7. Principle 7: IT Responsibility

- A process must be created to prioritize projects.
- The IT function must define processes to manage business unit expectations.
- Data, application, and technology models must be created to enable integrated quality solutions and to maximize results.

3.1.8. Principle 8: Protection of Intellectual Property

- While protection of IP assets is everybody's business, much of the actual protection is implemented in the IT domain. Even trust in non-IT processes can be managed by IT processes (email, mandatory notes, etc.).

- A security policy, governing human and IT actors, will be required that can substantially improve protection of IP. This must be capable of both avoiding compromises and reducing liabilities.
- Resources on such policies can be found at the SANS Institute (www.sans.org/newlook/home.php).

3.2. Data Principles

3.2.1. Principle 9: Data is an Asset

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data.
- Stewards must have the authority and means to manage the data for which they are accountable.
- We must make the cultural transition from "data ownership" thinking to "data stewardship" thinking.
- The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise.
- Part of the role of data steward, who manages the data, is to ensure data quality. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality - it is probable that policy and procedures will need to be developed for this as well.
- A forum with comprehensive enterprise-wide representation should decide on process changes suggested by the steward.
- Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at the enterprise level.

3.2.2. Principle 10: Data is Shared

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data.
- To enable data sharing we must develop and abide by a common set of policies, procedures, and standards governing data management and access for both the short and the long term.

- For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment.
- We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible.
- For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications.
- For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the enterprise.
- Data sharing will require a significant cultural change.
- This principle of data sharing will continually "bump up against" the principle of data security. Under no circumstances will the data sharing principle cause confidential data to be compromised.
- Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the enterprise-wide "virtual single source" of data.

3.2.3. Principle 11: Data is Accessible

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data.
- Accessibility involves the ease with which users obtain information.
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of enterprise users and their corresponding methods of access.
- Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.
- Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require an education process and a change in the organizational culture, which currently supports a belief in "ownership" of data by functional units.

3.2.4. Principle 12: Data Trustee

- Real trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs. This implies that a cultural change from data "ownership" to data "trusteeship" may be required.
- The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable.
- It is essential that the trustee has the ability to provide user confidence in the data based upon attributes such as "data source".
- It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the trustee.
- Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.
- As a result of sharing data across the enterprise, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognize the importance of this trusteeship responsibility.

3.2.5. Principle 13: Common Vocabulary and Data Definitions

- We are lulled into thinking that this issue is adequately addressed because there are people with "data administration" job titles and forums with charters implying responsibility. Significant additional energy and resources must be committed to this task. It is key to the success of efforts to improve the information environment. This is separate from but related to the issue of data element definition, which is addressed by a broad community - this is more like a common vocabulary and definition.
- The enterprise must establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the enterprise.
- Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the corporate "glossary" of data descriptions. The enterprise data administrator will provide this co-ordination.
- Ambiguities resulting from multiple parochial definitions of data must give way to accepted enterprise-wide definitions and understanding.
- Multiple data standardization initiatives need to be coordinated.
- Functional data administration responsibilities must be assigned.

3.2.6. Principle 14: Data Security

- Aggregation of data, both classified and not, will create a large target requiring review and de-classification procedures to maintain appropriate control. Data

owners and/or functional users must determine whether the aggregation results in an increased classification level. We will need appropriate policy and procedures to handle this review and de-classification. Access to information based on a need-to-know policy will force regular reviews of the body of information.

- The current practice of having separate systems to contain different classifications needs to be rethought. Is there a software solution to separating classified and unclassified data? The current hardware solution is unwieldy, inefficient, and costly. It is more expensive to manage unclassified data on a classified system. Currently, the only way to combine the two is to place the unclassified data on the classified system, where it must remain.
- In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level.
- Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labeling for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined.
- Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation. Headquarters information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.
- Need new policies on managing duration of protection for pre-decisional information and other works-in-progress, in consideration of content freshness.

3.3. Application Principles

3.3.1. Principle 15: Technology Independence

- This principle will require standards which support portability.
- For Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) applications, there may be limited current choices, as many of these applications are technology and platform-dependent.
- Application Program Interfaces (APIs) will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the enterprise architecture.
- Middleware should be used to decouple applications from specific software solutions.
- As an example, this principle could lead to use of Java, and future Java-like protocols, which give a high degree of priority to platform-independence.

3.3.2. Principle 16: Ease-of-Use

- Applications will be required to have a common "look and feel" and support ergonomic requirements. Hence, the common look and feel standard must be designed and usability test criteria must be developed.
- Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, customer physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application.

3.4. Technology Principles

3.4.1. Principle 17: Requirements-Based Change

- Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.
- We don't fund a technical improvement or system development unless a documented business need exists.
- Change management processes conforming to this principle will be developed and implemented.
- This principle may bump up against the responsive change principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. The purpose of this principle is to keep us focused on business, not technology needs - responsive change is also a business need.

3.4.2. Principle 18: Responsive Change Management

- We have to develop processes for managing and implementing change that do not create delays.
- A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need.
- If we are going to make changes, we must keep the architectures updated.
- Adopting this principle might require additional resources.
- This will conflict with other principles (e.g., maximum enterprise-wide benefit, enterprise-wide applications, etc.).

3.4.3. Principle 19: Control Technical Diversity

- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.

- Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.
- We are not freezing our technology baseline. We welcome technology advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.

3.4.4. Principle 20: Interoperability

- Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.
- The existing IT platforms must be identified and documented.

4.0 Glossary

Note: Also refer to the DFS Glossary

5.0 References

Protection of Intellectual Property

Resources on such policies can be found at the SANS Institute (www.sans.org).

Revision History and Contributors

Revision Date	Approved By	Author	Changes	Revision
01/29/2013		R Hauenstein	Initial Release	1.0

Reviewers/Contributors:

Name	Department/Contribution

Meta Tags

Note: Meta Tab in bold is the unique identifier

bt_(title)_global_principles

bt_guiding_principles