

# Agile Manifesto for Internal Audit

Disponibile anche in italiano  
[www.isaca.org/currentissue](http://www.isaca.org/currentissue)

The internal audit process is often regarded as a formal and bureaucratic activity necessary for compliance. But sometimes, due to lack of flexibility, it is distant from the enterprise's value creation operating cycle. Even the adoption of practical and efficient tools in audit tests, such as robotic process automation (RPA),<sup>1</sup> does not serve to change the perception that internal auditing is a process imposed to spy on daily work. Changing that view is possible, but it requires a significant reinterpretation of the audit process with strict adherence to audit management methodologies and founding principles. An audit should not be imposed as a tool of judgment to hand out punishments. Instead, it should be presented as a useful support tool for achieving business objectives through integration, cooperation and adaptability—words that are likely to lay the groundwork for change.

Over time, the internal audit process has undergone adjustments that have led to its current independent control role in the organization. Its position as the third level of defense is now indisputable in the context of achieving business objectives. The first level of defense requires a structured set of operations to implement actions necessary to guarantee the results expected by the business. The second level requires controls for the systematic verification of performance. The third level guarantees that the operating and control mechanisms are aligned with objectives.

Just introducing the internal audit function to the organization, regardless of the importance placed on it, is not enough. It is necessary to clarify the role of the audit process to entities to be audited so that its purpose is clear, and it is never identified as the prelude to sanctions. A negative image can affect the performance of the audit program.

To investigate how to change the image of the audit process and improve the way an audit is perceived and conducted, it is useful to conduct a gap analysis. The first step is to list the negative aspects of the

current state by identifying shortcomings that are typically listed during an audit. Then, based on the definition of internal audit, the predominant concepts to identify the desired state can be determined.

Finally, through a series of considerations, balancing needs that emerged to achieve the desired state from the current one, it is possible to derive a series of principles to follow as improvement points for effectively modeling the process. Principles represent individual subprocesses that provide intermediate results to be achieved. The same idea is found in Agile<sup>2</sup> methodologies, where the main process is



**LUIGI SBRIZ** | CISM, CRISC, CDPSE, ISO/IEC 27001 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

Is a lead auditor and a senior consultant on risk management, cybersecurity and privacy issues and has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously, he was head of information and communications technology operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia). Before that, he was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging an operational risk analysis with a consequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and system integrating a risk monitoring maturity model with internal audit. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn at [www.linkedin.com/in/luigisbriz](http://www.linkedin.com/in/luigisbriz) or <http://sbriz.tel>.

---

## The need for independent judgment does not require distancing the audit process from other business processes.

---

separated into a sequence of simple objectives, with fast implementation and subsequent evaluation of the result to allow for adjustments.

### Audit Aspects Perceived as Negative

Focusing on negative beliefs serves to illuminate the weaknesses of the audit process image. It does not mean those beliefs are valid, but negative perceptions can create just as much risk as negative facts. It is important to know those negative perceptions to understand which demand action and to be able to respond to them effectively, so they do not hinder the audit process. For example, if an organization imposes an internal audit to expose lack of compliance rather than to improve its internal culture, there could be negative consequences.

Recurring negative comments directed toward auditors from auditees include:

- They are only making theoretical observations.
- This has never happened before.
- These recommendations hinder productivity.
- They do not understand our reality.
- The audit is an abstract vision of our processes.
- We do not understand why they are checking right now and right here.
- Now we are burdened by deadlines.
- The production priorities should come first.
- This is not the right time.
- This control is a waste of time.
- We do not understand how this is helpful.
- Our needs have not been considered.

These types of observations are symptomatic of the impaired bond between internal audit and the realities of production. These comments could describe an uninvited stranger entering the house and demanding things without an apparent reason and without providing any form of compensation for the disorder

caused. Perhaps the most disagreeable feeling for an internal entity is to be considered a stranger. When recognition of an individual as part of a system or business operation is missing, then a person who could have played the role of a facilitator is likely to become an obstacle instead.

### Purpose of the Internal Audit

When there is a sense of distance between auditors and staff, and when objectives are clearly different, operational processes can be affected reflecting the misalignment between expectations and reality. This result is the opposite of the intent described in the definition of internal audit.<sup>3</sup> Its expected strengths are clearly evident in the enunciation of objectives and in the perimeter of its application.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, controls and governance processes.<sup>4</sup>

According to this definition, the audit process with respect to the controlled entity is independent—it has no common interests, it is objective (based on concrete facts), and it provides advice. Further, it creates value by providing knowledge and competence and by focusing on the facts in the right context. The concepts incorporated in the definition must not change. It is the process of achieving them that must be adapted to the life cycle of the enterprise. This must not be a rigid process, based exclusively on some preestablished business processes or on an audit plan that relies on an aging policy. The selection of the entity to be audited and the tests to be carried out must be modeled to align with the current business environment and the organization's risk profile.

Decisions on the audit process that are derived from general and unsuitable frameworks and repeated in an identical way over time risk ineffectiveness of the control system and, therefore, cannot produce the expected benefits.

The quality of an audit process is not proportional to the quantity of checks or tests performed. Adding a new control does not add value if the control is not justified by a pragmatic risk analysis. Understanding

the level of risk culture in the organization is necessary to obtain realistic assessments.

## Independence vs. Integration

The need for independent judgment does not require distancing the audit process from other business processes. The ability to carry out an objective evaluation by means of evidence rather than hasty preconceived judgments is all that is required. This ability is not altered by interacting with the processes to be controlled to respond to specific operational needs—for example, to ensure that risk analysis is reliable or to verify that the process is aligned with its requirements.

The ideal interaction is achieved through a request from those operating the processes to be verified (not mandated by the audit plan). This leads to a positive interaction, characterized by the implicit recognition of merit in the audit process, creating the conditions for integration between processes. The benefit for the audit process is the enhancement of its image as a resource that is useful for improving business processes.

## The full value of the audit opinion cannot be realized if it does not align with the pace of the business.

### Objectivity vs. Evidence

The need to create objective evidence does not require giving up the performance of less complex and therefore more frequent automatic tests that are:

- Aimed at specific, limited and well-defined areas
- Recurrent or systematic
- Carried out without the formal participation of the entire audit team

The performance of these tests can help create a perceptible—but not hostile—presence. A disciplined approach that carefully attends to the needs of the business and focuses on the risk events reported can promote a climate of trust and build tolerance for the increased presence of auditing in the field and the perceptible usefulness of the control action.

Still, the collection of evidence cannot be entrusted exclusively to sample tests based on an established plan and conducted by an audit team. Monitoring techniques with many simple and systematic checks are as capable of producing reliable results as sophisticated sample tests. They serve to create a culture of control with clear evidence of implementation. Alternatively, a formal approach—with checks carried out occasionally by a large staff of auditors who go into great detail over relatively long periods of time—is often perceived as jarring and can be met with resistance.

### Consulting vs. Cooperation

The consulting function of the internal audit—to solve the problems discovered in operational processes—cannot be fulfilled through simple suggestions in the audit opinion. The consulting phase must be incorporated as part of the entire improvement program for the operating processes and, for example, include a willingness to intervene at the request of those operating the processes.

It is easier to win cooperation if it is apparent to everyone that the proposed actions stem from the results of the risk treatment plan or the outcome of the audit. Offering assistance as part of the audit process does not affect the autonomy of the decision makers. It is not an operational sharing of tasks, but an active participation in the process of control, with reporting responsibilities and opportunities to recommend actions to achieve enterprise objectives more effectively.

The audit consulting function is not equivalent to culprit hunting. Rather, it is a joint research effort to improve the effectiveness of solutions. Sharing the purpose of an audit and its results with operators of business processes increases transparency and helps to improve the internal culture of the organization with respect to risk management and control capacity.

### Value Creation and Agility

The full value of the audit opinion cannot be realized if it does not align with the pace of the business. The speed of performing an audit must be in tune with the organization's speed of doing business. Many aspects of business operations evolve quickly, and internal change processes may be rapidly introduced. To be relevant, an audit must identify the points of



#### ENJOYING THIS ARTICLE?

- Read *Destination: Agile Auditing*. [www.isaca.org/agile-auditing](http://www.isaca.org/agile-auditing)
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>

deviation from business objectives with precision and timeliness.

To accomplish this, auditors must focus processes on specific issues and quickly apply remediations. This requires real flexibility in both planning and execution.

The increased speed of change of operational processes is one reason for the internal audit to follow a logic similar to that of the monitoring process through a systematic presence, adherence to operational processes, and flexibility in adapting to change while maintaining a distinct identity and independence of judgment. The audit's value cannot be contingent on increasing the number of participants in the audit team. Rather, there must be a review of the logic of intervention and the execution of recommendations to ensure the audit's adaptability to organizational needs.

---

## The internal audit process must be responsive to internal enterprise changes to easily align with the evolution of the business and guarantee the effectiveness of audit operations.

---

### Integration With Risk

The decision to start an audit activity and the definition of the relative perimeter of intervention must be based only on the logic of risk assessment for the business. In other words, the internal audit must be concretely risk-based, from the decision to conduct an audit to determining when to implement it, how to do it, and which business area it should cover.

The concept of risk-based audit<sup>5</sup> leads to the complete integration between internal audit and enterprise risk processes,<sup>6</sup> which means sharing the same remediation or response plans. Audit results must be systematically included in any consideration of the sources of vulnerabilities to ensure their integration in the risk assessment process and their complete synergy with risk decision-making.

One advantage of having a single risk assessment plan that includes the issues resulting from the

internal audit is that it allows the synergistic management of efforts to verify the effectiveness of implemented remedies. Risk management already carries out this control activity in a structured and comprehensive way for other risk-based processes; therefore, the participation of the internal audit team (which consequently will not have to monitor the remedy plan on its own) will only improve the effectiveness of these checks.

### Principles for an Internal Audit

Many points of improvement for the internal audit process have been discussed herein. They seem unrelated to each other, but, in reality, it is possible to achieve a coherent synthesis of them if the Agile Manifesto perspective is used. To integrate audit processes in business requires the ability to interact and cooperate in developing solutions and to adapt to existing operations without imposing constraints. These requirements can be fulfilled by respecting a set of principles similar to those used to define an Agile process. It means, instead of running a single monolithic process, adopting streamlined subprocesses that deliver each of the results that can be immediately evaluated and possibly modifying the overall process. Suitably redefined, these principles can become the Manifesto for the Agile Internal Auditor:

1. Create the expected value to satisfy the specific control expectations of the organization at any time.
2. Adapt to variations in the context of the control environment, objectively defined by a risk assessment.
3. When needed, produce an audit opinion on individual aspects of the audit without waiting to complete the entire audit plan or to meet a predetermined deadline.
4. Facilitate the emergence of synergies through cooperation between operational, control and audit processes.
5. Align audit methodologies and skills within the context of the examination and process evolutions.
6. Provide communications that are simple and transparent, and that present negative results as opportunities for improvement (reject a blame culture).
7. Ensure coordination between regular monitoring of remediation plans and risk mitigation plans.

8. Design an audit program that is inspired by risk assessment and not guided by an aging policy.
9. Use innovative tools to improve the effectiveness of the audit process, thereby improving the process being audited.
10. Establish clear and simple audit methodologies and rules to encourage integration between processes.
11. Analyze the work done in a holistic way to understand from experience how and where to improve.
12. Adopt identified improvements as integral parts of the audit process, consequently aligning related procedures and sharing improvements with interested parties.

## Conclusion

The internal audit process must be responsive to internal enterprise changes to easily align with the evolution of the business and guarantee the effectiveness of audit operations. However, internal audit operations must not impose additional demands on the enterprise to acquire these abilities. It is possible to develop them by redefining the design of the audit process. This does not require a comprehensive review of audit techniques or rethinking its definition. It can be achieved through a restructuring of the audit process.

The restructured approach must be based on principles derived from Agile logic to direct the audit process to interact effectively with business processes. Integration is essential to establish mutual trust and to encourage cooperation that will maximize synergies and result in common advantages. Further, integration aids in internal audit's alignment with business needs, improving efficacy without affecting cost or quality.

## Endnotes

- 1 ISACA®, *Implementing Robotic Process Automation (RPA)*, USA, 2020, [https://www.isaca.org/bookstore/bookstore-whl\\_papers-digital/whprpa](https://www.isaca.org/bookstore/bookstore-whl_papers-digital/whprpa)
- 2 Manifesto for Agile Software Development, "Principles Behind the Agile Manifesto," <https://agilemanifesto.org/principles.html>
- 3 Institute of Internal Auditors North America, *Standards and Guidance—International Professional Practices Framework (IPPF)*, USA, July 2015, <https://na.theiia.org/standards-guidance>
- 4 *Ibid.*
- 5 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 4," *ISACA® Journal*, vol. 3, 2020, <http://www.isaca.org/archives>
- 6 Sbriz, L.; "Capability Maturity Model and Risk Register Integration," *ISACA Journal*, vol. 1, 2022, <http://www.isaca.org/archives>