April 2025

Best Practices in Artificial Intelligence

The User's Perspective on Information Systems Governance

The success of an IT application depends largely on the implementation of best practices. This is particularly the case for systems based on Artificial Intelligence. They are not fundamentally different from other applications, but they are more complex, and above all, their results are sometimes astonishing. They often seem like miracles. But, beyond their specificities, they are information systems based on IT architectures like any other, and as such, it is important that they adhere to a certain number of best practices common to all information systems; this is information systems governance.

The areas concerned are:

- System design and functionality,
- Development and testing,
- Production and MCO (maintenance under operational conditions).

Best practices for AI-based applications must comply with those of traditional IT, as identified by COBIT and the following quality standards: CMMI and ITIL. These practices particularly concern information systems governance, and a list of these best practices has been compiled by the European Club for Information Systems Governance (see appendix below). In addition to these lists, there are a few best practices specific to AI. Please note: these apply to all AI-based systems but do not include generative AI applications. They will be the subject of another document that we will prepare when we have sufficient experience.

Importance of general best practices, particularly regarding the design and implementation of Artificial Intelligence

Like all major developments, AI-based systems require significant design and implementation efforts, and they also involve risks that must be managed. Added to this is the fact that most of these operations involve multiple company entities. For these reasons, it is necessary to manage these operations as corporate projects.

However, observation shows that too often, AI-related operations are not managed in project mode. This attitude is probably due to the belief that these developments are simple, easy to implement, and always profitable. This overlooks the fact that these are always complex operations, involving multiple people or departments, that implementation and implementation times are often long, and that it is often necessary to organize deployments, particularly the training of future users. As can be seen, the risk level is quite high.

These measures address three key points:

- An Artificial Intelligence project is always a business project. It must be managed in project mode, a steering system must be put in place, and sufficient operational control must exist.
- Before deciding to implement an Artificial Intelligence-based system, it is imperative to conduct a study to assess the scope of the future system, its feasibility, and its profitability.
- The economic study must assess the value creation induced by the Artificial Intelligence-based system. To achieve this, it must be comprehensive. It must at least include:
    - The impact of the future system on productivity (doing the same thing with fewer resources) and efficiency (performing more operations with the same resources).
    - Evaluate the amount of investment, particularly in research, development, and implementation. - Estimate the system's operating costs during regular operation.
    - Calculate the return on investment.

The design, development, and implementation of an AI-based system is always an investment, even when it involves the simple implementation of seemingly simple functions.

Securing the User of Artificial Intelligence

The FutureTech of CSAIL at the Massachusetts Institute of Technology (MIT) has created a database in the AI Risk Repository listing more than 700 cases of AI systems that have encountered difficulties and allowing for an objective assessment of the potential risks of these applications. The three most common risk factors are:

- The security and robustness of AI systems (76%),
- Unfair prejudice and discrimination (63%),
- Compromise of privacy (61%). A particular effort must be made to implement good practices to significantly reduce the importance of These three risk factors.

Enhance Reliability of User Relations

1. Inform the user that they are in contact with Artificial Intelligence

    As soon as the user connects to any AI-based system, a clear message must inform them that they are in contact with an AI system. This information is independent of the nature of the application and the system on which it runs: PC, tablet, smartphone, local or remote server, cloud, etc. The message must be written in the user's language, and an audio message must be available for the visually impaired.

2. Human Control of AI-based Systems

The user must be able to interrupt AI-based processing at any time using a red button that is accessible at all times. The system state is then saved, and if the user wishes, they can resume processing at any time from where they left off. It must also be possible to launch a new process with new parameters.

3. Respect for privacy, particularly regarding information communicated to the AI-based system

Personal information entrusted to an AI-based system, including identity and banking information, must be inaccessible to any other person. This data must be stored on a secure site and must be encrypted.

A security audit and, if necessary, stress tests of the AI-based system must be conducted periodically. The latest security auditor's certificate must be accessible online.

If personal data must be transmitted by the system to a third party, this may only be done with the user's explicit consent.

When personal data entered passes from the user's workstation to the AI-based system, it must also be end-to-end encrypted. The same applies to data transmitted to third parties. A confirmation message confirming receipt of this data must be sent by this third party.

If personal data is not secure or is only partially secure, or if security tests have not been performed or have revealed weaknesses, the system must be declared untrustworthy and, in this case, it must not be made available to a large, uninformed public.

4. Transparency of operations.

At any time, the user of an AI-based system must be able to know where they stand and, to this end, must be able to view the history of transactions they have performed. All previous transactions and the results obtained must be available to the user. Only the user who entered the data can view it. They can modify the data they entered, and if necessary, a new processing operation can be restarted. Under no circumstances can a third party view this information.

In technical terms, this requires a transaction log: see point 19 below.

5. Possibility of human processing

In the event of difficulty, the user must be able to request human assistance, including remote application setup. Of course, this requires that the workstation and the AI-based system be connected to a network.

The user must be able to express themselves in their own language and receive responses clearly and distinctly. The system must offer audio in several languages or, failing that, provide a written exchange with automatic translation.

If the system is a standalone system, a phone number must be displayed and callable using a standard telephone (landline or mobile) at the rate of a local call. If this is not possible, it must be indicated in the initial message indicating that the system does not have a phone number.

This support must be systematically evaluated ex-post, including response times to user requests (call pick-up, duration of dialogue, actual restart) and the quality of the support provided.

6. Explainability of Decisions Made

Most AI-based systems are required to make decisions. These decisions must be explainable by the system. If it cannot justify its decisions, it must be declared unreliable and not made available to a large, uninformed public.

In the event of a dispute, the user must have access to a complaints procedure offering the opportunity to communicate with a human being.

7. Explainability of Algorithms

An Artificial Intelligence-based system relies on a number of algorithms. They must be clear and understandable.

Sensitive, and sufficient documentation must be available and accessible to all users. This documentation must be periodically updated.

Some algorithms may be protected by trade secrets, especially if they are not protected by patents. In this case, the relevant part of the documentation is only accessible to developers, decision-makers, and authorized auditors, and simplified documentation must be accessible to all users.

Generally speaking, it is recommended to have, alongside technical documentation, lightweight, easy-to-read documentation for users.

8. Equal treatment of individuals without possible discrimination

It is essential to ensure that the AI-based system treats all individuals equally, regardless of their origin, gender, religion, etc. It must comply with the Charter of Fundamental

Rights of the European Union (1) and applicable national non-discrimination legislation. Absence of bias tests must be conducted regularly (see point 20 below).

Particular attention must be paid to complaints from users complaining of being discriminated against by the system.

9. Train users to be critical of results

Users must be informed that an AI-based system can make errors and that it is advisable to perform checks.

Clear messages must appear on the screens displayed by the system, particularly when presenting results.

The system provider must provide users with a video teaching them how to ensure the accuracy of the results displayed, using simple examples showing how simple checks can help them ensure the quality of the answers. If users find a result questionable, it is important to instruct them to send a message to the system administrator with a copy of the disputed results.

When the AI-based system is integrated into a more complex system, such as a self-driving car or an industrial robot, the nine points above must be adapted to these specific contexts.

A Reliable and Managed System

It is important to ensure that any information system, whatever it may be, is reliable and managed. Likewise, the IT architecture enabling its operation must be mastered. In the case of AI-based systems, given the challenges and risks, the level of requirements is higher than for traditional management systems. This justifies strengthening the best practices to be implemented.

10. Governance of Data Feeding the AI-based System

AI-based systems require data to function, particularly systems based on deep learning. To do this, one or more databases will be created to configure the future system.

The quality of this data is fundamental. To ensure this, it is necessary to perform a few checks:

- Verify the origin of this data. This often allows you to assess its quality and exercise caution when its origin is suspect.

1 - Article 21: “Any discrimination based on, in particular, sex, race, color, ethnic or social origin, genetic characteristics, language, religion or beliefs, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation is prohibited.”

- Verify that the file or database is exhaustive, and if it is not, ask why not.
- This data is then cleaned. All suspect or suspected information has been eliminated, and some values may have been replaced with estimates. This cleaning can be done manually or automatically. It is important to ensure that this cleaning has been done in a reasonable manner without degrading the quality of the data.

To configure the system, this data often needs to be indexed. For example, in the case of a photo-based pattern recognition system, it is necessary to write a label for each image. This work can be done manually or more or less automatically.

The quality and effectiveness of AI-based systems directly depend on the quality of the training data.

11. Have a clear procedure for qualifying training and testing data

It is very important to ensure that the dataset used to train the system is not used for testing. If this is the case, the tests will not be effective because they will not detect potential anomalies.

The databases used to train AI-based systems and those used for testing must be qualified. To achieve this, it is necessary to implement an efficient and rigorous process. A written procedure must describe this process and allow for ensure the quality of these operations.

12. Have diverse development and testing teams

Experience shows that "one-size-fits-all" teams sometimes make mistakes because all their members think and react the same way. To avoid this, it is recommended to form development and testing teams that include people with diverse backgrounds. This particularly concerns the presence of women, users, "literary" people, etc., in the project team.

13. Have a procedure for reporting and handling anomalies and errors

Anomalies and errors can occur even in well-established AI-based systems. Users notice that the system gives a strange, inadequate, or downright false response. They must be able to report the anomaly they observe to the manager responsible for operating the system. To this end, it is useful to be able to save the screen(s), the IT context (the log of previous transactions), and the user's observations or questions.

This user feedback detection procedure has several advantages. First, it allows us to understand the difficulties encountered by users. This makes it possible to identify possible improvements. And, of course, it is also useful for detecting bugs that need to

be fixed. Statistics on incidents and their causes should be periodically compiled.

Among user complaints, there are those from people who feel they are victims of gender or racial bias, etc. Particular attention should be paid to these complaints, and checks should be carried out to ensure whether they are real or imaginary.

Important point: it is important to respond to all user messages, regardless of their nature. This can be done within the application or by email.

14. Ensure the technical robustness of the system

It is important to verify the robustness of the system. This is done by analyzing the frequency of incidents and their severity. But this is not enough, especially when launching a new AI-based system into production. To assess the system's robustness, it is recommended to perform stress tests.

To do this, the application will be subjected to:

- Abnormal data entries, all of which must be rejected,
- Degradation of the parameter databases to ensure that the system automatically detects and rejects them,
- The ability to simultaneously launch large volumes of normal transactions, as experience shows that certain anomalies appear when the system is close to saturation,
- Unexpected shutdowns of operations in progress to observe the conditions under which the system restarts,
- ….

It is recommended to perform these tests automatically on a test machine and avoid performing them on the production system. It is good practice to periodically repeat the tests to ensure that the application does not degrade.

15. Have a real-time control station for all the activity of each AI-based system.

To monitor the activity of an AI-based system, it is recommended to have a PC that can monitor its operation in real time and, if necessary, intervene. Many indicators can be monitored, including:

- The number of users connected at a given time,
- Average response time,
- Queue length,
- Number of transactions processed per second,
- Anomalies detected,
- Number of tasks left pending,
- Number of user messages received,
- ….

In the event of a system crash, the operator must have all the information at the control station to understand what is happening and, if necessary, be able to initiate actions to return the situation to normal.

A responsible and competent person must be designated to monitor the system and intervene if necessary. If the system operates 24 hours a day, it is necessary to organize accordingly. To facilitate monitoring and these interventions, it should be possible to relocate the control station to a laptop or tablet running 5G.

In the case of a single-user AI-based system, a control station is not necessary; however, it is useful to have some statistics to understand what is happening in the event of system degradation or failure.

16. Periodically assess the security level to ensure it is sufficient.

Given the challenges associated with the application and the degree of confidentiality of the information entrusted to it, it is necessary to:

Periodically ensure that the objective security level is met.

These checks can be performed by the system operator, but for reasons of prudence, it is preferable to entrust them to an external third party. It is necessary to ensure that they have IT auditing skills.

Points to check include, among others:

- Management of system access authorizations,
- The effectiveness of login controls,
- The possibility of circumventing these controls (existence of bypasses, widely distributed and known access codes, etc.),
- The existence of a connection history,
- Encryption of transactions, particularly from remote workstations,
- Encryption of stored data, particularly personal information,
- The impossibility of viewing transactions made by a third party,
- Data backup on a remote computer system,
- The system's disaster recovery capability,
- …

It is recommended to perform these security checks at least once a year. 17. Have a periodic test schedule for the entire system

Maintenance must be monitored because this information can sometimes lead to degradations in system performance. For this reason, it is good practice to monitor maintenance operations and emergency interventions. To this end, it is recommended to

have a procedure for recording maintenance requests, tracking modification operations, and conducting tests prior to production launch.

It is also necessary to periodically schedule a series of tests to assess the quality of controls and processing, as well as system performance, in order to detect any potential system degradation.

To achieve this, it is necessary to have a standard test set stored on a test machine, onto which the programs to be tested and operational data are previously copied. If possible, the test machine should have the same configuration as the production machines. Where possible, the tests should be able to run automatically. Another precaution: the test machine must be disconnected from the network during testing.

18. Have a medium-term audit program

A system based on artificial intelligence, particularly if it is widely used and intended for a non-technical audience, must be subject to a periodic audit.

It is prudent to conduct an audit before the application is put into production, and then it is recommended to conduct a periodic follow-up audit. The timing depends on several factors: the level of stakes, the significance of the risks, the number of potential users, the application's visibility, risk aversion, and the reputation of the company putting the application into production. Generally, this type of general audit is performed every 2 or 3 years.

It is recommended that these audits be entrusted to a professional IT auditor, who is, if possible, familiar with artificial intelligence best practices. At the end of the mission, the user will submit a report including recommendations for improving the operation of the AI-based system.

19. Need for a transaction log

To track operations and, in the event of a problem, understand what happened, it is essential to keep track of them. This requires recording all transactions. Technicians call this type of system a log. It is possible to limit yourself to recording only the data entered and the results returned, but it is possible to go further and record intermediate processing. However, this must be done reasonably, as the volumes to be stored can become very large.

To view the history, it is advisable to have a program for formatting this data. It must be possible to search for information on a particular transaction or a specific group of transactions.

To avoid having excessively large histories, it is necessary to provide a function for

purging this data.

20. Have bias detection tools available

Every system has biases. Even humans have biases, and some are unconscious. However, in the case of artificial intelligence-based systems, they can lead to deviations that can have significant consequences. The most serious are gender or racial biases. To avoid these, it is necessary to implement bias detection tools.

These are essentially statistical programs that allow you to compare the percentages of results for two distinct populations, for example, the hiring of men and women for a given position. All you need to do is compare hiring rates to assess the significance of gender bias.

As we can see, it is essential to ensure that best practices are implemented, otherwise AI-based systems will drift. Ms. Virgina Dignum, a computer science professor in Sweden and UN consultant on the development of Artificial Intelligence, observes: "Artificial Intelligence is a car without brakes, driven by a driver without a license, on a street without traffic signs."

List of General Best Practices in Information Systems Governance

1 – Governance in Information Systems Design

1. 1 Ensure the integration of the future information system into the company's strategy.
1. 2 Evaluate the value creation of the information system.
1. 3 Design the information system architecture.
1. 4 Integrate into the existing architecture.
1. 5 Manage the project in project mode.
1. 6 Place great importance on organization.
1. 7 Define the overall design in two stages.
1. 8 Write a reference document.
1. 9 Identify functions and processes.
1. 10 Take into account the specific role played by the IT system.
1. 11 Involve those affected by the future information system in its design.
1. 12 Start with the existing system and develop it.
1. 13 Designate an information system manager.
1. 14 Choose an appropriate architecture.
1. 15 Comply with internal control rules.
1. 16 Assess and monitor risks.
1. 17 Define appropriate security measures.
1. 18 Calculate the investment amount.
1. 19 Monitor project progress.
1. 20 Track invested expenditures.
1. 21 Estimate the projected operating costs of the information system.
1. 22 Evaluate the return on investment.
1. 23 Give company management a key role.
1. 24 Have the project validated by all stakeholders.
1. 25 Establish an information system project dashboard.

Chapter 2 – Governance in Information Systems Operations

2. 1 Designate an information system manager.
2. 2 Monitor the entire information system.
2. 3. Feed a database recording all operations to create a dashboard of information system activity.
2.4. Track the details of operations.
2.5. Ensure the security of operations and databases.
2.6. Periodically audit the information system.
2.7. Record all incidents and forced access attempts.
2.8. Record all anomalies that occur.
2.9. Track any anomalies that occur.
2.10. Verify the contents of databases.

2.11. Manage information assets.
2.12. Implement sufficient controls.
2.13. Perform specific controls on sensitive transactions.
2.14. Establish an internal control dashboard for the information system.
2. 15 Document the information system.
2. 16 Have a written procedure.
2. 17 Measure significant performance indicators.
2. 18 Measure productivity indicators.
2. 19 Monitor the overall cost of the information system.
2. 20 Calculate the average cost per unit produced.
2. 21 Work on unit costs.
2. 22 Analyze the details of the operations performed.

Chapter 3 – Governance in Information System Management

3. 1 Designate an information system manager.
3. 2 Have a consensus decision-maker, recognized by the other relevant decision-makers.
3. 3 Ensure the manager has sufficient authority.
3. 4 Appoint a responsive person.
3. 5 Have a suitable management body.
3.6 Report periodically.
3.7 Establish a dashboard.
3.8 Implement a problem escalation procedure.
3.9 Prevent conflicts from arising and address them as soon as they arise.
3.10 Track incidents.
3.11 Consult periodically with users and decision-makers to identify the development requests they wish to implement.
3.12 Select requests based on simple criteria.
3.13 Plan changes.
3.14 Practice delegation of authority.
3.15 Follow the schedule and measure progress.
3.16 Forecast and monitor workload.
3.17 Set and monitor the operating budget.
3.18 Verify the impact of changes.
3.19 Periodically conduct an information system assessment.
3.20 Evaluate the value created by the process.
3.21 Manage risks.
3.22 Manage security.
3.23 Ensure compliance with internal control rules.

Chapter 4 – Governance in Information Management
Information System Development

4.1 Designate a leader for information system developments.
4.2 Have a medium-term vision for the information system.
4.3 Write a guidance document.
4.4 Have these guidelines validated.
4.5 Define a cycle and frequency for information system development.
4.6 Stabilize the information system scope.
4.7 Validate extensions or reductions to the information system scope.
4.8 Periodically consult users and decision-makers to identify development requests they wish to implement.
4.9 Select development requests based on simple criteria.
4.10 Plan changes.
4.11 Monitor the schedule and measure progress.
4. 12 Forecast and monitor the workload.
4. 13 Set and monitor the operations budget.
4. 14 Manage major changes in project mode.
4. 15 Prepare the work to be done.
4. 16 Evaluate the necessary workload and set the budget.
4. 17 Set priorities.
4. 18 Set deadlines.
4. 19 Improve the IT system.
4. 20 Have the changes made tested by people who regularly use the information system.
4. 21 Have a testing platform.
4. 22 Update the IT system documentation.
4. 23 Improve the existing organization.
4. 24 Update the procedure note.
4. 25 Provide written instructions to those using the information system.
4. 26 Train those involved with the information system.
4. 27 Subsequently evaluate the information system.
4. 28 Set a date for the next review.

For more details, read the document: https://www.cegsi.org/index.php/documents/les-bonnes-pratiques-en-matiere-de-gouvernance-de-systemes-d-information/les-bonnes-pratiques-en-matiere-de-gouvernance-des-systemes-d-information

To download the full text: https://www.cegsi.org/index.php/documents-a-telecharger/category/autres-documents