FEATURE

Enterprise Risk Monitoring Methodology, Part 3

Risk-Based Internal Audit

Internal audit often selects the entities to audit using an aging policy or in response to an incident. Then, the audit is conducted following a standard checklist, probably the same for all the entities. In contrast, risk-based internal audit is a valuable concept because it provides a method to optimize the auditing process. It means to use the risk knowledge about the entities to introduce a criterion to prioritize the audit visits and focus the audit tests only where it is necessary. The process will be faster and with fewer resources, but how can it be implemented effectively and efficiently? A holistic method to integrate risk monitoring with internal audit that considers both processes as part of a single collaborative control system is proposed herein. The processes can continue to operate in the same way they do currently, but by sharing the same basis of controls and working in a single coherent and centralized environment, nothing will be duplicated and each operation will be focused on its specific task in a synergistic way.

Luigi Sbriz, CISM, CRISC, ISO/IEC 27001 LA, ITIL v4, UNI 11697:2017 DPO

Has been the risk-monitoring manager at Magneti Marelli for more than four years. Previously he was responsible for information and communication operations and resources in the APAC Region (China, Japan and Malaysia) and, before that, was the worldwide information security officer for more than seven years. For internal risk monitoring, he developed an original methodology merging an operational risk analysis with a consequent risk assessment driven by the maturity level of the controls. He also designed the cybermonitoring tool. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn (*https://it.linkedin.com/in/luigisbriz*) or *http://sbriz.tel*.

An expected outcome of risk monitoring is a map of weaknesses useful for establishing the priorities of the audit plan (auditing high-risk areas before lower-risk ones). An expected outcome of internal audit is a set of remediation plans that can be merged into the risk treatment plan (an action plan or a remediation plan are the same thing); the audit opinion can also assure the high quality of the risk assessment performed.

A collaborative approach and use of a common web-oriented tool enables better focus on operations and a more robust monitoring of all action plans. As a result, there is also a minor overlap of tasks, increased confidence in the risk assessment, lighter document management and an improved organization of the process (in terms of quality, time, cost and relations with other processes).

Continuing on themes explored in the previous installments of this series on enterprise risk monitoring methodology,[1, 2] part 3 of this series demonstrates that the risk department cannot work alone within an organization. The first installment in this series described managing risk analysis and risk treatment plans that are strictly aligned with the requirements of the International Organization for Standardization (ISO) and involve all the necessary resources without any redundancy. The second installment in the series described how to use maturity levels to simplify risk assessment and reuse it to automatically feed other frameworks.

A method to integrate risk monitoring with internal audit and to insert the audit remediation plan into the risk treatment plan is established herein. It will result in a cyclical interconnection (risk audit) with risk monitoring results, thereby providing objective reasons to issue an audit plan, improving internal audit's confidence in risk assessment and turning the audit findings into a single integrated action plan comprehensive of both processes.

Introduction

A relationship between the processes of risk monitoring (see parts 1 and 2 for a proposal to implement it) and internal audit is even emphasized in its definition:

> *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 evaluate and improve the effectiveness of risk management, control, and governance processes.*[3]

There is a dual perspective in this relationship. The risk process constantly monitors risk and consequent action plans, but needs a concrete method to be able to trust the (self-) assessment of the operational risk. The auditing process objectively determines issues in the checked internal processes, but needs an efficient way to control the progress of its remediation plans (follow-up visits are not frequent).

A strong similarity between some parts of these two processes is evident (e.g., action plans); therefore, an advantage is expected from cooperation between them. The risk process monitors actions (controls and countermeasures) to treat risk, but without physical checks on their effectiveness. However, the audit process performs on-site checks of the effectiveness of controls and action plans, but it cannot systematically monitor the progress of remediation plans. In general, internal audit rechecks an entity only during the follow-up stage, typically after one year or longer.

The idea is to use an operating model between these two processes using the output of one as input for the other and focusing the processes on the activities they know how to do best or for which they were designed. Risk monitoring's strength is the evaluation and treatment of risk, but it suffers from the missing assurance of the assessment quality. Internal audit's strength is performing the fieldwork to assure the effectiveness of key controls without constantly following the progress of remediation plans.

> “THE IDEA IS TO USE AN OPERATING MODEL BETWEEN THESE TWO PROCESSES USING THE OUTPUT OF ONE AS INPUT FOR THE OTHER AND FOCUSING THE PROCESSES ON THE ACTIVITIES THEY KNOW HOW TO DO BEST OR FOR WHICH THEY WERE DESIGNED.”

Therefore, the terminal phase of the risk process could provide useful indications to build an objective audit plan (risk-based auditing process) through using the outcome of the risk assessment. The terminal phase of the auditing process could instead include the audit findings in the risk treatment plan so to manage them in the same way as the risk countermeasures. Moreover, the audit opinion can strengthen confidence in risk assessment.

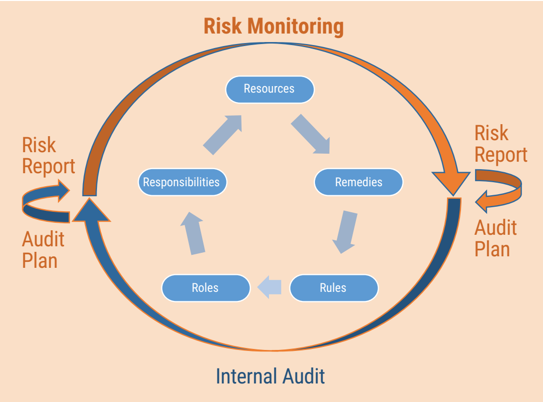
This close cooperation between processes is totally aligned with the guiding principles of the service value system[4] to facilitate value creation. If one tries to think of processes as if they are services, it is quite easy to see this correspondence.

Conceptual Model

An overall simplified scheme of the proposed methodology allows having the right perspective to understand the mechanism as a whole and to begin to deepen the individual parts (**figure 1**).

A virtuous cycle to analyze and assess risk and to manage them and re-examine their admissibility with organizational objectives takes place only with complete confidence in risk assessments. Based on this assumption, it is natural to feed the internal audit process with the results of risk monitoring and then feed the same risk monitoring with the outcomes of internal audit (both audit opinions and

Figure 1—Scheme of Interaction Between Risk Monitoring and Internal Audit



findings) as a guarantee of the quality of risk assessment and considering the same control.

Risk monitoring uses a risk assessment checklist to evaluate risk components and issue a set of reports or charts with analysis and treatment of the risk. This allows a first remote certification of the results or an adjustment of them to proceed (see parts 1 and 2 of this series or the following responsible, accountable, supportive, consulted, informed [RASCI] matrix). The results of the risk assessment lead to the development of an audit plan prioritized on the risk detected. This action is based on the auditability index[5] and, of course, on the confidence achieved in the evaluation. A quick off-site check (e.g., a telephone interview, an email) can be considered a first step toward trusting the risk assessment and its results.

Field audits allow the identification of all operating problems, either ones that have occurred or have the potential to occur, that affect the organization's objectives. The final audit report contains the list of resources in need of a remediation plan. This audit remediation plan will be included in the risk treatment plan, so each audit test will confirm whether or not it is connected with risk control (on ERA side). This last relationship is a requirement of this method. Each risk control will be linked to one or more audit tests to build the liaison risk audit.

Then the risk monitoring process is restarted in an iterative way and is followed in cyclical sequence by issuing the risk report with the priorities for auditing, by a field audit, by a consequent audit report that moves the issues into the risk treatment plan and by the adjustment of the controls' risk assessment. The basis of the controls used, risk or audit, has to be the same because the key controls of the audits must match the control statements used in the risk monitoring. The audit key control is checked by an audit test and so must be linked to a risk-control statement to confirm its assessment.

Into this schema a typical Deming cycle[6] can be identified with a plan for the treatment of the risk, a do phase to implement its intended actions, a check both for risk assessment consistency and effectiveness of its actions, and an acting phase to immediately address the issues or to seize opportunities to improve.

The cycle—integrating the phases of risk evaluation with the field control work (audit side)—assures proper alignment with any change in the organization's objectives by a periodic updating of the risk-assessment checklist, an effective risk assessment by the audit process and a continuous centralized control on the risk treatment plan (including audit findings).

> “A QUICK OFF-SITE CHECK (E.G., A TELEPHONE INTERVIEW, AN EMAIL) CAN BE CONSIDERED A FIRST STEP TOWARD TRUSTING THE RISK ASSESSMENT AND ITS RESULTS.”

Risk Monitoring Plan

Risk monitoring is finalized once a risk treatment plan is issued to address any issue, but only until the risk level is no longer under an acceptable value.[7] This value is a consequence of the business objectives and must be formalized to understand when the controls or countermeasures are considered sufficient. Therefore, the risk will have to come from an in-depth analysis of the business context.

This is not an out-of-the-box feature and must be tailored to organization objectives. A suitable implementation is explained in the previous installments of this series, and it is a useful reminder of an organization's need to piece together the five factors rotating around the achievement of the organization's objectives in the risk perspective. The five factors are:

1. **Resources**—Any asset, process, skill or action that affects organizational objectives
2. **Remedies**—Any action or activity taken to improve internal processes or to reduce risk
3. **Rules**—The set of control statements to be evaluated (and audited) derived from organizational requirements
4. **Roles**—All the organizational positions involved in the risk management and internal audit processes
5. **Responsibilities**—Operational or control rules (tasks) assigned to all the organizational positions involved

Roles and responsibilities are included in an RASCI matrix. Resources are identified by a strength, weakness, opportunity and threat (SWOT) analysis. Remedies are actions such as controls in place or countermeasures identified in the risk analysis and included in the risk treatment plan (RTP). Rules are the basic controls currently running and evaluated in the risk assessment, sometimes referred to as the Statement of Applicability[8] (i.e., the full list of controls actually in place, what they can do and which can be controlled). According to this methodology, the checklist is intended to cover any relevant operation performed by the organization.

This checklist of rules is used for measuring their level of implementation from the risk monitoring perspective that is the basis for the design of the audit tests in the internal audit process.
It is quite evident that there must be a close relationship at the level of the software system between control statements, audit tests, and catalogs of standard activities and resources to be able to optimize and automate the data interchange between the processes.

> “THE BENEFITS ACHIEVED BY THE RISK OWNERS ARE EASIER AND MORE ROBUST CONTROL OF THE WORK'S PROGRESS AND THE HEADS OF DEPARTMENTS BEING ABLE TO ACT PROMPTLY ON DELAYS OR PROBLEMS.”

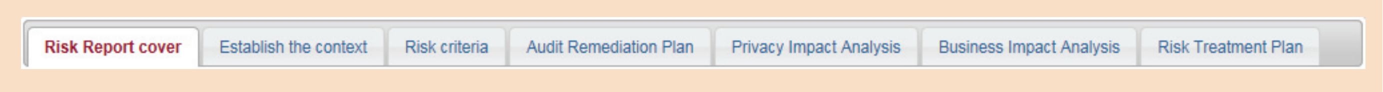
Notes on the Definition of Risk Provided by ISO 31000:2018
An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories, and can be applied at different levels. Risk is usually expressed in terms of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).[9]

Risk Monitoring "Do"

The risk report (see part 1) is the document summarizing the overall process of risk monitoring. It includes all the relevant resources, why and how they are protected, the risk analysis, the risk assessment, and the remediation plans divided by treatment area, i.e., auditing, privacy, continuity (**figure 2**).

In addition to the action plans, another output of risk monitoring is available—a key performance indicator (KPI), called "auditability index" (see part 2), dedicated to measuring the audit priority of an entity. An algorithm, weighting answers with respect

Figure 2—Header of the Risk Treatment Report



> “THE ADOPTED ENTERPRISE RISK CHECKLIST, CONVENIENTLY AGGREGATED, MUST MEET THE FULL SET OF ALL RELEVANT RULES IDENTIFIED BY THE ORGANIZATION FOR ITS FUNCTIONING.”

to those used for the maturity level and with a ranking based on the concept of “trust” in the answers provided, will be able to evaluate the urgency of performing an on-site audit.

For example, a rating of “full compliance” in risk monitoring is considered the best, but in internal audit, it is just a statement to be verified. Could one trust a statement where everything is perfect? In an auditing perspective, a convincing statement claims to work more for improvement (know the risk and work to avoid it, even if it is low) than for a declaration of total absence of problems (maybe the risk is unknown).

At this phase, a systematic central control over the progress to implement the identified countermeasures is important. It does not matter how countermeasures have been identified, either by a risk evaluation or an audit test, because they must be completed as planned or re-evaluated in case of risk-based delay. Activities to counteract risk, to improve processes or to remedy negative outcomes from the audits must be standardized and managed in a single environment without distinctions to avoid organizational structures being duplicated.

The benefits achieved by the risk owners are easier and more robust control of the work’s progress and the heads of departments being able to act promptly on delays or problems.

Internal Audit “Check”

Establishing the scope of the audit is the first step in managing an audit.[10] For internal audit, the scope can be identified as the physical location plus one or more internal processes of the organization. The audit scope generally includes a description of the physical and virtual locations, functions, organizational units, activities and processes, in addition to the time period covered. A virtual location is where an organization performs work or provides a service using an online environment allowing individuals irrespective of physical locations to execute processes.[11]

The natural choice for internal audit is to consider the enterprise risk checklist (control statements) as the source for the audit key controls on which tests are efficient. The enterprise risk scope is made through the contribution of all policies, regulations, laws, standards, contractual clauses and other subjects that have a high or severe impact on the objectives of the organization.

In short, the adopted enterprise risk checklist, conveniently aggregated, must meet the full set of all relevant rules identified by the organization for its functioning. This choice fits exactly the set of risk components that must be kept under control to reduce risk occurrence and effectively counter it. If there is another control statement that is not yet included but is relevant to the organization’s objectives, then it must be added as a new entry or combined with an existing one.

So far, it has been shown that the audit scope shall be derived from the risk scope or its subset due to risk management’s wider coverage. A pragmatic approach to building the statement of applicability (boundaries of auditability) of the audit scope is to include as key controls all the control statements whose severity is classified as high or very high and those whose severity is medium, but with high risk.

The severity of the control statement is a measure of the impact of the control on the organization’s objectives. It is a mandatory attribute for each control in risk scope, and its alignment with organizational objectives must be periodically checked and updated, at least at every change of organizational objectives.

The whole set of audit key controls can be broken down in smaller homogeneous subsets following a suitable criterion and, therefore, they can be named by the main process involved (e.g., finance, security, quality, environment, health and safety [EHS]). Accordingly, it is easy to refer to them as audit schemas.[12] Of course, any other method to define the audit schema is allowed; for example, building it by grouping the controls in some way. Some methods to create an audit schema for a single purpose include: all the controls included in a specific certification schema (e.g., quality, safety), matching the competencies of an internal auditor's group (e.g., information security) or impact from a relevant regulation (e.g., the US Sarbanes–Oxley Act of 2002). The reason for working with simpler and more-focused audit areas is to obtain small specialized teams, which require less time to perform the audit and increase the number of visits.

Even the classical concept of an audit program[13] can be managed easily. For each entity or group of entities (e.g., all the plants of a legal entity), an audit program can be set by a matrix of relationships between the entities and the different audit schemas established. Each audit schema is a single audit performed over the key controls and identified by a subset of the risk checklist's control statements.

The relationship matrix is physically implemented through a simple database table, and a suitable web form is used for its maintenance. If one considers the checkbox an audit code, one can understand that it is easy for the system to identify and automatically aggregate the results of all the audits involved into a single overall audit report (**figure 3**).

A single audit or audit program does not affect the conventional fieldwork of audit but rather, with the sharing of part of the same control checklist and the management of outcomes in an integrated environment, makes it clear that the overall process is flexible in its definition, focused exactly on the intended topic and cooperative for a rational distribution of tasks by competence.

> “THE AUDITORS ARE FREED FROM THE NEED TO FOLLOW ACTION PLANS BECAUSE THEY ARE AUTOMATICALLY PASSED TO THE OPERATING PERSONNEL AND THE CONTROL DELEGATED TO THE RISK MANAGEMENT STRUCTURE.”

Internal Audit “Act”

It is at this point that the idea to share the same mechanism to manage the action plans both for not-acceptable risk (provided by a risk-treatment plan) and for the failed audit tests (requiring a remediation plan) came about. Stressing a bit more this idea of a unique management system of action plans, one can see that it is only a matter of nomenclature (countermeasures vs. remediation plans), but in the end it is merely an action plan either to build a countermeasure to reduce a risk or to solve an issue due to a failed audit test. Nothing else.

The operative management of the action plans in a common environment is in charge of the resource owners and, in the end, this simplification introduces others' evident advantages. Organizational and cross-functional relationships are more orderly and solid. During the closing meeting, the audit report will be ready on the fly, avoiding any final transcription. For each failed audit test, through the use of a specific feature, it will be allowed its automatic insertion into the risk treatment plan.

This last operation produces a positive practical effect. The auditors are freed from the need to follow action plans because they are automatically passed to the operating personnel and the control delegated to the risk management structure.

Figure 3—Graphical Representation of an Audit Program Built by a Matrix of Entities and Audit Schemas

Sites of the Legal Entity	SOX Schema	EH and S Schema	Security Schema	Quality Schema
Gobi desert site	☑	☑		☑
Sahara desert site		☑	☑	
Antarctic desert site	☑		☑	
Patagonian desert site	☑			☑

To allow internal audit more time to dedicate to more frequent periodic checks, minimizing the saving and formatting of the audit test outcomes is recommended. Unlike a third-party audit, the evidence is used only to clarify the findings of operating structure during the closing meeting or limited to a quick dispute, but immediately after, there is no reason to save them (if not otherwise required by policy).

The audit report (**figure 4**) will be qualified by a specific cover to summarize the descriptive information of the audit and its outcomes, but all other parts will be dedicated to risk analysis and action plan, exactly like in the risk report. Therefore, for the risk report and audit report, only the covers are different and summarize their specific information. Remediation plans (from audit tests) and countermeasures (from risk analysis) are combined because common management is more effective, but, if required, it is always possible to display them separately (a computer-only effort and, therefore, acceptable).

In some cases, the summary of the audit outcomes on the cover is not considered suitable to represent the work done. It is possible to use additional pages to display in detail the full list of the audit tests and their outcomes. Even if technically possible, managing data should be avoided when not necessary. In the cover, there is at least the list of the processes involved in the audit scope, the list of the resources and the list of critical action plans, which is considered suitable for most audits.

Minimum Set of Documents

Different types of documents are available, but only two are important: the risk report and the audit report. In just a few pages, they summarize all relevant information on the specific process in accordance with the need-to-have principle (provide more details only if strictly required).

They are made up of a cover followed by the risk analysis, assessment and action plan. This is split in homogenous groups by actions, i.e., remediation plans for audit tests, business impact analysis (BIA) for continuity, privacy impact assessment (PIA) for International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) ISO/IEC 29134:2017 *Information technology—Security techniques—Guidelines for privacy impact assessment* or data protection impact assessment (DPIA) for the EU General Data Protection Regulation (GDPR), and risk treatment plan (RTP) for all general actions.

For authorized users (e.g., auditors), the audit report cover is editable like a form (**figure 5**) to allow its customization. The minimal set of information to be managed consists of a narrative about the audit purpose, the composition of the teams split by audit schema, a summary for management that highlights the strengths and weaknesses, and the audit opinion. The last function, represented by a lambda check icon, allows for closing of the audit.

Moreover, from the outcomes of the audit tests, the following are automatically provided (no manual transcription needed):

- The audit scope built reading the key controls involved
- The list of critical resources discovered
- The critical actions included in the remediation plan and the history of the audit visits

Should other information be necessary, it is always possible to include it in the online reports or charts with the option to download it in PDF or Excel format.

Printing or downloading a report is against the logic of always getting the most up-to-date data. Printing a report means removing it from a system that ensures its integrity and updating, so it is better to display it on the fly when necessary (updated) and only what is useful (legibility). In the design of the interface, it is possible to prepare different sets of data for presentation depending on two principles:

1. Quick access, which means fewer selections are needed
2. Capability of the device, which means formatting based on screen size (e.g., smartphones)

Quick access could also mean preparing different (small) viewpoints of data depending on the identified needs to access the data. Managing the capability of

Figure 4—Header of the Audit Report

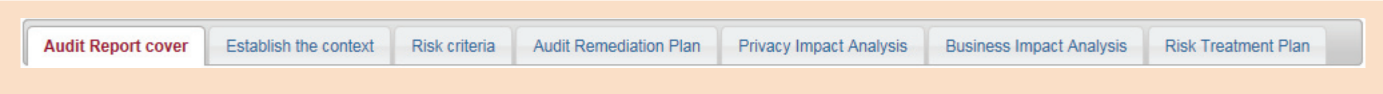
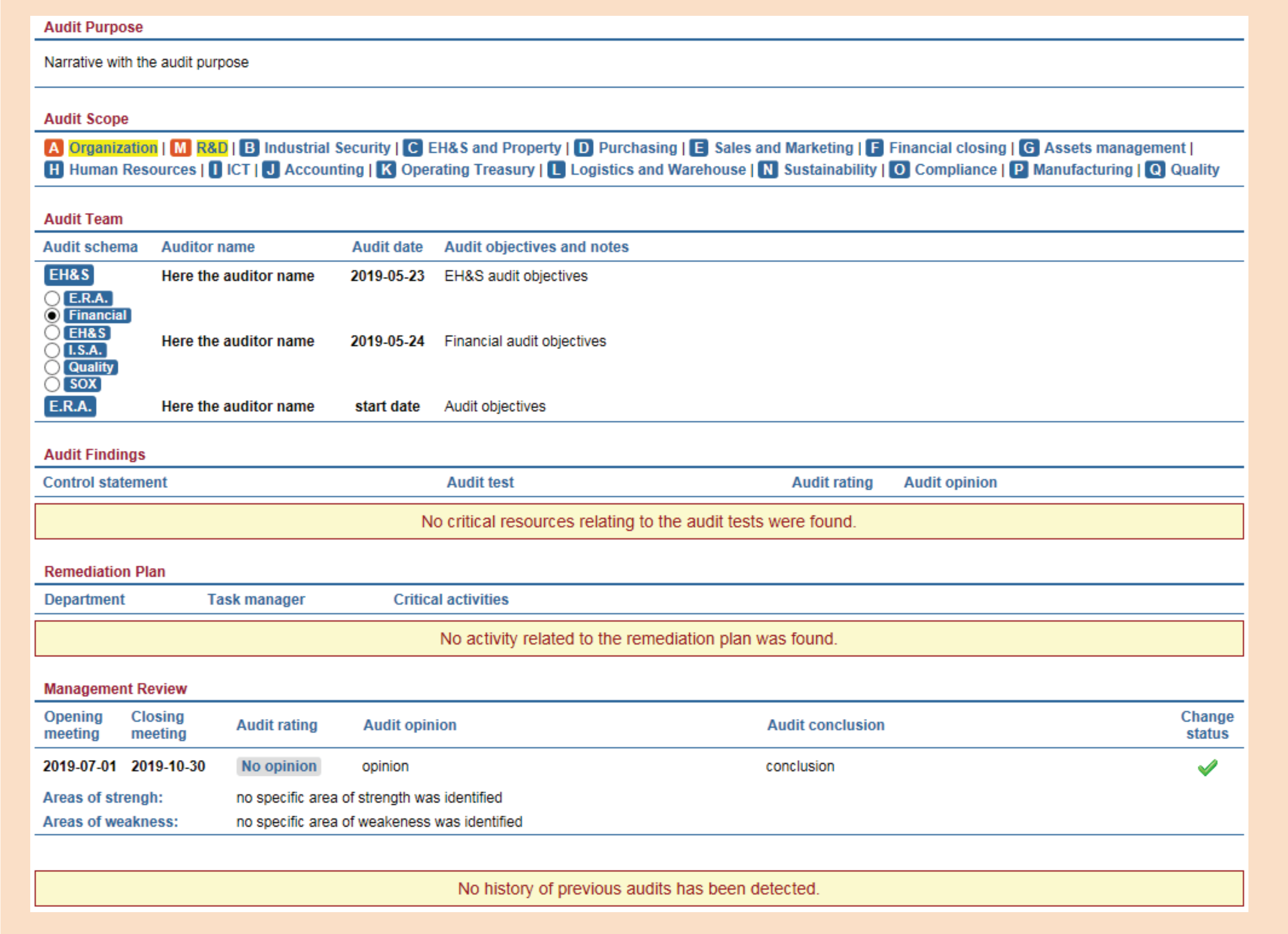


Figure 5—Data-Entry Form of the Cover of the Audit Report



Audit Purpose

Narrative with the audit purpose

Audit Scope

A Organization | M R&D | B Industrial Security | C EH&S and Property | D Purchasing | E Sales and Marketing | F Financial closing | G Assets management | H Human Resources | I ICT | J Accounting | K Operating Treasury | L Logistics and Warehouse | N Sustainability | O Compliance | P Manufacturing | Q Quality

Audit Team

Audit schema	Auditor name	Audit date	Audit objectives and notes
EH&S	Here the auditor name	2019-05-23	EH&S audit objectives
○ E.R.A. ● Financial ○ EH&S ○ I.S.A. ○ Quality ○ SOX	Here the auditor name	2019-05-24	Financial audit objectives
E.R.A.	Here the auditor name	start date	Audit objectives

Audit Findings

Control statement	Audit test	Audit rating	Audit opinion

No critical resources relating to the audit tests were found.

Remediation Plan

Department	Task manager	Critical activities

No activity related to the remediation plan was found.

Management Review

Opening meeting	Closing meeting	Audit rating	Audit opinion	Audit conclusion	Change status
2019-07-01	2019-10-30	No opinion	opinion	conclusion	✓

Areas of strengh: no specific area of strength was identified

Areas of weakness: no specific area of weakeness was identified

No history of previous audits has been detected.

the device is possible with, for example, Media Queries (CSS3),[14] the Navigator userAgent (DOM)[15] or other equivalent methods. The result is the availability of different queries that are focalized to quickly access small pieces of data vs. a single heavy document to print. So, why use paper?

Considerations About the Organization

A few considerations about the organization's structure support this methodology. Recalling the RASCI of part 1 of this series, a place for internal audit can be introduced by adding a role called "internal auditor" with some changes in the tasks (**figure 6**). These changes include accountability for the audits entrusted to the internal audit process when the risk-monitoring process maintains it for the management of the frameworks and risk assessment.

Internal audit operations are enabled by the outcomes of risk monitoring, and the internal audit outcomes feed the risk monitoring operations, also improving the overall quality with a check on the effectiveness of the existing controls.

The cyclical cooperation between the two processes shows how natural it is to treat them as services for the organization's governance. The concept of service is evident in their interfaces: Risk monitoring delivers the risk components to make the decision about which is the next entity to audit; instead, internal audit provides the list of resources

> "THE CYCLICAL COOPERATION BETWEEN THE TWO PROCESSES SHOWS HOW NATURAL IT IS TO TREAT THEM AS SERVICES FOR THE ORGANIZATION'S GOVERNANCE."

needed to be protected from misalignment in respect to organizational objectives. The action plan is a shared resource.

Thinking of these processes as cooperating services, it is advantageous to adopt Agile[16] methodology concepts. Instead of an infrequent, full and in-depth audit, the speed of the internal audit, visits and tests can be increased with a visit plan driven by risk and light tests for controls with low level of risk and in-depth tests only on high risk. Consequently, the audits are carried out quickly (several times with less amplitude and with the right competence engaged) and, in this way, the risk assessment is more frequently adjusted in accuracy and trust. A significant result of internal audit is the proper identification of areas of weakness and the objective issuing of a remediation plan (focused only on the audit findings).

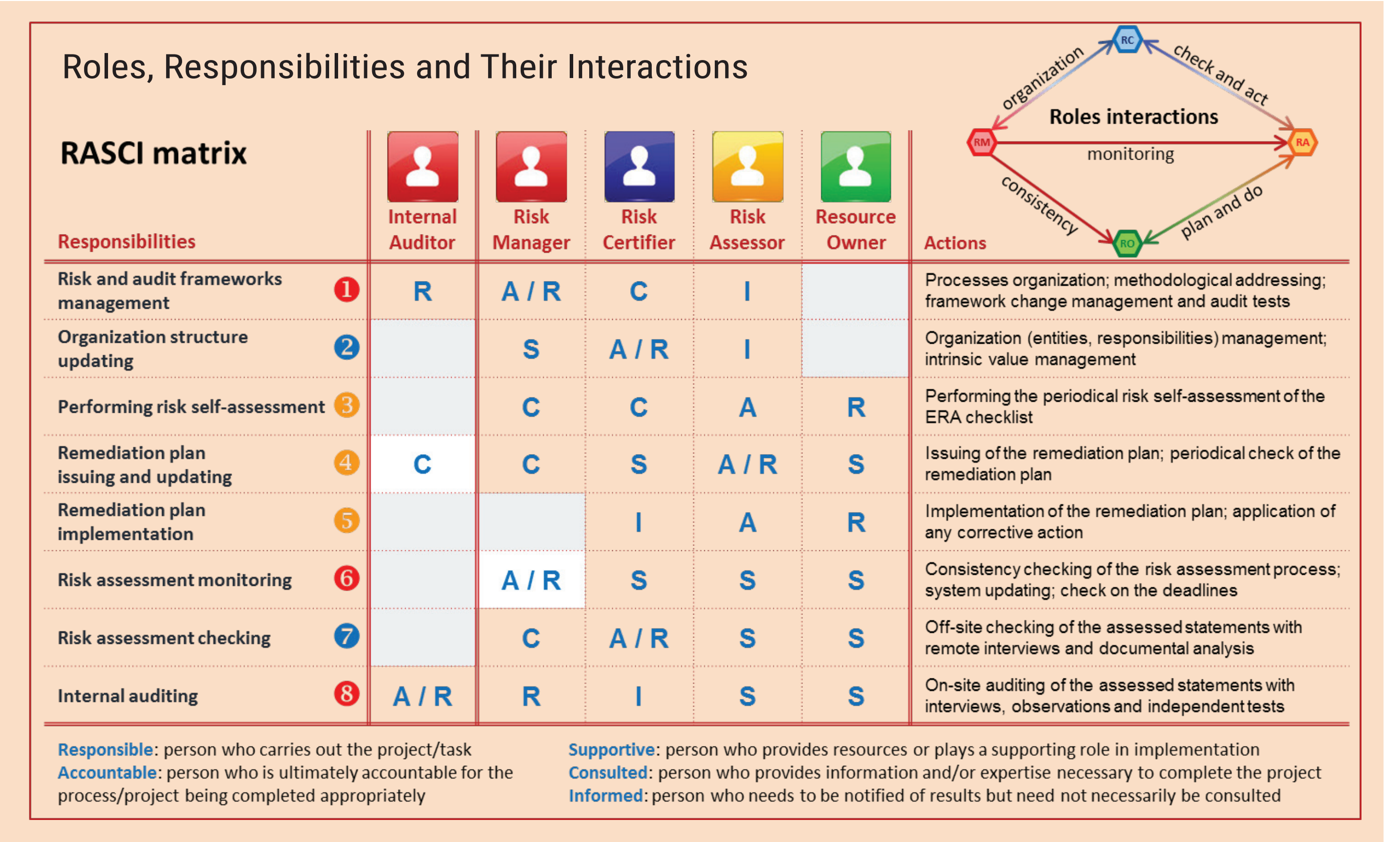
To improve audit frequency, it is possible to divide groups of auditors by competence in order to create small audit teams dedicated to a single audit schema. When the audit scope meets a single audit schema and the depth of the audit test depends on the risk level of the key controls, then the number of audits performed must increase to cover the same number of controls. Consequently, there are more visits meant to improve the awareness of controls of the audited personnel.

The “ERA review” managed by the risk monitoring team could be added to the audit schema list. This is an on-site lean audit with the aim of checking the consistency of the risk-control implementation by interviews, observations and eventual document analysis, but without an independent audit test. In this way the audit is light, fast and can involve a number of controls in a short time. Even without a thorough check, it improves the awareness of risk controls and confidence of risk assessment.

Even with the best collaboration between processes, a referee among them is always necessary. A simple organizational chart is proposed to address any potential conflicts. This position (the name is not important) could also be responsible for the coordination of other processes that aim to ensure the alignment of the control operations with the organization’s objectives.

In this hypothetical scheme (**figure 7**), internal audit should be dedicated to the control of internal processes, partners and suppliers, and to checking

Figure 6—Example of RASCI Matrix Including Internal Audit and Risk Monitoring



Roles, Responsibilities and Their Interactions

RASCI matrix

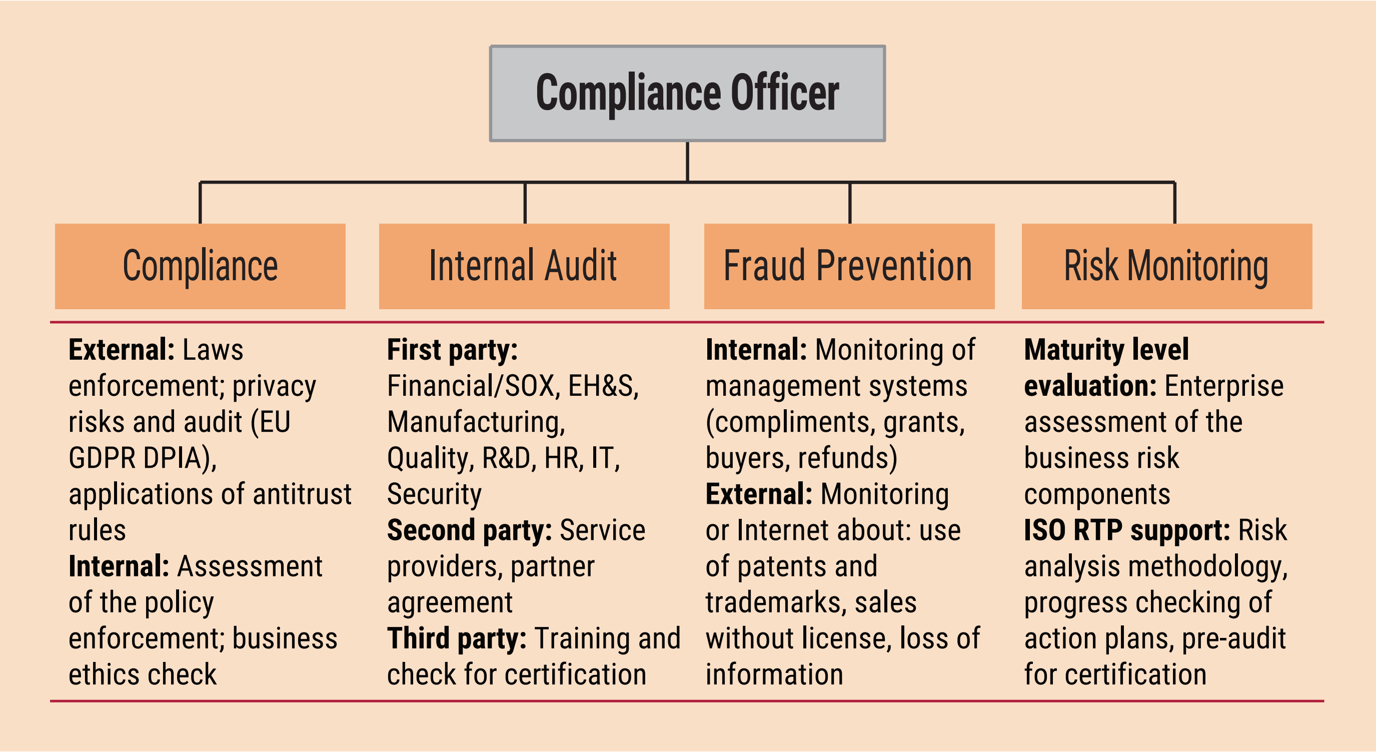
Roles interactions
RC
RM
RA
RO
organization
check and act
monitoring
consistency
plan and do

Responsibilities		Internal Auditor	Risk Manager	Risk Certifier	Risk Assessor	Resource Owner	Actions
Risk and audit frameworks management	1	R	A / R	C	I		Processes organization; methodological addressing; framework change management and audit tests
Organization structure updating	2		S	A / R	I		Organization (entities, responsibilities) management; intrinsic value management
Performing risk self-assessment	3		C	C	A	R	Performing the periodical risk self-assessment of the ERA checklist
Remediation plan issuing and updating	4	C	C	S	A / R	S	Issuing of the remediation plan; periodical check of the remediation plan
Remediation plan implementation	5			I	A	R	Implementation of the remediation plan; application of any corrective action
Risk assessment monitoring	6		A / R	S	S	S	Consistency checking of the risk assessment process; system updating; check on the deadlines
Risk assessment checking	7		C	A / R	S	S	Off-site checking of the assessed statements with remote interviews and documental analysis
Internal auditing	8	A / R	R	I	S	S	On-site auditing of the assessed statements with interviews, observations and independent tests

Responsible: person who carries out the project/task
Accountable: person who is ultimately accountable for the process/project being completed appropriately

Supportive: person who provides resources or plays a supporting role in implementation
Consulted: person who provides information and/or expertise necessary to complete the project
Informed: person who needs to be notified of results but need not necessarily be consulted

Figure 7—A Governance, Risk and Compliance (GRC) Organization Proposal


Compliance Officer
Compliance
Internal Audit
Fraud Prevention
Risk Monitoring
External: Laws enforcement; privacy risks and audit (EU GDPR DPIA), applications of antitrust rules
Internal: Assessment of the policy enforcement; business ethics check
First party: Financial/SOX, EH&S, Manufacturing, Quality, R&D, HR, IT, Security
Second party: Service providers, partner agreement
Third party: Training and check for certification
Internal: Monitoring of management systems (compliments, grants, buyers, refunds)
External: Monitoring or Internet about: use of patents and trademarks, sales without license, loss of information
Maturity level evaluation: Enterprise assessment of the business risk components
ISO RTP support: Risk analysis methodology, progress checking of action plans, pre-audit for certification

and training for preaudit certifications. Risk monitoring performs the risk assessment and supports the risk-analysis methodology for ISO certifications. Other control processes could be "compliance" to check law or policy enforcement or "fraud prevention" to detect situations with a high risk of fraud. The top of this chart cannot be an operational position that could be verified.

Practical Implementation

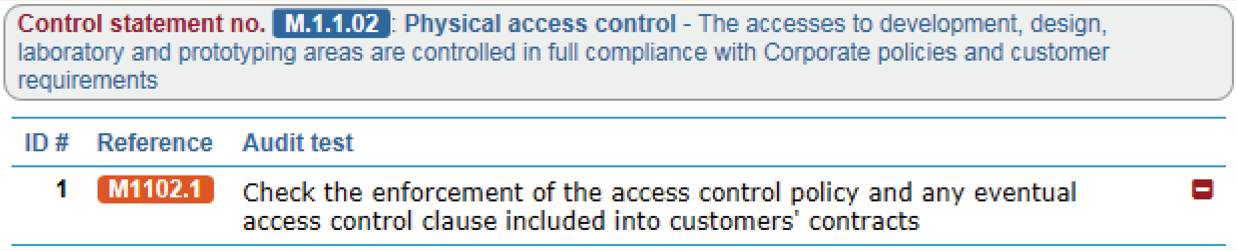
How is this convergence between risk monitoring and internal audit technically implemented? This union is based on two cornerstones. The first is the use of a single common checklist, completely assessed by risk monitoring, with each key control (also known as control statement) linked to the audit tests to be executed by internal audit. The second are the findings of internal audit that are managed by risk monitoring into a single integrated environment for the management of all action plans.

The main goal is to keep the relationship between the control statements and the audit tests alive and easy to change. On each control statement, one can enter zero or more audit tests and customize or delete them through a pop-up window (maintenance form). Through a coding convention, the audit tests are automatically supplied with a code; then, manually, a narrative for the audit test is supplied to establish the kind of audit carried out on the field to ensure the effectiveness of the control statement (**figure 8**).

A technical clarification about the use of this relationship is necessary. In each control statement, a customized list of standard actions, standard resources and roles all managed through a pop-up window are included. The reason is to be able to provide a preconfigured action plan in case of a failed audit test that will be customized only by the assigned manager (and not created entirely from scratch). During the insertion phase, any eventual duplication of actions is automatically rejected; however, everything is changeable by the local risk assessor, including the duplication of records.

The audit-fieldwork form is similar to the maintenance form of the audit test. During any audit test, it is possible through the execution to insert into the form the audit opinion and an observation. It will write the audit opinion via a pop-up window linked to the key control. Auditor information is automatically retrieved by the username profile, and further fields can be easily added to the form. Of course, the need-to-have principle should be seriously considered before doing so.

Figure 8—Web Form of a Control Statement



Control statement no. M.1.1.02 : Physical access control - The accesses to development, design, laboratory and prototyping areas are controlled in full compliance with Corporate policies and customer requirements

ID #	Reference	Audit test	
1	M1102.1	Check the enforcement of the access control policy and any eventual access control clause included into customers' contracts	⊟

Each record in the form is provided with a trigger (an icon), useful during the closing meeting. For each finding which is recognized as high severity with the need for an audit plan, this icon will automatically insert a preconfigured action plan into the RTP on the right side of the form. Consequently, the risk assessor will take care of this and appropriately customize it.

Another technical note about the preconfigured action plan: For easy identification of any action plan originated by a failed audit test compared to those originated by the risk assessment, there is a specific SWOT factor used only for this purpose. It is named “audit test,” and it is considered a strength factor because it allows one to solve the problem in advance using an action plan and avoiding risk or, at least, reducing its impact.

Additional logical correspondences between an audit and a risk include:

- The audit test is considered a resource because it is of value for the organization.
- A remediation plan is treated as a set of countermeasures for a risk plan because it faces some risk.
- The reports, risk and audit keep a different cover, but all other parts share the same content.

Supposing that members of the audit team are working on separate processes, they can work simultaneously in parallel, each using their own web form. Any eventual evidence collected (file) can be uploaded in a special web folder ready for re-examination of the tests during the closing meeting. Once the audit is completed, the files can be deleted (unless otherwise requested by the policies).

Software Tools

Some considerations must also be made for the software development model. This is last because it is not a methodological topic, but it is no less important. Methodology without technological support cannot provide any practical results.

As a first consideration, one should start with the data collection. The typical work with spreadsheets cannot be included in the set of options because the need to collaborate and work together without much effort to realign the input data and share the outcomes is quite evident. Even the use of a web-based spreadsheet can be a bit tricky to build all data interrelationships.

Then comes the availability of pages built dynamically by the role of the users. The presentation layer must be driven by the user role to be more intuitive for the end user and not by the system constraints. Therefore, instead of preparing two different layouts, one for authoring and the other for the reporting, in the same web page there will be some rows or parts that are editable and others that are not, depending on the user role. The training will be easier and clearer.

Finally, using a software package (out-of-the-box tool) vs. software development (everything developed) should be addressed. A software package means quick delivery time, but licensing costs, cost of setup and feasibility of *ad hoc* solutions must be evaluated. Software development means a low-cost solution (in particular, with open source) and unlimited customization, but delivery time and costs for know-how and development must be taken into account. The organization's ability to adapt to the constraints of the software package will determine the final decision and, thus, the cost.

> "THE ORGANIZATION'S ABILITY TO ADAPT TO THE CONSTRAINTS OF THE SOFTWARE PACKAGE WILL DETERMINE THE FINAL DECISION AND, THUS, THE COST."

Conclusion

Risk monitoring and internal audit are two processes that naturally interact with each other by connecting the mutual inputs/outputs and producing only advantages. Both must be focused on their own tasks (i.e., risk evaluation, action plans, effectiveness of controls, remediation plans) without any redundancy or overlapping.

There are some concrete advantages. The resulting synergy between the two collaborating processes introduces benefits in terms of:

- Better quality managed action plans (single point of control for all action plans)
- A single web-oriented, risk assessment checklist in common with the audit process (less effort to manage the processes)
- Performance improvement in the audit process (small audit scopes run more frequently and are more focused on risk)
- Greater flexibility in the process setup (the risk checklist and the audit test lists and their relationships can always be changed)
- Simplified document formats and online work (a web-based tool means no need to use paper)
- A single environment for risk-treatment and remediation plans (a rational way to avoid redundancy)
- Solid multilevel centralized control (a sound organization allows different types of assessment certifications)

Moreover, after having removed any redundancy in the processes, having made them more agile and having increased their quality, the organization will also have greater confidence in risk assessment (to compensate for the first phase in self-assessment mode).

The processes have been compared for their collaboration behavior as services. This introduces the possibility of adopting specific operational models typical of service management in addition to the traditional purely organizational approach. Adopting the service-value model to the methodologies to manage control processes can lead to pleasant surprises in terms of quality, time and cost.

When risk monitoring and internal audit work in a cooperative, synergic way and are fully consistent, the result provides focused analysis and actions (advising) to contrast risk. So structured, this operation adds value to the organization, exactly as is the expectation of the internal audit mission.

Endnotes

1 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 1" *ISACA® Journal*, vol. 2, 2019, *http://www.isaca.org/ archives*

2 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 2," *ISACA® Journal*, vol. 2, 2019, *http://www.isaca.org/ archives*

3 The Institute of Internal Auditors North America, "Standards and Guidance—International Professional Practices Framework (IPPF)," July 2015, *https://na.theiia.org/standards-guidance/*

4 AXELOS, ITIL—IT Service Management, *https://www.axelos.com/best-practice-solutions/itil/*

[5] *Op cit* Sbriz, Part 2

[6] Moen, R.; C. Norman; "Evolution of the PDCA Cycle," Asian Network for Quality Conference, Tokyo, Japan, 17 September 2009

[7] International Organization for Standardization (ISO), ISO 31000 *Risk Management*, Switzerland, 2018, *https://www.iso.org/iso-31000-risk-management.html/*

[8] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001 *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, Switzerland, 2013, *https://www.iso.org/isoiec-27001-information-security.html*

[9] *Ibid*.

[10] International Organization for Standardization, ISO 19011 *Guidelines for Auditing Management Systems*, Switzerland, 2018, *https://www.iso.org/standard/70017.html*

[11] *Ibid*.

[12] *Ibid.*

[13] *Ibid*.

[14] W3C; Cascading Style Sheets, 26 August 2019, *https://www.w3.org/Style/CSS/*

[15] W3, HTML Document Object Model, 19 January 2005, *https://www.w3.org/DOM/*

[16] AgileManifesto.org, "Manifesto for Agile Software Development," 2001, *http://agilemanifesto.org/*