21 principles of enterprise architecture for the financial sector

Thiago Souza Mendes Guimarães

November 20, 2012

The article lists the most relevant architectural principles for an IT department to follow in the financial market, with details about each principle. These principles are essential for an IT department to take on a strategic role in the company and to indicate actual value generation in IT decisions within an environment where pressure and business decisions are critical.

Structure of these principles

This article was developed with the purpose of proposing certain principles that must drive an enterprise architecture initiative. The main motivation that led to the development of this list is the difficulty of implementing enterprise architecture in an environment as hostile as the financial market. There is great pressure on the technology segment, which is usually not perceived as strategic. An even greater challenge is showing that IT decisions can add value and differentials to businesses.

This list was organized and developed based on the selection and adjustment of the most relevant principles established throughout my experience in the financial market. Despite being selected within the financial segment context, most of these principles apply to any type of industry after only a few minor adjustments.

Definitions

Principles are high-level definitions of fundamental values that guide the IT decision-making process, serving as a base for the IT architecture, development policies, and standards.

The principles of architecture define general rules and guidelines to use and implement all information technology (IT) resources and assets throughout a company. They must reflect a level of consensus between several corporate components and areas, constituting the basis for future IT decisions.

Each architecture principle must focus mainly on business goals and key architecture applications.

Format of each principle

Each principle must be formally stated. Some suggestions regarding the format in which principles must be stated are available in related literature. This article follows the format suggested by The
Open Group Architecture Framework (TOGAF), in which each principle is presented according to the following format:

Name
The name must represent the essence of the rule and be easy to remember. Specific technology platforms must not be mentioned in a principle's name or description.

Description
The description must succinctly and directly convey the fundamental rule. Most information management principle descriptions are similar among different companies.

Rationale
This must highlight business benefits generated by adhering to the principle, using business terminology. It must emphasize the similarity between information and technology principles and those that regulate business operations. The rationale must also describe its relationship to other principles and intentions compared to a balanced interpretation. It should describe situations in which a certain principle would outweigh another in the decision-making process.

Implications
This item must highlight requirements, both for businesses and IT, to comply with the principle regarding resources, costs, and activities or tasks. The impacts in businesses and consequences of adopting a principle must be detailed. Readers must be able to easily answer the following question: "How does this affect me?" It is important not to simplify, trivialize, or question the merit of such impacts. Some implications are exclusively identified as potential impacts, with a speculative characteristic as opposed to being fully analyzed.

Four categories of principles
Usually, there are around 20 enterprise architecture principles that must be followed. A very short list contains more generic and ethereal principles, hindering practical applications. On the other hand, an excessively extensive list is too specific and generates inconsistencies and conflicts between principles and changes resulting from technological, environmental, and contextual evolution. The following list has 21 principles, organized in four categories.

• General principles
• Information principles
• Application principles
• Technology principles

General principles
Principle 1. IT and business alignment
Description
Information management decisions are always made under the business alignment perspective in order to generate maximum benefits for the company as a whole.
Rationale

This principle means "service above all." A better alignment between IT and the business must generate a competitive edge for the financial institution.

Decisions based on the corporate perspective have greater long-term value than decisions based on a certain perspective of a group with a specific interest. An optimal ROI requires information management decisions to be aligned with the company's priorities and positioning. No single area must affect the benefit of the company. This principle, however, must not prevent anyone from performing tasks and activities.

Implications

Aligning IT with the business and promoting optimal corporate benefits requires changes in how information is planned and managed. Technology alone is not enough to promote such changes.

IT must direct its processes towards the front office.

IT cost management must focus on IT services directed toward establishing a competitive edge.

IT management must add responsiveness and availability indicators.

IT architecture must implement a complete IT vision that is focused on business.

Some areas might need to waive their specific preferences to benefit the company as a whole.

Application development priorities must be established by and for the entire company.

Application components must be shared among all areas of the financial institution.

Information management initiatives must be conducted based on a corporate plan. Individual areas must follow information management initiatives in accordance with corporate plans and priorities. Planning is modified whenever necessary.

As new needs arise, priorities must be adjusted proportionally. A corporate representation committee must make such decisions.

Principle 2. Maximum benefits at the lowest costs and risks

Description

Strategic decisions for solutions must always strive to maximize benefits generated for the business at the lowest long-term risks and costs.

Rationale
Decisions must not be made based solely on reaching lower solution costs. Every strategic decision must be assessed based on cost, risk, and benefit perspectives. Lower costs often represent greater risks and, perhaps, fewer benefits.

Implications

A solution must be selected based on a qualitative or quantitative cost, risk, and benefit assessment.

Most times, quantitative assessments are simpler based on cost perspective but more complex for risks and even more intricate for benefits. The quantitative assessment must always be conducted whenever possible and sufficient.

A qualitative assessment of one or two perspectives is sufficient when a quantitative assessment of other perspectives (for example, cost) is properly conducted and already leads to a decision.

Operating risks must be quantified whenever possible.

IT infrastructure must also be optimized based on business requirements and technological capacity to generate lower costs and risks, thus benefiting the focus of the company.

Principle 3. Business continuity

Description

Corporate activities must be maintained, despite system interruptions.

Rationale

As system operations become more inherent, we become more dependent of them. Therefore, we must consider the reliability of such systems throughout their entire conception and application. Business areas throughout the entire company must be able to continue conducting their normal activities, regardless of external events. Hardware failures, natural disasters, and lack of data integrity must not interrupt business activities. Business activities must be able to employ alternative mechanisms to convey information.

Implications

Dependence on shared applications implies that business interruption risks must be expected and managed in advance. Management includes, but is not limited to, periodic revisions, vulnerability and exposure tests, or designing mission-critical services to ensure continuity through redundancies or alternative resources.

Recoverability, redundancy, and maintenance must be approached at inception.

Applications must be assessed regarding criticality and impact on the company's mission to determine which continuity level is required and which corresponding recovery plan must be implemented.
Principle 4. Compliance with standards and policies

Description

Corporate information management processes must comply with all applicable internal policies and regulations.

Rationale

The information management corporate policy must comply with internal policies and regulations. This does not prevent improving corporate processes that conduct policy and regulation changes.

Implications

The company must ensure compliance with all internal policies and regulations regarding data conveyance, retention, and management.

It must inform and provide access to all applicable rules. Efficiency, need, and common sense are not the only incentives. Changes in standards and regulations might lead to changes in processes or application.

Principle 5. Adoption of the best practices for the market

Description

IT activities must always be aligned with the best practices for the market regarding IT governance, processing, and management.

Rationale

A company always strives to adopt the best practices from its industry in its business activities. A company's IT area must follow the same strategy to enhance business activities. The IT area must deliver projects and service-level agreements (SLAs) on progressively shorter deadlines and with increasingly higher quality within an effective cost-control process.

Implications

Best practices for IT disciplines must be identified and studied to implement them properly. These areas, among others, must follow best practices:

- IT processes must be certifiable and use established metrics.
- There must be a global risk perspective, focused on failure 0, and records of incidents and events.
- The management of IT costs per service (revenues and expenses), must be financially comparable to those of the market.
- IT management must be focused on indicators and a program perspective.
- Personnel must be increasingly qualified and motivated.
- The established IT architecture must be effectively applied in projects.
Information principles

Principle 6. Information treated as an asset

Description

Information is a valuable asset to the company and is managed based on this concept.

Rationale

Information represents a valuable corporate resource, with actual and measurable value. Information is the basis of the decision-making process. Therefore, it must be carefully managed to ensure constant awareness of its location, reliability of its contents, and access whenever and wherever necessary.

Implications

This is one of three closely related principles regarding information:

- Information is an asset
- Information is shared
- Information is easily accessible

The implication alludes to an awareness task implemented to ensure that all areas within the company understand the relationship between the value of information, sharing, and accessibility.

Principle 7. Shared information

Description

Users have access to information that is necessary for performance of their respective tasks. Therefore, information is shared between different corporate areas and positions, depending on the security levels established for that particular set of information.

Rationale

Necessary access to accurate information is essential to improve the quality and efficiency of the decision-making process of the financial institution. It is less expensive to maintain integral information in a single application and share that than to maintain duplicate information in multiple applications.

The company has plenty of information, but it is stored in hundreds of incompatible databases. The speed in which information is obtained, created, transferred, and absorbed is driven by the organization's capacity to effectively share these information islands throughout the company.

Shared information promotes better decisions because they are less dependent of less-reliable sources and information managed in the decision-making process.
Implications

To enable information sharing, a common set of policies, procedures, and standards must be developed and followed to regulate information management and both short-term and long-term access.

In the short term, to preserve a significant investment in existing systems, investments in software capable of migrating information from an existing system into a shared information environment are required.

Normalized data models and metadata that define such shared environments must be developed, in addition to a repository to store the metadata and make it accessible.

As existing systems are replaced, common information access and developer guidelines must be adopted and implemented to ensure that all information in new applications remains available in the shared environment.

In both short and long-term, common methods and tools to create, maintain, and access shared information must be adopted throughout the company.

Information sharing implies a significant cultural shift.

The information-sharing principle is constantly confronted with the information security principle. Information sharing must not compromise the confidentiality of information under any circumstance.

Shared information must be used by all collaborators to perform their respective tasks. This ensures that only the most up-to-date and accurate information is used in the decision-making process. Shared information shall become the only virtual source of corporate information.

Principle 8. Accessible information

Description

Information is accessible for users to perform their respective duties.

Rationale

Unrestricted access to information increases the efficiency and efficacy of the decision-making process, low response turnaround time for information requests and service deliveries. Employee time is saved and the consistency of information is enhanced.

Implications

Accessibility involves the facility with which users obtain information.

The manner in which information is accessed and made available must be sufficiently flexible to satisfy a wide array of corporate users and their respective access methods.
Access to information does not necessarily mean granting access privileges to users to modify or disclose it. This requires an educational process and changing the company's culture.

**Principle 9. Common terminology and data definitions**

**Description**

Data is defined coherently throughout the company, and definitions are comprehensible and accessible by all users.

**Rationale**

The data employed in the development of applications must have a common definition so that the data can be shared. A common terminology facilitates communication and promotes efficient dialogs. Additionally, data and interfaces must be shared among different systems.

**Implications**

We are inclined to believe that this issue is handled appropriately, since there are individuals with "data administration" functions and stated responsibilities. However, an additional significant energy is required, in addition to resources applied in this task. This is essential to develop the information environment.

The company must first establish a common terminology for business activities. Such definitions must be uniformly used throughout the company.

Whenever a new data definition is required, efforts regarding such definition must be coordinated and reconciled with the corporate data description "glossary." The company's data administrator needs to be responsible for such coordination.

Ambiguities arising from multiple data definitions must be replaced by a definition that is accepted and understood by the entire company.

Several data normalization initiatives must be coordinated.

Functional data administration responsibilities must be assigned.

**Principle 10. Information security**

**Description**

Information is protected based on integrity, availability, confidentiality, incontestability, and authenticity. Every piece of information is submitted to a security assessment based on those five factors.

Security traceability includes proper inception and application of the auditing system and monitoring tools.

**Rationale**
Open information sharing and disclosure must be balanced with the need to restrict the availability of confidential, proprietary, and sensitive information.

Current laws and regulations require data privacy and, simultaneously, allow free and unrestricted access. Temporary information (ongoing projects for which disclosure is still not authorized) must be protected to prevent unjustified speculation, misinterpretations, and improper use.

**Implications**

The addition of confidential and non-confidential data requires "de-confidentiality" analyses and procedures to maintain proper control. Data proprietors and functional users must determine whether the addition increases the level of confidentiality. Adequate policies and procedures to handle such revision must be implemented, including for the "de-confidentiality" process.

Current practices that involve the use of separate systems for different confidentiality levels must be reconsidered. Is there a software solution to separate confidential and non-confidential data? It is more expensive to manage non-confidential data in a confidential system. Currently, the only way to combine both is to place non-confidential data in the confidential system, where it remains.

To provide appropriate access to open information yet maintain security, the security restrictions must be identified and implemented at the data level, not at the application level.

Data security can be applied to restrict access to read-only or no-reading statuses. Sensitivity labels must be established for access to temporary, decisive, confidential, sensitive, or proprietary information.

Security must be planned in data elements from the beginning, rather than added later. Systems, data, and technologies must be protected against unauthorized access and handling. The source of information must be protected against unauthorized or accidental modifications, fraud, catastrophes, or disclosure.

Information must be rated regarding the five factors established in this principle. It is essential to quantify the financial impact of violating each one for more critical information.

**Application principles**

**Principle 11. Technological independence**

**Description**

Applications do not depend on specific technological options and, therefore, can function on different technology platforms. The IT architecture must be planned to reduce the impact of technological changes in the business.

**Rationale**
The independence of technological applications allows them to be developed, adapted, and operated under the best cost-to-benefit ratio. Alternatively, technology (which is subject to supplier dependence and obsolescence) becomes the users' motivation, rather than their requirements.

This principle is based on the concept that each IT decision renders us dependent of such technology. The purpose of this principle is to ensure that the software is not dependent on specific operating system software or particular hardware.

**Implications**

This principle requires standards that support portability, which are often called *open standards*.

Application program interfaces (APIs) must be developed to integrate existing applications with operating environments and applications developed based on the enterprise architecture.

Middleware must be employed to disassociate applications from specific software solutions.

**Principle 12. Easy-to-use applications**

**Description**

Applications are easy to use. The technology is transparent to users, so it enables them to concentrate on their tasks, rather than on system operation issues.

**Rationale**

The more that users need to understand the technology employed, the less productive they will be. The easy-to-use concept is a positive reinforcement for using applications. It encourages users to work within the integrated information environment rather than developing isolated systems to perform tasks outside of the integrated corporate environment. Most of the knowledge required to operate systems is very similar. Formatting is limited to a minimum, and system misuse risks are low.

Using an application must be as intuitive as driving a car from another brand.

**Implications**

All applications must have the same appearance and layout. Thus, a standard layout must be developed and usability testing criteria must be implemented.

**Principle 13. Component reusability and simplicity**

**Description**

The enterprise architecture is built over low-coupling, reusable, modular components that implement services.
Systems architecture must be as simple as possible to maintain yet meet all business and corporate requirements. Whenever complexity is required, it must be encapsulated to promote simplicity of solutions built on the architecture.

Rationale

Reusable components represent opportunities to reduce IT development times and costs. Reusable components leverage investments in current systems. Modular components increase the systems' capacities to adapt to different evolution needs, because the change is isolated from affected modules.

Implications

The architecture establishes standards and guidelines to develop system components.

Principle 14. Adaptability and flexibility

Description

IT systems are conceived to generate change, and they reflect alterations in laws, social needs, or other types of changes.

Adaptability and flexibility reduce the complexity and promote integration, which improves the company's business activities.

Excessive customization increases costs and reduces the ability to adapt.

Rationale

Adhering to this principle has several benefits:

- Allows the infrastructure to support changes that frequently occur in business processes within the company.
- Renders the infrastructure more adaptable to IT changes and IT market strengths.
- Allows the improvement of business processes.
- Promotes a simpler and faster system integration process, with less revision processes
- Allows systems to evolve to meet business needs and changes

Complex systems with several data and transactional functions are difficult to manage and make changes extremely risky.

The goal is to avoid dependency failures that can result from highly coupled applications.

Implications

Initially, the systems might require more time to conceive and greater systemic consideration as operations go beyond the systems' traditional boundaries.

Initial costs might be higher, but the integration process will be less expensive.
Systems will last longer; therefore, the return will be greater.

A system can be suboptimal in the short-term but present optimization gains in the long term.

Adaptability and flexibility performance metrics must be established.

The development of applications based on components must be promoted and facilitated.

A minimum number of suppliers, products, and configurations must be maintained to allow maximum flexibility when implementing changes.

Excessively complex configurations of components, undue customized tuning, and hardware and software customization based on transient, local, or other conditions must all be avoided.

The discipline of configuration must be maintained, sacrificing performance and functionality in some cases.

Resource restrictions must be considered.

**Principle 15. Convergence with the enterprise architecture**

**Description**

The convergence with the enterprise architecture is promoted in the right time, and in line with the company’s investment strategy.

The convergence with the enterprise architecture takes place as new applications are built, new technologies are implemented, and older systems are updated or decommissioned. Exceptions to the enterprise architecture might be supported for specific cases if there is a consensus that the benefits of using a solution from a specific technology exceed those arising from the adoption of the enterprise architecture.

**Rationale**

Convergence offers several advantages:

- It allows the enterprise architecture to evolve and accommodate changes in business and technologies.
- It avoids conversions of obsolete systems, which are extremely expensive.
- Over time, it preserves the investment while promoting the benefits of the enterprise architecture.

**Implications**

Delayed convergence could reduce the benefits of the enterprise architecture.

Convergence requires a realistic and tangible approach to migration to the enterprise architecture.

It requires an explicit transition strategy for current systems after the target technology is identified.
Allows decommissioning a system sooner when that is appropriate.

Convergence does not allow waiting indefinitely. It requires a business case for exceptions, an exception process, and an exit strategy. It must establish temporary or permanent exceptions, as well as exit strategies for temporary exceptions.

Convergence requires sponsorship to replace obsolete technologies.

**Principle 16. Enterprise architecture also applies to external applications**

**Description**

As new outsourcing contracts and agreements are entered into, they must reflect and incorporate the enterprise architecture principles.

This is one of the ways to keep enterprise architecture in line with the business. Outsourced activities must not be exceptions to the enterprise architecture simply because they are outsourced.

**Rationale**

To be successful, enterprise architecture must be integrated with all stages of IT projects: inception, planning, and acquisition.

**Implications**

Procurement areas must receive enterprise architecture training

This requires partnerships and efficient communication between business, acquisitions, contract management, and IT areas to get the benefits offered by the enterprise architecture.

IT acquisitions must include requirements based on the enterprise architecture.

The investment vision for the business must include IT requirements.

**Principle 17. Low-coupling interfaces**

**Description**

Interfaces have low coupling, are self-described, and offer low impact on the financial institution in case of changes.

**Rationale**

Low-coupling interfaces are preferable, because when interfaces between independent applications are highly coupled, they are less generic and more susceptible to causing unwanted, secondary effects when they are changed.

**Implications**
Low coupling means that the services (corporate APIs, for example) are conceived with no affinity to a certain service consumer. Therefore, the service is completely uncoupled to a service consumer. However, the service consumer is dependent of the service (that is, contains references for service interfaces).

The service is also responsible for exception treatment. The result is a low-coupling architecture.

**Principle 18. Adherence to functional domains**

**Description**

The business rules and functionality of a system are consistent with the mission of that system. There is complete adherence to the functional domain in which the system is located.

**Rationale**

The purpose of this principle is to avoid functional redundancy between systems. Functional redundancy can cause loss of data integrity and increase maintenance costs related to the redundant business rule.

**Implications**

Systems must be located in proper functional domains, with explicit definition of the manager in charge of the functional domain.

Each new functionality request must be submitted to the respective manager.

Applications that are already in production with functional redundancy should be replaced entirely or partially in a timely manner. The functional redundancy of such applications must not be promoted.

**Technology principles**

**Principle 19. Changes based on requirements**

**Description**

Changes in applications and technologies are implemented only to meet business needs.

**Rationale**

This principle promotes an atmosphere where the information environment changes to reflect business needs, rather than changing the business to reflect IT changes. This ensures that the business operation is the basis for any change proposal.

Involuntary effects on businesses resulting from IT changes are mitigated.
Technology changes can generate opportunities to improve the business process and, subsequently, alter business needs.

**Implications**

Changes in implementation follow a complete assessment of proposed changes, based on the enterprise architecture.

A system development or technical improvement is not implemented unless there is a documented business need.

A business need must be considered, but it must also be aligned with other enterprise architecture principles. There must be a balance between business needs and IT operations.

**Principle 20. Control of technical diversity and suppliers**

**Description**

Technological diversity is controlled to minimize significant costs related to the maintenance of expertise and connectivity between several different processing environments.

Supplier management must focus on the lowest number of suppliers possible to meet business needs and reduce risks.

**Rationale**

There is a real and significant cost related to the infrastructure required to support alternative technologies for processing environments. There are other infrastructure costs to maintain the architecture of multiple interconnected processors.

Limiting the number of supported components and suppliers simplifies and reduces maintenance and management costs.

A smaller number of suppliers and software packages represent a greater ease and lower integration costs.

Business advantages of minimum technical diversity include:

- Standard component packaging
- Predictable implementation impact
- Predictable returns and validations
- Defined tests
- Greater flexibility to accommodate technological advances

A common technology throughout the entire company generates scalable economic savings for the company. Technical management and support costs are better controlled when limited resources focus exclusively on this shared technology set.
Implications

Policies, standards, and procedures that regulate the acquisition of technology or contracting with new suppliers must be directly bound to this principle.

Technology decisions are guided by the technological blueprint.

Procedures to increase the set of acceptable technologies to meet evolved requirements must be developed and implemented.

This principle does not require freezing the technological baseline. Technological advances are welcome and incorporated into the technological blueprint when they are compatible with current infrastructures, are likely to improve operating efficiency, or there is a need to increase capacity.

The selection of contracted suppliers must be a strategic decision, always considering other types of services that could be provided by the same supplier.

Principle 21. Interoperability

Description

Software and hardware must follow established standards that promote data, application, and technology interoperability.

Rationale

Standards help ensure coherence, thus improving the ability to manage systems, raise user satisfaction, and protect current IT investments, thus maximizing return on investment and reducing costs.

Interoperability standards also help ensure support from several suppliers to their respective products, thus facilitating integration.

Implications

Interoperability and industry standards must be followed unless there is a mandatory business reason to implement a non-standard solution.

A process to establish standards, periodic revision, and exceptions must be established.

Current IT platforms must be identified and documented.

Summary of the principles

General principles

1. IT and business alignment
2. Maximum benefits at the lowest cost and risk
3. Business continuity
4. Compliance with standards and policies
5. Adoption of the best practices for the market

**Information principles**

6. Information treated as an asset
7. Shared information
8. Accessible information
9. Common terminology and data definitions
10. Information security

**Application principles**

11. Technological independence
12. Easy-to-use applications
13. Component reusability and simplicity
14. Adaptability and flexibility
15. Convergence with the enterprise architecture
16. Enterprise architecture also applies to external applications
17. Low-coupling interfaces
18. Adherence to functional domains

**Technology principles**

19. Changes based on requirements
20. Control of technical diversity and suppliers
21. Interoperability
Related topics

- For more information related to this article, check these resources:
  - The Open Group Architecture Framework (TOGAF).
  - Service virtualization - Financial services, IBM video on YouTube (1:15)
- Download a free trial version of Rational software.
- Evaluate other IBM software in the way that suits you best.
- Try building and deploying your next project on the IBM Bluemix cloud platform, where you can take advantage of pre-built services, runtimes, frameworks, application lifecycle management, and continuous integration.

© Copyright IBM Corporation 2012
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)