Guide to implementing a Continuous Auditing System

Solution approaches and best practice experiences

Developed in the DIIR working group in Continuous Auditing

Version 1.0
published: 26.04.2021
(Englisch version: 5.06.2026)

DIIR Deutsches Institut für Interne Revision e.V.

Content

1 Introduction

The constantly increasing pressure to conduct audits efficiently and to achieve audit results in a timely manner poses serious challenges to the profession of internal auditing. At the same time, the growing number of legal and regulatory requirements is intensifying this pressure and demands a more agile development of the methodological approach to meet these requirements.

The increasing pace of economic changes and the resulting impact on business models, increasing complexities, risk fluctuations, and ultimately the digitization and automation of business processes, increasingly call for an internal audit function in the company that is both proactive in its planning and timely in its response. It is therefore essential that internal auditing changes from a static, time period-based (one to five years in advance) risk assessment and audit planning towards a direct situational-reactive analysis of risks and control effectiveness with rolling audit planning.

The DIIR working group in Continuous Auditing was founded in 2015 to provide targeted information on possible solutions and best practice experiences in a guide for the introduction of a Continuous Auditing System (CA-System). Over the past few years, the participants in the working group have intensively exchanged their experiences in various sectors (including banking, chemicals, and industry) and published their findings in a series of articles.

The articles published since 2017 have addressed the following topics:

1. Auditing's response to more complex audit requirements: Continuous Auditing – The added value of Continuous Auditing from the user's perspective [1]
2. Using Continuous Auditing with a model company – The added value for audit planning and preparation[2]

[1] Cf. Bauch, M. et al., ZIR 3/2017, Erich Schmidt Publication Berlin, p. 130 ff.
[2] Cf. Gorschenin, E. et al., ZIR 3/2018, Erich Schmidt Publication Berlin, p. 140 ff.

3. The added value of Continuous Auditing for audit execution, reporting and follow-up – Use of Continuous Auditing based on a model company[3]

4. Use of Continuous Auditing – Challenges and outlook for the future[4]

Based on this and the desire to publish a targeted reference work for the introduction of a CA-System, this guide deals with a definition of Continuous Auditing (CA) that is practicable from the point of view of the working group participants, as opposed to Continuous Monitoring (CM). The guideline describes possible approaches and incentives for the basic decision-making process as to whether CA should or can be used. Further, examples for the use of CA are presented for the core audit processes of audit planning, audit preparation, and audit execution.

Finally, tools currently available on the market or used by participants that can support CA-processes are briefly presented and the advantages and disadvantages of using tools are briefly summarized.

The introduction of a CA-System and the associated decisions might result in completely different added values depending on the industry and the size of the company or the internal audit department, the authors point out that the suggestions provided in this guide, which are to be understood as best practice, are only intended to help in the decision-making process, but are neither to be understood as a requirement nor as a final solution.

In the following chapters, the terminology will first be explained, defined, and delimited, supplemented by assumptions and basic principles, in order to present the understanding and view of the DIIR working group in Continuous Auditing and to establish a foundation for further work. In addition, a conceptual distinction between CA and CM will be made. The objectives and the added value of using CA will be presented, supplemented by some assumptions and basic principles for the following explanations.

[3] Cf. Jacka, C. et al., ZIR 5/2018, Erich Schmidt Publication Berlin, p. 237 ff.
[4] Cf. Bauch, M. et al., ZIR 6/2018, Erich Schmidt Publication Berlin, p. 248 ff.

1.1 Clarification of terms, assumptions and basic principles

The exchange of experiences within the working group makes it clear that progress in implementing the CA varies considerably. There are also significant differences in the presentation of results, risk addressing and the downstream workflow for dealing with risks. At the same time, the technical implementation is likewise highly individual and shaped by both the existing toolset of a company and market developments: Not long ago, solutions based on a standalone data warehouse (DWH) were prioritized, however there seems to be a trend towards tools for the scalable implementation of mass data analyses (possibly cloud-based). In addition to a component for data storage, there is usually a component for maintaining the analysis logic and a presentation component (visualization) for the results, which itself may also offer interaction options for the user.

Despite the heterogeneous CA-approaches in the working group, there is agreement that a CA-analysis always addresses a relevant risk, pursues a specific objective, must be reproducible and, if critical, triggers an action (information, assessment, short or ad hoc review, etc.).

Fig. 1: Continuous Auditing basic assumptions[5]

The combination of risk-oriented analysis along with downstream activity denotes a Key Risk Indicator (KRI). Alternatively, there is also the option of pursuing specific performance targets, which can be expressed as Key Performance Indicators (KPI). The combination of the two indicators results in audit objectives, which can be referred to as Key Audit Indicators (KAI). These are the basis for the practical applicability of Continuous Auditing. Possibilities for application cover the entire audit lifecycle.[6]

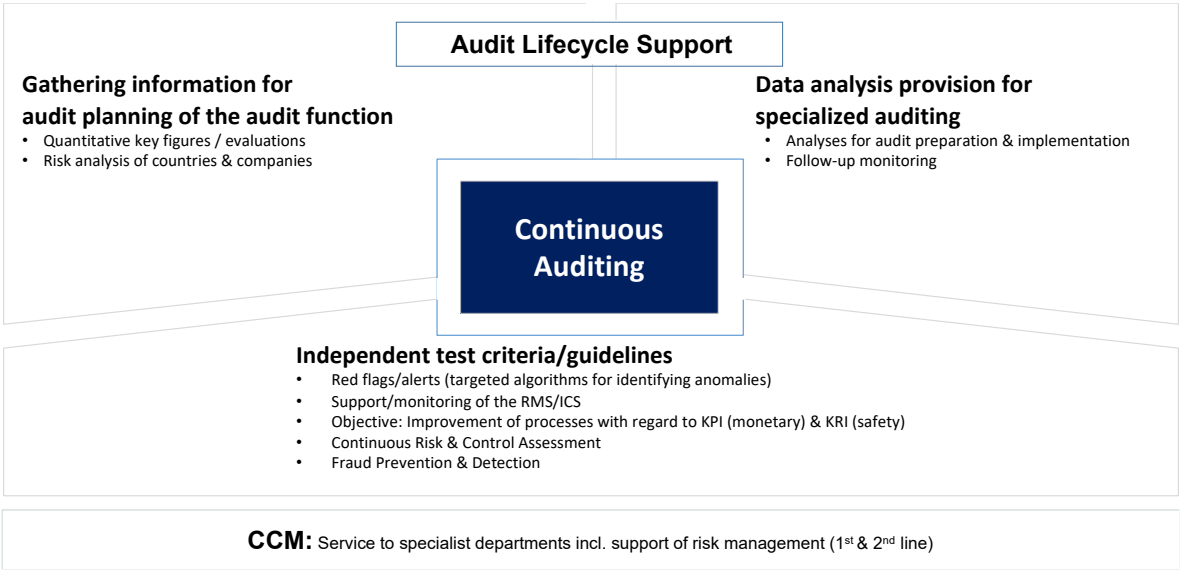
The results derived from the use of CA are primarily used by internal audit for the risk-oriented and efficient planning and execution of audit activities. They can also be used for clarifying any anomalies with the departments at a later date and, depending on interest, can also be made available to the department. Should

[5] Cf. „Antwort der Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Publication Berlin, p. 130 ff.

[6] Cf. Chapter 4.1.1 Audit Lifecycle Support.

the department wish to carry out further analysis, these activities are to be performed by the department itself. It is clearly stated that internal audit carries out its auditing activities independently and objectively and does not take on any commissioned work from the respective departments that might jeopardize its independence and objectivity.[7] Possibilities for collaboration between internal audit and other (audited) organizational units are presented in Chapter 3.3 Collaboration models.

Fig. 2: Characteristics of CA-Systems[8]



1.2 Goals and added values

Due to the constant digitization and automation of business processes and transactions, as well as the extensive support provided by IT services. Internal audit today has large volumes of data at its disposal, which can be used as a source for more in-depth data analysis. The progressive penetration of products and processes with IT has created completely new control and monitoring mechanisms.

[7] Cf. Standards 1100 Independence and Objectivity in the International Standards for the Professional Practice of Internal Auditing 2017.

[8] Cf. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Publication Berlin, p. 130 ff.

In addition, new subject areas are emerging for which suitable control, steering and monitoring mechanisms must be implemented.

The introduction and use of the CA approach described here leads to several audit-related improvement potentials, which are depicted in the following diagram:

Fig. 3: Improvement potential through Continuous Auditing[9]

Time	➢ Continuous risk assessment and follow-up tracking ➢ Timely identification of weaknesses in the RMS / ICS ➢ Timely execution of analyses based on current and historical data ➢ Reduction of audit duration
Efficiency	➢ Concentration on essential facts ➢ Reusability ➢ Efficient use of resources
Quality	➢ Increase in audit reliability ➢ High risk coverage ➢ Reduction of errors
Added value	➢ Continuous monitoring leads to timely process improvements ➢ Increased overall process knowledge strengthens focus on key risk areas ➢ Increase in the degree of coverage of audit fields or the depth of audits

Furthermore, through consideration as an addressee of the analyses, CA can also provide direct added value for the first- and second-line departments.[10]

The use of CA, specifically the ongoing control and monitoring actions or risk assessments, lead to:

- a regular adjustment of the annual audit plan in terms of effective rolling audit planning based on valid information about changes in the company's risk landscape,

[9] According to „Antwort der Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Publication Berlin, p. 130 ff; RMS/IKS: Risikomanagement/Internes Kontrollsystem.

[10] Cf. The three-line model in the IIA's position paper on https://www.diir.de/fachwissen/iia-und-eciia-publikationen/ (Date: 13.02.2021).

- more target-oriented definition of the audit scope as part of the standard audits from the annual audit plan, since data collected during the year is already available in the internal audit department,
- the identification of necessary ad hoc/special audits due to extraordinary developments in business units, and
- ongoing communication between the responsible management of the business units and internal audit, ultimately leading to a better understanding requirements and tasks.[11]

1.3 General CA-definitions

The use of the term CA already has a history of almost 30 years. As early as 1989, Vasarhelyi introduced a continuous process auditing system at AT&T Bell Laboratories. It was used to analyze large (paperless) databases.[12] A first definition of the term was given by the CICA/AICPA Associations[13] in a joint research report in 1999, which is regarded as the basis of the most widespread understanding of Continuous Auditing.[14]

The core statement is that CA enables an independent auditor to use relevant and current data (based on monitored events) to derive the need for action and to perform specific audit procedures. In addition, later publications on CA definitions introduce the information technology component, which is presented as an important part of the ongoing data collection and processing in the given context. The definition is also expanded to include data sources and the use of information in conjunction with risk-oriented audit planning and execution.

The IIA[15] also introduced a definition during the publication of the Global Technology Audit Guide on Continuous Auditing (2nd Edition) in 2015: "Continuous auditing – the

[11] Cf. Online Audit Manual, DIIR Working Group in MaRisk, December 2017.
[12] Vasarhelyi, M. A.: The Continuous Audit of Online Systems (https://www.researchgate.net/publication/255667612_The_Continuous_Audit_of_Online_Systems, Date: 14.08.2019).
[13] Canadian Institute of Accountants (CICA), American Institute of CPAs (AICPA).
[14] Cf. Eulerich, M./Kalinichenko, A.: Die Continuous Auditing-Diskussion aus wissenschaftlicher Sicht, in: ZIR 01/2014, p. 34-44.
[15] The Institute of Internal Auditors (The IIA).

combination of technology-enabled ongoing risk and control assessments. Continuous auditing is designed to enable the internal auditor to report on subject matters within a much shorter timeframe than under the traditional retrospective approach."

It adds: "Continuous auditing comprises ongoing risk and control assessments, enabled by technology and facilitated by a new audit paradigm that is shifting from periodic evaluations of risks and controls based on a sample of transactions, to ongoing evaluations based on a larger proportion of transactions. Continuous auditing also includes the analysis of other data sources that can reveal outliers in business systems, such as security levels, logging, incidents, unstructured data, and changes to IT configurations, application controls, and segregation of duty controls."[16]

Although CA has been present in the literature for almost three decades, a commonly accepted unified definition and associated understanding has not been established. Thus, the existing definitions contain differences that allow for divergent interpretations. For this reason, the DIIR working group in Continuous Auditing has decided to derive its own practice-oriented CA-definition, based on the IIA's presentation, as a basis for further discussion (see Figure 4).

Fig. 4: Practice-oriented CA-definition of the DIIR working group in Continuous Auditing[17]

Practice-oriented CA-definition of the DIIR working group in Continuous Auditing
CA is the combination of risk and control assessments throughout the audit lifecycle, which are supported by machines and carried out in repetitive intervals depending on the indicators used and the risk at hand. *The use of CA increases the effectiveness and efficiency of internal auditing by enabling the audit function - compared to the traditional audit approach - to identify audit items that deviate from the target state earlier and by supporting it in carrying out audits more quickly.*

[16] Cf. Institute of Internal Auditors (IIA): Global Technology Audit Guide (GTAG) Coordinating, Continuous Auditing and Monitoring to Provide Continuous Assurance, 2. Ed. 2015 (https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG3.aspx, date: 14.08.2019).

[17] Ebd.

In addition, CA includes the definition of a group of addressees for the transfer of the (audit) results obtained and the initialization of (follow-up) measures.

To take full advantage of CA, it is necessary to conduct regular reviews and make any necessary adjustments.

In addition, the working group defines an indicator in the context of the practice-oriented CA definition as any results generated based on specified parameters/variables using analysis logics.[18]

An example of an indicator is "Goods returned > €5 million". Here, the €5 million represents the parameter and the ">" character represents the analysis logic. Both the analysis logic and the parameters can be extended as required.

Finally, a distinction is made between CA and CM: The IIA defines CM as ongoing first- and second-line activities to ensure that rules, processes, and business procedures are effectively implemented or performed as components of the Internal Control System (ICS). The activities include the identification of applicable control objectives and evaluation criteria, as well as the implementation of automated test actions to identify activities and transactions that do not comply with defined requirements.[19] Thus, the distinction is primarily related to the group of people responsible at various levels of the three lines (see also chapter 3.2 "Classification in the three-line model").

The main components of CA are the Continuous Controls Assessment (CCA) and the Continuous Risk Assessment (CRA). In terms of content, CCA is closer to CM in that it describes the assessment of the effectiveness of the essential components of the ICS. During the CRA, potential risks to the company are assessed, incorporating the probability of their occurrence and their impact. On this basis, the necessary focus and prioritization are derived, including those for the activities of internal auditing.

[18] Ibid.

[19] Cf. Institute of Internal Auditors (IIA): Global Technology Audit Guide (GTAG) Coordinating, Continuous Auditing and Monitoring to Provide Continuous Assurance, 2. Ed., 2015 (https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG3.aspx, date: 14.08.2019).

2 Framework conditions for CA-Systems

As already presented in the previous chapters, the application of CA methods is an important factor in shaping internal auditing for the future. The increase in value added by a CA-System under optimized conditions can be justified in several ways: Qualitatively better findings, an associated higher validity of the conclusions drawn, and a higher acceptance by the addressees. However, the introduction of a CA-System is also associated with fundamental challenges. The following descriptions partly reflect aspects from the use of data analysis. To begin with, the requirements for the application of CA will be discussed.

In the first step, it is crucial to define the desired output (in this case, the KAI), which can then trigger audit actions in the second step. When introducing CA-Systems, structured data from existing ERP systems and/or databases is primarily used.[20] However, it is also possible to evaluate unstructured data.

Examples of qualitative or unstructured data include images, video clips, scanned business documents, notes, or PowerPoint presentations, which can come from both internal and external data sources. The continuously growing use of social media generates messages, comments, chats, or forum posts in unstructured or at least semi-structured form. In contrast to structured data, unstructured data must first be converted into an analyzable, structured form.

Once the hurdles in the analysis of unstructured data have been overcome, the company has access to further relevant information (depending on the analyzed database), for example about customers, business partners, the industry, or its own business processes. The information obtained must be interpreted (e.g., from a business perspective) in order to derive findings for the audit lifecycle. The combination of new information with existing, structured data (e.g., company data, economic data, market data) provides additional analysis options.

[20] Examples are order data, sales data or access authorizations of users.

External data sources also provide supplementary information for possible CA scenarios, e.g., by analyzing discussions in social networks about one's own company. If an important or relevant topic is identified, it can be examined in greater detail as part of new audit reviews. News and its effects on the company's own share price or the sales behavior of products can also be determined as part of analyses of unstructured data. But even with internal data sources, there are various ways to use them, e.g.:

- Analysis of submitted claim reports associated with approved compensation payments regarding clusters to detect potential employee fraud at insurance companies.
- Analysis of frequently occurring incidents, e.g., at the hotline, which hint at overarching problems.
- Analysis for clustering of changes in the protection needs of an application/IT asset to identify changing functional scopes or insufficient knowledge regarding the information being processed.

The amount of unstructured data and the high number of data sources will continue to grow in the future and the ability to draw relevant insights from such data will become an increasingly important potential competitive advantage for companies in the course of this.

In principle, certain framework conditions must be considered when using Continuous Auditing. These are explained in the following chapter.

2.1 Legal and organizational framework

CA activities must not violate applicable law as well as legal norms and internal regulations, respectively. At best, all relevant regulations are known before the start of productive CA operations and have already been checked for compliance. Existing regulatory gaps might be addressed using a company agreement, for example. The following questions can provide guidance:

- Does a company agreement exist in which the performance of (mass) data analyses have already been regulated? Does this company agreement also include continuous data analyses?
- Has the approval of the departments responsible for data generation been obtained for the use of the data in CA processes?

- Does the central consolidation of data from different source systems in a DWH (data warehouse) contradict existing agreements/regulations? Is it legitimate for audit staff to have access at any time?
- Are there any data-protection restrictions on the central consolidation of data from different countries in a data warehouse?
- Has adequate documentation been prepared for the selected procedure within the CA-System to ensure compliance with legal evidence-retention requirements (e.g., EU General Data Protection Regulation)?

In addition to the legal challenges, there are also organizational ones. For internal audit, this may mean that—wherever CA deviates from a traditional audit—existing process guidelines need to be expanded. In larger companies, it could be expedient and sensible to set up an independent CA unit. The support processes, interfaces, tasks and responsibilities as well as their boundaries to other auditing units should be defined in this context. Since CA has company-wide implications, all directly and indirectly involved areas of a company (including specialist departments, IT, compliance, data protection, works council) should be included both during concept development and in operational use.

When designing a CA-System, industry-specific regulatory requirements or cross-industry standards may need to be taken into account. These include the International Standards of the Institute of Internal Auditors (IIA),[21] which aim among other things, to ensure the independence of the internal audit process."

2.2 Content and methodological framework

As part of the introduction of a CA-System, the first step is to identify relevant KAIs, define them professionally in a meaningful way, and check their feasibility. This is also one of the most important content-related challenges.

The term "professionally meaningful" is to be understood as meaning that

[21] https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Standards__Version_6.1___20180110.pdf (date: 13.02.2021).

- a KAI measures with sufficient validity, one or more risks and/or performance targets relevant for the company ("causality") rather than merely capturing a coincidental or weak statistical relationship ("correlation").
- a predefined goal, for example one derived from the corporate strategy - is to be achieved and the degree of attainment can be measured using KAI (e.g., at least 75 % of all material orders are to be automated).

By "feasibility" it can be understood, for example, that

- the required data are available in sufficient quality, with adequatly long histories and must remain reliable in the future; existing data gaps must be capable of being properly addressed. (Accordingly, any identified data gaps or anomalies may themselves constitute an audit finding.)
- the commitment to obtaining data and validating the trustworthiness of data sources is acceptable.
- the required technical data transformations and calculations can take place with an appropriate (time) commitment.

Furthermore, internal audit and the respective department should agree on a precise definition of the KAI, including the follow-up actions to be taken if a threshold is exceeded (e.g. initiating a special audit). Such clarity will increase acceptance of the proposed approach.

Setting thresholds for KAIs is a major methodological challenge. Threshold values can either be defined (e.g., through expert judgement or top-down specification) or calculated using statistical methods based on existing data. In practice, threshold values should be reviewed and adjusted regularly (at defined intervals) or, if necessary, on an ad hoc basis, since

- a threshold that is too low causes too many anomalies resulting in excessive effort and unnecessarily follow-up activities,
- a threshold that is too high may generate too few anomalies leading to insufficient risk coverage and too few follow-up activities.

Therefore, internal audit staff should ideally possess sufficient statistical expertise to ensure a methodologically sound approach.

2.3 Technical framework

Since the availability of electronic data for CA-activities may be limited initially, key technical challenges lie in the acquisition, preparation, and provision of all required internal and, where applicable, external data. Ideally, the data should be available in an internal or organization-wide DWH,

- in which the data are modeled according to the intended use,
- in which the data is updated at appropriate intervals,
- that supports the required (data) processing speed,
- and whose data delivery processes are clearly defined and controlled, enabling continuous statements on data quality (e.g., completeness, accuracy, integrity, timeliness).

The complexity of setting up and operating a DWH increases when a heterogeneous IT application landscape exists within the organization (e.g., SAP, non-SAP) or processes are supported by decentralized data processing (e.g., Microsoft Excel) with their own data sets. Even in a homogeneous system landscape, DWH data modeling remains complex if identical systems are configured or applied differently. Furthermore, when operating the DWH, it must be considered noted that both changes in the IT application landscape (e.g., decommioning or upgrading existing applications or implementing new ones) and changes that affect data generation (e.g. process changes) must always be assessed for their potential impact on the DWH. These developments also require adjustments to the automated CA analyses within the CA (e.g., modifying or replacing a KAI).

Internal auditors should also be proficient in visualization and analysis tools (e.g., for process mining or statistical methods), which ideally allow direct access to the DWH.

An alternative way of using data is to set up and use read-only permissions to pre-existing analytics in essential core systems or analytics tools, and/or an existing first or second line DWH.

2.4 Personnel framework

The framework described above inevitably lead to the challenge that internal audit must be adequately staffed with personnel who possess the appropriate skillsets. In addition to technical and statistical expertise, knowledge of data analysis techniques and data protection regulations, the organization's own processes and an understanding of the business model are essential. Skills in data visualization and strong communication abilities - particularly in interactions with departments and stakeholders - are also of considerable importance. In recent years, the terms "Data Science" (as an overarching concept for these competencies) or “Data Scientist” (as a corresponding job profile) have become widely established. Clearly, not every auditor can and should qualify as a Data Scientist; likewise not every Data Scientist brings extensive auditing experience. A combined team – with complementary competencies and ideally subject matter experts e.g., in sales or accounting – supported by a regular knowledge exchange, represents an effective and necessary approach.

Attracting experienced employees—both for the company in general or for internal audit in particular—is currently a significant challenge in many organizations. From a Data Scientist’s perspective, CA projects can enhance the appeal of working in internal audit, almost as a positive side effect.

2.5 Side note: Data protection/security

The large scale (mass) processing of data also requires careful consideration of the applicable legal framework. The guidelines issued by the DIIR working group in Internal Audit & Data Protection[22] may be helpful to this regard.

In principle, the scope of data to be analyzed should be defined and limited as much as possible within the respective context (even if this conflict with the analysis objective). Access to the data should be restricted to a clearly defined group of individuals and a deletion concept must be in place. Moreover, when conducting the analysis, it is essential to ensure that all relevant steps are documented appropriately.

[22] Cf. Guide to Internal Audit and Data Protection at https://www.diir.de/arbeitskreise/interne-revision-datenschutz/veroeffentlichungen/ (date: 13.02.2021)

Several questions arise from the applicable legal framework:

- Has the limitation of the data processing purpose been ensured?
- Has an assessment been carried out to determine whether personal data or even special categories of personal data are being processed?
- Have the various interests been appropriately balanced?
- Is personal data anonymized or at least pseudonymized before processing?
- Is the need-to-know principle applied consistently?
- Are agreements on commissioned data processing (processor contracts) necessary when involving external experts?
- Has a data protection impact assessment been conducted where it is mandatory?

Internal audit should consider establishing a fundamentally coordinated procedure with the Data Protection Officer and, where necessary, the Works Council, and should also coordinate with them on a case-by-case basis. A company-wide agreement can be used to define the applicable framework.

3 The role of Internal Audit

Internal audit operates – independently and objectively – as the organization’s monitoring function on behalf of the executive management or the supervisory board. The following chapter positions these responsibilities within the context of the three-line model and outline potential cooperation models.

3.1 Support for the company's objectives

As a third line, the central responsibility of internal audit is to identify potential for improvement within the company. This is ensured particularly by reviewing the effectiveness of the ICS, the RMS, and the design of the first and second lines.

Due to the increasing pressure to conduct audits efficiently and to deliver timely audit results, internal audit must adapt its methodological approach to effectively contribute to the achievement of the company's objectives.

3.2 Classification in the three-line model

As an updated version of the "three-lines of defense model", the three-line model has served as an organizational framework for governance design since 2020. Within this model, internal audit constitutes the third line. In this role, it assesses the effectiveness of the ICS, RMS, and monitoring measures in the first and second lines and identifies opportunities for improvement. Given its mandate within the organization, internal audit is a key driver for implementing

Continuous Auditing and periodic audit methods to efficiently perform ongoing monitoring activities and risk assessments.[23]

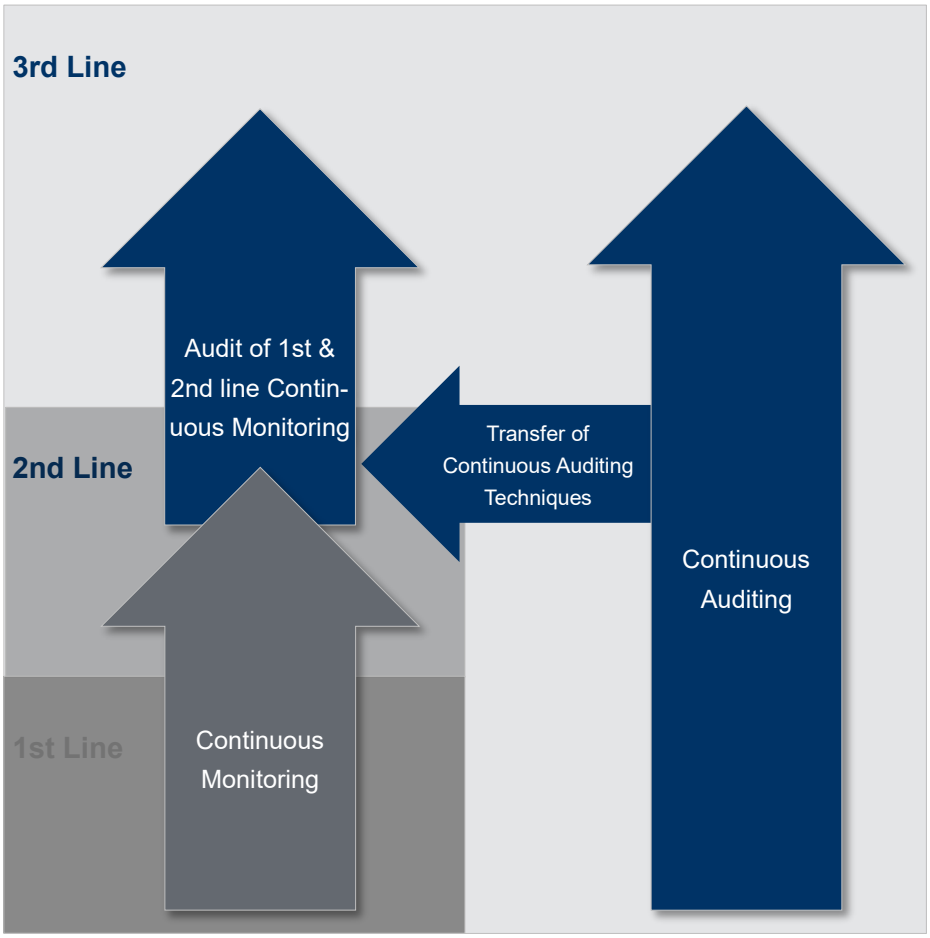


Fig. 5: CA in the context of the three-line model[24]

Any form of cooperation between internal audit and other departments is feasible as long as first and second line responsibility (definition of processes, assessment of risks, control of compliance) is not delegated to internal audit. If the interaction points between internal audit and the departments are clearly defined, CA strengthens internal company collaboration and functionality.

[23] Cf. Online Audit Manual, DIIR working group in MaRisk, December 2017.

[24] Based on: Institute of Internal Auditors (IIA): Continuous Auditing: Coordinating Continuous Auditing and Monitoring to provide Continuous Assurance, 2nd Ed., p. 11.

In the following chapter, some possible collaboration models are presented in more detail.

3.3 Collaboration models

The integration of departments into the CA-System and the associated distribution of roles is often subject of controversial discussion. Specifically, the question of whether internal audit, in its role as the third line, may or should provide analysis logics and analysis results from the first and second lines is being discussed. Arguments such as endangering the independence of internal auditing, or the lack of auditability and reliability of analyses developed internally often oppose the idea of joint process improvement and the realization of potential synergy effects through the collaborative approach of combining departmental expertise and the perspective of internal auditing.

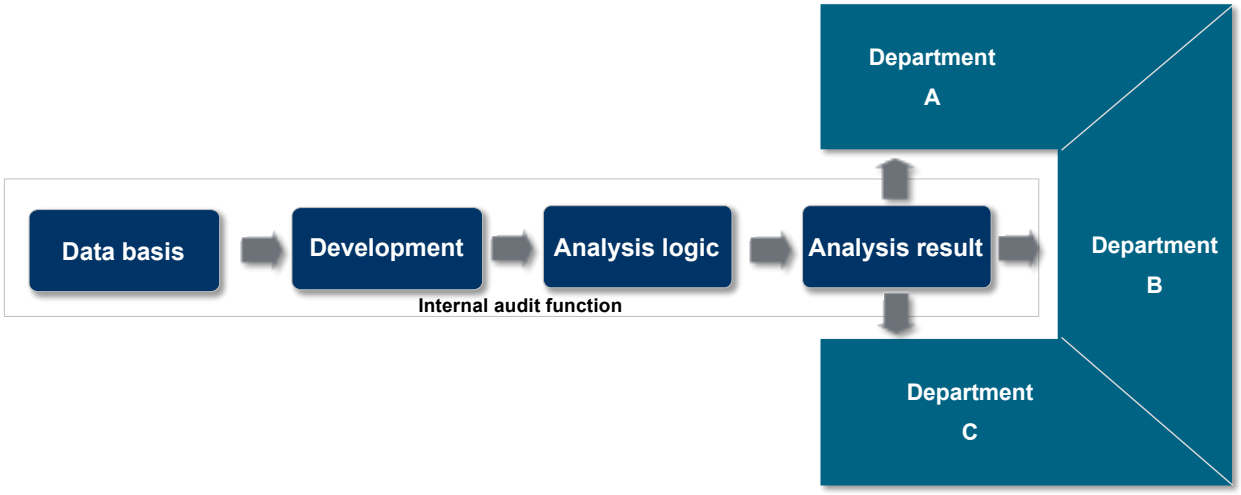
When implementing a CA-approach it is essential to consider the interdependencies between the characteristics of continuous monitoring processes by a department in the first or second line and the characteristics of CA by internal audit. For example, expanding CA-activities is particularly effective in areas where the respective department has not yet implemented CM processes. The same applies in reverse. In this context, it is always necessary to analyze across companies whether monitoring activities are duplicated, which do not increase process and control security, but rather cause additional costs.

The following three scenarios for the design of collaboration differ essentially in the scope of responsibility for process steps and results. In principle, all three scenarios can be applied and are used in practice. The guiding principle for the detailed design of collaboration models should be the preservation of internal audit's independence.

Scenario 1: Internal audit as service provider for analysis results

The departments (e.g., Procurement, Production, Sales, Human Resources) serve as recipients of the analysis results, which are based on the analysis models developed in internal auditing. These analysis results can, for example, provide evidence of effective control implementation as part of second-line risk management or support the classic operational ICS.

Fig. 6: Internal Audit as a service provider for analysis results



Scenario 1 requires a collaboration model that clearly defines responsibilities and unambiguously sets out the tasks of those involved in the process. It is imperative that the analyses developed by internal audit deliver reliable results. In particular, the completeness and accuracy of the underlying data basis must be ensured by internal auditing with the greatest possible care. The processing of results is carried out by the departments, but they are required to approach internal audit in the event of serious complaints. This active supply of the first and second line from the CA-System of internal audit requires, for example, a strict separation into a CA-workflow (audit indicators) and a CM-workflow (departmental indicators).

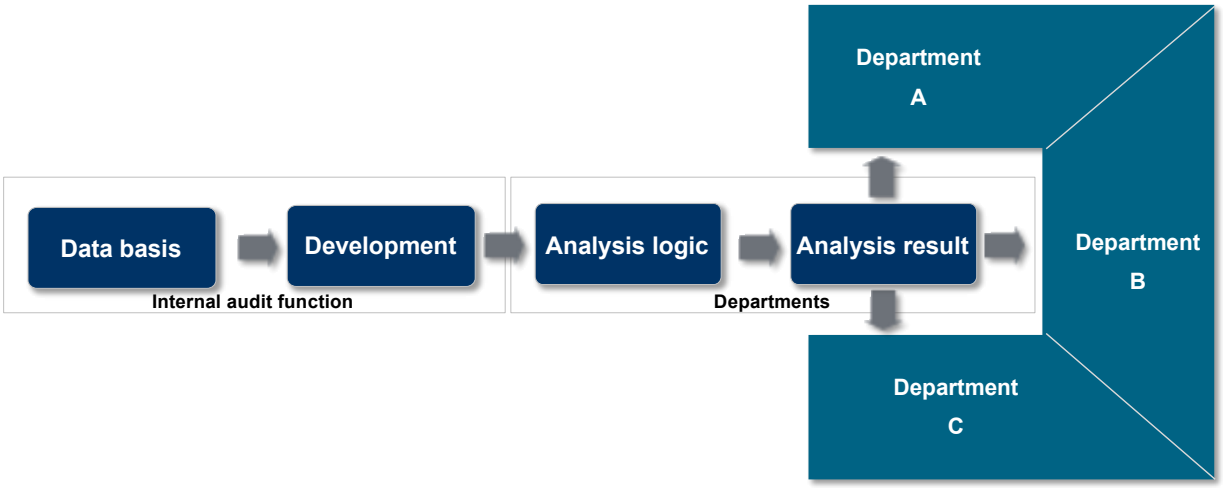
In such a service model, internal audit may no longer be independent if the first and second lines do not assume responsibility for the content of the analysis results. Independence certainly exists if the analysis results provided are used in addition to the existing ICS/RMS of the first and second line or if the analysis results are provided as part of audits. A possible implementation option would be for internal audit to use its analysis tools to create a list of results (containing, for example, false positives or irrelevant results) and to provide these results to the first and second lines for further analysis. The review of the results could take place continuously and be documented in an audit report.

Scenario 2: Provision of developed analysis logics to the departments

Another approach is to allow departments to benefit from findings from audits in which data analytics have been used. This involves

making the analysis logics available, e.g., in the form of a set of indicators, for full adoption in the departmental systems or first- and second-line monitoring/analysis tools used.

Fig. 7: Provision of developed analysis logics to the departments

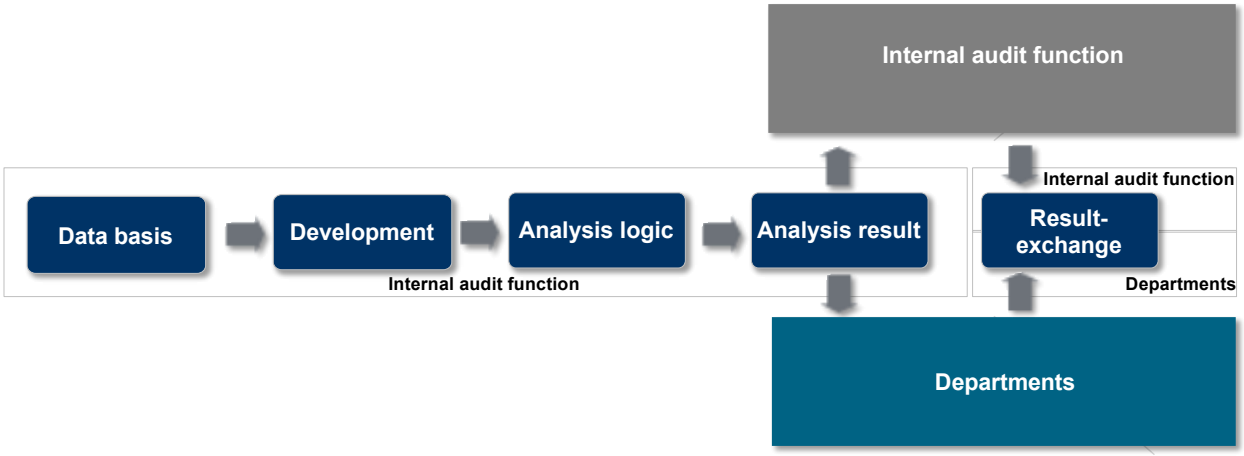


For example, the KAI "invoice receipt before purchase order" is transferred to accounting and will be used continuously in the accounts payable ERP system in the future. At this point, however, it is crucial that the responsibility for the correctness and completeness of the analysis logic is transferred to the specialist department. Any further development of the analysis logic, including the definition of threshold values and future adjustments to process changes, must be carried out exclusively by the specialist department. This ensures that these audit fields can also be audited in the future without any conflict of interest. A clear transfer of responsibility must ensure that internal auditing does not become part of the ICS of the specialist department.

Scenario 3: Collaborative approach

Apart from the previously described scenarios, it is possible for analysis results to be used simultaneously by both specialist departments and internal audit. While specialist departments focus on conventional control objectives, internal audit additionally assesses audit-specific objectives. These include, for example, risk cover-age, performance-related targets, or the evaluation of interactions with other departments. The specialist department evaluates the results of the analysis considering its predefined control objectives, e.g., compliance with process specifications.

Fig. 8: Partnership approach



In this particular scenario, cross-departmental process optimization potential is combined with process-integrated departmental aspects. An exchange on the analytic results is absolutely essential.

4 Supporting the use of CA in audit practice

After defining and describing CA and embedding CA in the company's governance model, the following chapters focus on its application. This is based on examples of various support options both within and outside the standard auditing process. The purpose of the presentation is to deliver concrete suggestions and possible applications in order to be able to use the defined approach in a practical and individually adaptable manner.

4.1 CA-support in the standard audit process

CA offers a standard audit process that can be applied in individual phases of the audit lifecycle[25] and throughout the entire process, ranging from planning to follow-up.

[25] Cf. DIIR Position Paper „Risikoorientierte Prüfungsplanung“, DIIR 2010.

4.1.1 Audit lifecycle support

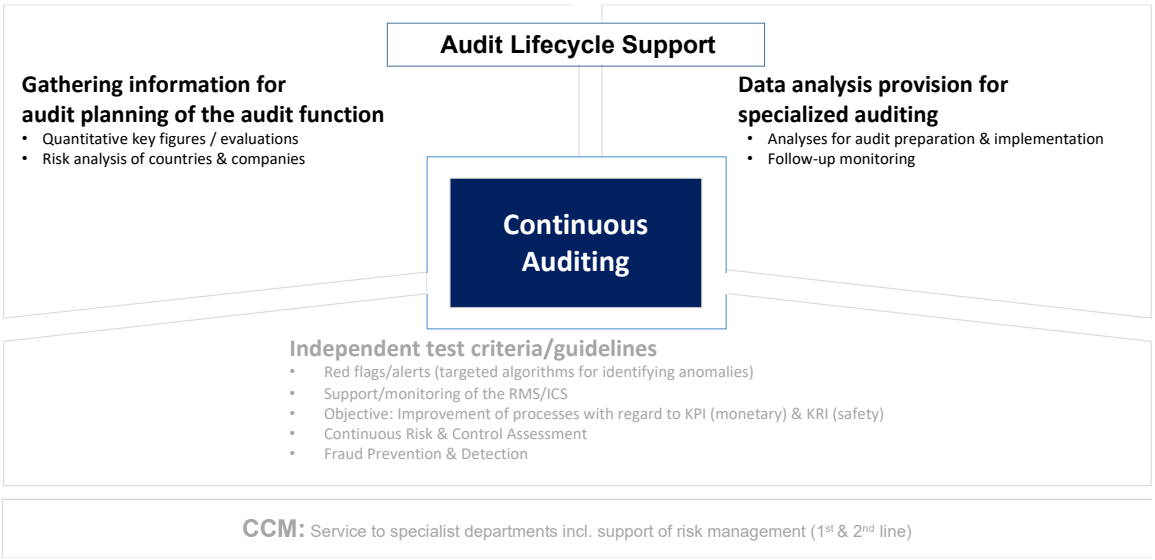


Fig. 9: Characteristics of CA Systems - Audit lifecycle support[26]

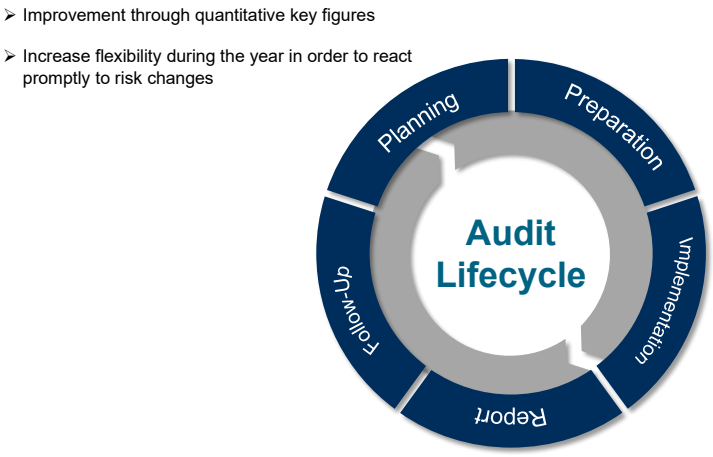
Planning

Risk-based audit planning includes the identification of audit objects, risk assessment, prioritization based on risk, and the design of the audit program.[27]

[26] Cf. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Publication Berlin, p. 130ff.

[27] Cf. DIIR Position Paper „Risikoorientierte Prüfungsplanung“, DIIR 2010.

Fig. 10: The added value of CA for audit planning and preparation[28]



The use of CA leads to a timely adjustment in audit planning based on a continuous risk and control assessment. CA provides support for both the identification of audit objects and risk assessment. The information required for planning is collected from various sources to derive appropriate KAIs. With increasing digitization, electronic information in established IT applications primarily serves as a source, whereby data quality must be taken into account. An overview of possible information sources is shown in Appendix 1.

In addition, an initial risk assessment is carried out for newly identified audit objects. Threshold values are defined together with the KAIs so that any required action can be derived from the risk values. Thus, a distinction can be made between KAIs for the identification of audit objects and indicators for risk adjustment.

[28] Cf. „Der Mehrwert von Continuous Auditing für die Prüfungsplanung und -vorbereitung“, Gorschenin, E. et al., ZIR 03/2018, Erich Schmidt Publication Berlin, p. 140 ff.

Fig. 11: Examples of KAIs for identifying new audit items

KAIs for identifing new audit objects
Creation of new organizational units in the electronic organizational chart
Release of a new IT service in a configuration management database (CMDB)
Registration and approval of a new external service provider in the outsourcing management system
Approval of a new program or project in the project management system
Approval of a new product data record in the ERP system
Release of a new data record in the master data management system

Fig. 12: Examples of KAIs for adapting the risk assessment of audit objects in the purchasing process

KAIs for adapting the risk assessment of audit objects in the purchasing process
Change in the number of customers
Increase in the number of returns
Increase in the number of cancellations in the purchasing process
Increase in average distribution costs
Increase in incoming goods without an order
Increase in orders below release limits

If the threshold value of a KAI for identifying audit objects is exceeded (e.g., change to >0), the audit object must be included in the audit universe and an initial risk assessment must be performed. When the operation of an IT service is discontinued, a corresponding indicator (in this case <1) can be defined, which can trigger an archiving process of the associated audit object.

Several thresholds can be defined for risk change indicators (e.g., for an early warning vs. direct need for action). The early warning can serve as a trigger for a deeper consideration of the audit object, while the threshold

for the need for action triggers an update of the risk classification of the audit object. The basis for this is the individually designed risk model of the applying company.

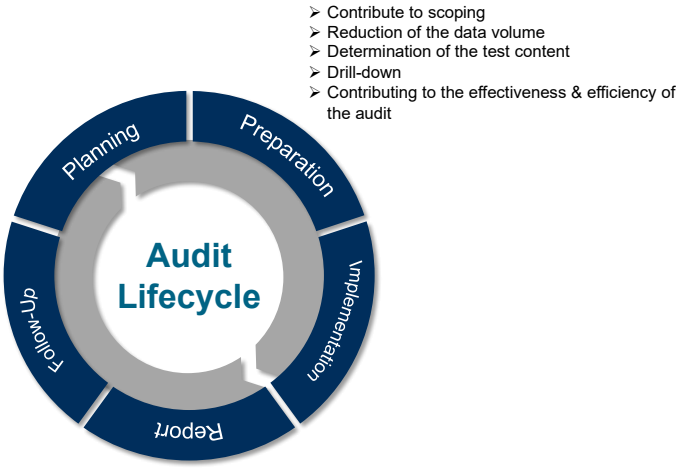
When deriving a KAI, a review of the circumstances that led to a defined threshold being reached is recommended. As expertise increases and any resulting adjustments are made, reassessments can also be successively automated, if required, by considering the size of the company and the purpose of the application. Later integration of machine learning processes for further refinement of the indication is possible.

Starting with a (quarterly) annual frequency, the update cycles for risk and the corresponding adjustments of the audit plan should be reduced gradually at first and the associated learning effects should be incorporated.

The targeted implementation of CA-Systems leads to faster adjustments in risk-based audit planning through continuous and detailed information. There are opportunities to update risk assessments in a timely manner and to automate the risk-based audit planning process making the overall internal audit process more effective.

Preparation

Fig. 13: The added value of CA for audit preparation[29]



[29] Cf. „Der Mehrwert von Continuous Auditing für die Prüfungsplanung und -vorbereitung“, Gorschenin, E. et al., ZIR 03/2018, Erich Schmidt Publication Berlin, p. 140 ff.

In the audit preparation phase, the scoping (of the audit objects) is specified in more detail and thereby the precise audit content is defined before starting the audit procedures. In the traditional audit approach, the preparation phase ends with a detailed audit plan,[30] which contains a prioritization or a selection of audit procedures to be performed. This can be, for example, a pre-selection of controls from a risk-control matrix. The audit preparation serves in particular to develop a written plan with regard to objectives, scope, schedule, and allocated resources (IIA Standard 2200).[31] The KAIs used within the CA-System support the definition of the audit content by identifying potential risk areas or deriving audit questions, among other things. This increases the quality of the audit (see appendices 2-4).

CA also allows the scope of the audit to be reduced, e.g., by focusing on risk-relevant business units, business areas, or business transactions. If the validity of the KAIs is not confirmed during the audit, they must be corrected or refined.

CA can also deliver the added value sought in an agile audit approach by performing a risk-based preselection of audit objects. Based on the knowledge gained from the first sprints,[32] adjustments can be made to the KAIs if necessary to prioritize the subsequent sprints or to identify additional relevant audit objects or to reprioritize or, if necessary, delete audit objects that are already in focus.

Implementation

When conducting internal audits, a CA-System can add considerable value, given that the analysis of KAIs provides the audit team with in-depth knowledge of the audit subject right at the start of the fieldwork phase, which would otherwise only be available at a later point in time or not at all. In the execution phase, the audit team gathers further information, including through interviews and document analysis, prepares evaluations, and can also use this information to understand the business transactions that were identified based on KAIs.

The combination of existing KAIs from different areas, such as

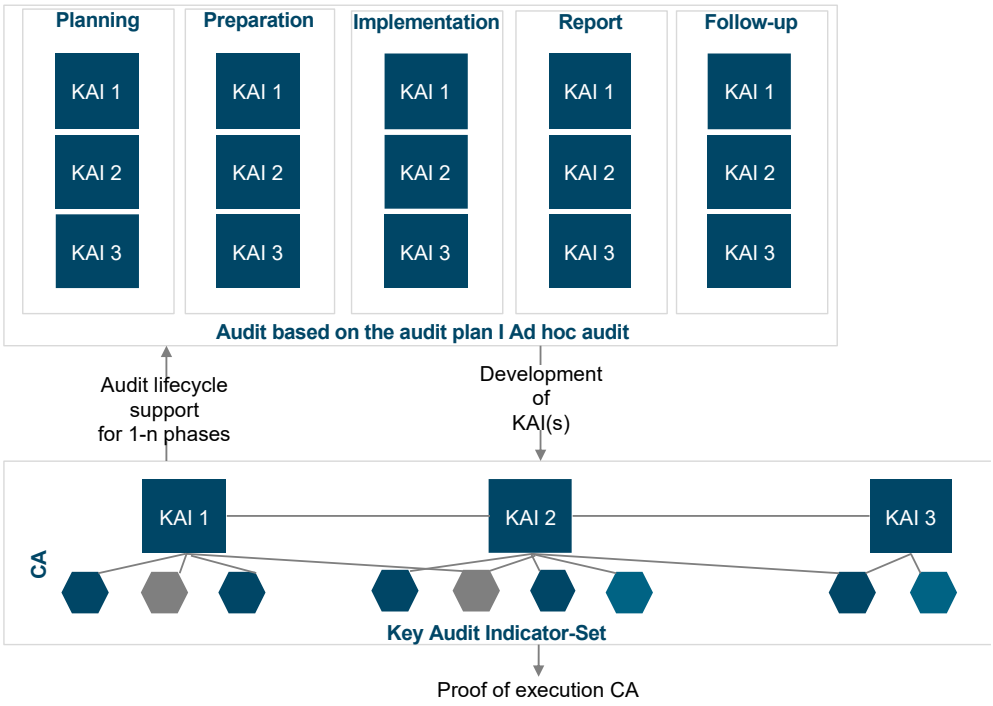
[30] Cf. Amling, T./Bantleon, U., 2007, p. 75.

[31] Cf. DIIR - Deutsches Institut für Interne Revision e.V., International Standards for the Professional Practice of Internal Auditing, Standard 2200 Planning individual engagements.

[32] A sprint is to be understood here as a run with a specified period of time in which a specified plan to search for a goal is implemented.

finance and procurement, facilitates a cross-divisional understanding that would not have been possible without a CA-System or through focusing on a specific audit field in a business area. This may facilitate the root cause analysis for anomalies and enable the identification of process optimization potentials for a process chain in its entirety. After analyzing the KAIs, an audit team can expand its audit questions and select conspicuous individual cases. With the help of an established CA-System, the database of the KAIs is usually available, so that a deliberate sample selection based on conspicuousness criteria, or a random selection based on the determined population can be made. The combination of indicators with the classical audit procedures provides enhanced added value for the implementation.

Fig. 14: Audit Lifecycle-Support through a Key Audit Indicator-Set[33]

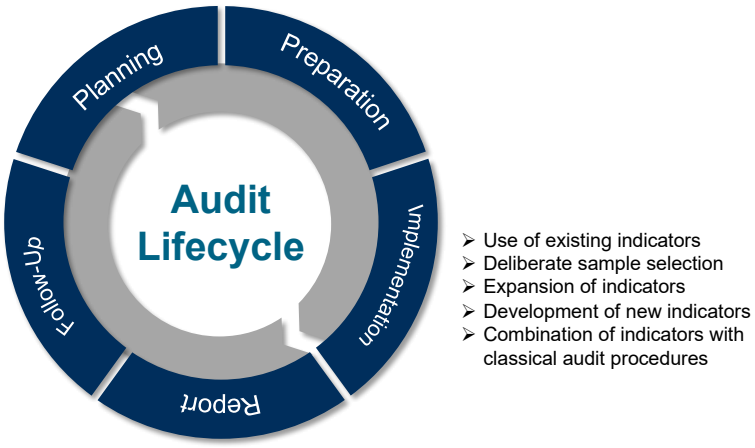


In addition, the implementation phase is essential for a CA-System for adapting an existing set of indicators and/or for expanding this set with new KAIs. The use of unique data analyses and the analysis of the audit object result in KAIs which will be useful for the phases of the audit lifecycle in the future, if necessary, in combination with the existing KAIs. Thus, the implementation phase is the idea generator for the (further) development of KAIs.

[33] Cf. Bauch, Kriegelstein: Die inverse Beziehung zwischen „Continuous Auditing und der Digitalisierung“, Specialist lecture DIIR Digitale Tage 2019.

Another option for the audit implementation phase is the process-supported continuous provision of data analysis logics and/or -results, possibly by a central data analysis department within internal audit. According to the CA definition of the working group[34] the repetition frequency depends on the underlying risk and the indicators used. Accordingly, this provision or central access represents another variant that leads to an additional benefit for the existing audit lifecycle. During the creation of the audit process and the selection of the audit object (company, department, process) or corresponding systems, for example, a data analysis is generated by requesting specific data and sent to a central data analysis unit. This unit checks the plausibility of the analysis results and, in turn, makes the results available to the audit team for audit execution. If further or independent data analyses are performed in audits, the provision of a data analysis portfolio adapted to the existing corporate processes and system landscapes is another value-added task of a CA-System.

Fig. 15: The added value of CA for audit execution[35]



Report

The traditional report format in text form based on a KAI set can be supplemented with key figures and statistics within the scope of an audit process to provide the responsible

[34] Cf. Chapter 1.3, Fig. 4: Practice-oriented CA-definition of the DIIR working group in Continuous Auditing.

[35] Cf. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Publication Berlin, p. 237 ff.

departments and management boards with a visual aid in assessing the findings and measures and to better understand and classify the verbalized audit result. If the process is already based on the relevant KAI, the results can be carried over and supplemented with visualization.

In addition, automated reporting constitutes yet another potential application for the assistance provided by a CA-System. Besides the extension of existing reporting of an internal audit by selected KAIs, proof of implementation itself can also be generated. Such reporting shows the coverage of audit fields and processes by the existing KAIs and explains where conspicuities arose. The findings and recommendations of the audit activities that are initiated as a result, including in the form of future program audits and ad hoc audits, shall be appropriately linked to relevant KAIs.

Fig. 16: The added value of CA for the audit report[36]

In principle, the use of an increased number of existing KAIs can lead to a reduction in classic audit actions and results. The more KAIs are implemented, the more automated reporting can be pursued to the greatest extent possible, which might even represent a real-time analysis of corporate indicators and identify areas for further action Ultimately, current results can be visualized continuously in a dashboard or performance scorecard - supplemented by

[36] Ibid.

company or industry benchmarks, if necessary - and sent via specific e-mail notifications as required. In this way, audit managers are provided with information about their audit areas and, for example, addressees in the specialist department are notified simultaneously by e-mail about anomalies that need to be analyzed. In addition to individual reporting on the subject matter of the audit, which needs to be automated and standardized, higher-level reporting to management and stakeholders should also be considered.

Follow-Up

If data analyses are used in the context of internal audit audits, these data analysis logics, which have been developed once for the audit subject, can be used again in the context of follow-up as a means of making a reported implementation of measures measurable or verifiable.

Fig. 17: The added value of CA for follow-up[37]

- Monitoring of agreed & measurable measures
- Short-term reaction in case of lack of implementation "Follow-Up Monitoring".
- Exceeding of a threshold value initiates audit if necessary

In addition, the increase in KAIs assigned to an audit can reveal lack of implementation prior to reporting an implementation or after completion of action tracking, allowing for short-term response to these variations. Thus, after measures have been agreed upon, these same KAIs can be used to monitor the sustainable realization of measures. In the event of an increase in anomalies, an action can be taken, such as updating

[37] Cf. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Publication Berlin, p. 237ff. and Bauch, M., Kriegelstein-Sternfeld H., Die inverse Beziehung zwischen Continuous Auditing und der Digitalisierung, Specialist lecture DIIR Digitale Tage 2019.

the risk assessment or initiating an ad hoc audit. The continued use of KAIs can lead to the initiation of a follow up audit and the reintroduction of an audit item into the annual planning. This provides the opportunity to detect an increase in an assigned risk at an early stage, even after the completion of the action tracking, and to react more quickly with actions. Within the framework of the use of key figures for follow-up, the definition of different threshold values is one way of determining the depth of audit action depending on the risk. Not every anomaly should automatically lead to an escalation in the form of a follow-up audit. Figure 18 shows how measures can be defined depending on threshold values.

Fig. 18: Threshold values that result in different actions[38]

Action	Threshold	Description of action
Special audit	> 6 %	The department is informed that there is a need for action. Initiation of a timely special audit.
Examination based on the examination planning	>3 %	The department is informed that there is a need for action. The department receives feedback. Creation of an examination proposal.
Accompaniment	>2 %	The department is informed that there is a need for action. Exploratory talk. The department receives feedback.
Monitoring	>1 %	The department is informed that there is a need for action. The department receives feedback.
First line coverage	<=1 %	No need for action. The department carries out independent, continuous control activities in parallel.

By combining already implemented indicators with new KAIs, previously invisible correlations may become transparent, enabling the identification of potential for improvement. The development of KAIs for follow-up also offers the opportunity to support audit planning for subsequent periods with quantitative indicators. As explained, these indicators allow for increased flexibility during the year to be able to react promptly to changes in connection with the audit areas.

[38] Cf. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Publication Berlin, p. 237 ff.

4.1.2 Audit workflow support

Whereas the audit lifecycle support refers to KAIs that are to be used in addition to the conventional audit procedures (e.g. interview, process walkthrough) or replace these audit procedures to a certain extent or entirely, the use of a CA-System for audit workflow support provides, among other things, key figures that are used to support the audit process itself.

With the help of control variables such as audit duration, audit time consumption, audit status, and deviation from the target, each audit manager can be provided with a dashboard for the internal control of the respective audits. Based on a continuous updating of the key figures, the user can react immediately to any changes and, for example, reallocate the existing resources. The manual monitoring and control requirements can be reduced through using CA methods. By combining these internal control indicators with other indicators, such as the number of open follow-up-points[39] or their criticality, a comprehensive KAI reporting can be built up, which can be made available to the audit management, the management, or the board members at any time. The goal should be to implement a standardized reporting dashboard for each reporting level, which is continuously updated without manual intervention. The time-consuming manual creation of complex presentations for each reporting level on different occasions can thus be reduced. As a result, resources that have been freed up can be deployed differently.

[39] Number of open agreed measures and recommendations from audits carried out.

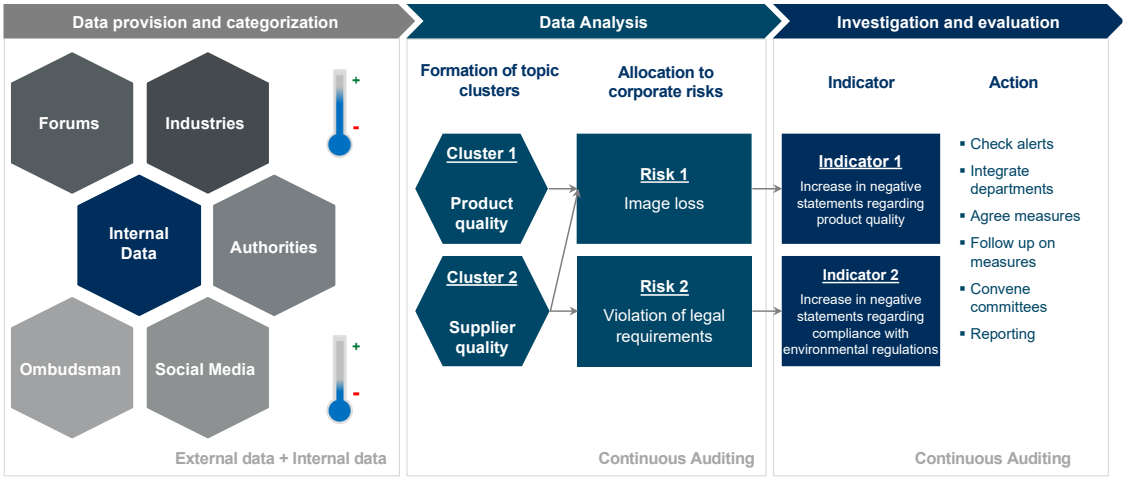
Fig. 19: Examples of audit workflow support

Agile planning & control	Individual dashboards for internal audit management for each audit manager using Key performance indicators such as audit duration and audit time consumption
Continuous Management Dashboard	Standardized management dashboards per reporting level (e.g., audit manager and executive board) Combination of internal control and other key figures, such as the number of open measures
Automated Approval Workflow	Automation of workflows for the approval of milestones
Automated Quality Management	Automation of controls of the internal control system of the internal audit / quality gates Automated quality checks, e.g. with regard to duplications and work errors in documents
Automated Issue Management	Automated daily screening of information from various data sources (including the Internet, external databases) using text mining to improve audit planning & preparation.
Knowledge Search	Creation of search functionalities to make content from audits, knowledge databases specifically accessible to all auditors
Digital Audit Approach	Digitization of audit guides/checklists & analysis of audit requirements in terms of automation or support by data analytics logics.
Sample Selection Tool	Sample selection based on conspicuousness criteria
Automated document tray	Automated systematic filing of documents provided, for example, by the auditee.
Unstructured Data Analyzing	Automated analysis of e.g. supplier & customer contracts with regard to certain check criteria (example: 2 signatures with corresponding authorizations available)
Automated Text-Mapping / Generation	Automated assignment of firmly defined topics to findings / generation of keywords for text passages and reports

Depending on the absence/existence of an IT infrastructure, for example in the form of an audit management system, there may also be a requirement to automate the manual approval workflow from planning to follow-up. This approval workflow is accompanied by quality assurance via so-called quality gates, which can be equated with certain milestones in the process. Using an automated workflow, the corresponding approval steps can thus be archived for each audit process, without any system discontinuities and in an unmodifiable format.

Another type of workflow support is provided by automated issue management. This involves continuous automated screening of external information from various data sources (including the Internet, external databases), which is facilitated with the help of text mining methods.

Fig. 20: Combination of internal & external data to form KAIs[40]



By combining external information such as news about key suppliers (including quality problems, raw material shortages), corporate/industry benchmarks, and geopolitical risks with internal information, the result can be used by the audit manager for audit planning in the form of key figures or risk notes. In addition, as part of audit preparation, information prepared per audit field can improve the creation of a work program. Furthermore, text mining algorithms can also be used for the automated assignment of firmly defined topics (assignment to audit fields, assignment of key words) to findings. Based on historical data, an algorithm can be taught to generate keywords that are assigned accordingly. This keyword generation method can in fact also be used for any text passages or complete reports.

In addition to a CA-System in the narrower sense that uses standardized KAIs, documents from the auditee that are received via a central storage location (drive, document management system) can also be processed automatically and systematically. In addition to filing, adding information (e.g. provision date) or unpacking, a filing overview can also be created that can be used as a central tracking document. This could also be used to create an automated match with the requested document. Furthermore, an e-mail update function can also be implemented that informs the review teams daily whether the requested documents have been provided completely and on time or are still outstanding even though the provision deadline has been reached.

[40] Bauch M., Kriegelstein-Sternfeld H.: Antwort der Revision auf komplexere Prüfungsanforderungen: Continuous Auditing, DIIR Congress, 15. November 2017.

The use of a CA-System in the form of audit workflow support means in the broadest sense that the degree of automation in the support processes is increased to increase the effectiveness and efficiency of an internal audit. The objective is to create a tool-based holistic view of internal auditing processes. One means to this end is so-called Robotic Process Automation (RPA), in which manual activities are trained by software robots, also known as bots, and will be carried out continuously and automatically in the future.[41]

4.2 CA support outside the standard internal auditing process

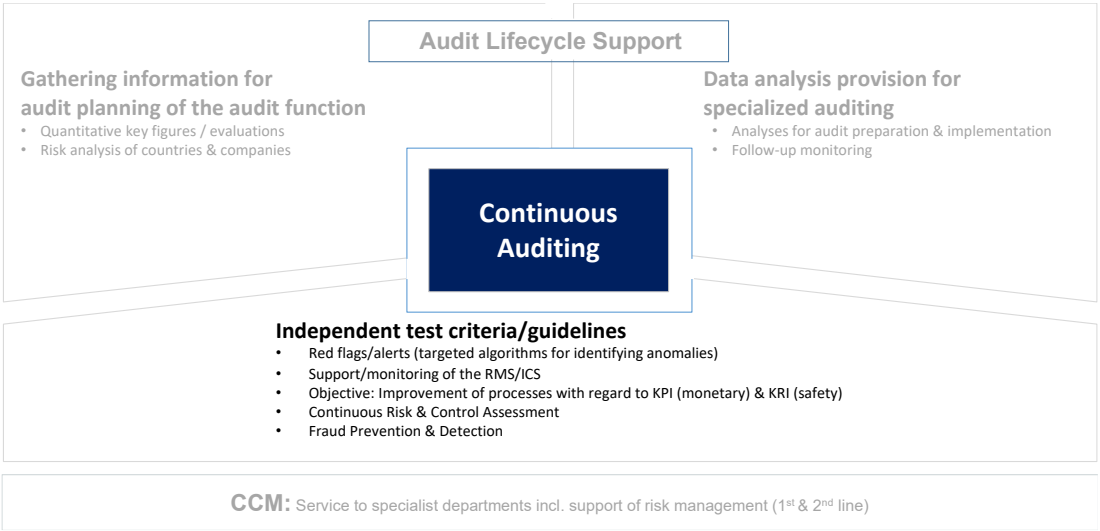
4.2.1 Overview of independent audit criteria / specifications

An essential characteristic of a CA-System is the use of independent audit criteria/specifications: This ultimately includes any KAIs that do not support the regular audit lifecycle but are used in addition to it and independently. Generally, structured data from ERP systems and/or databases used in the company form the basis of such a stand-alone CA-System. KAIs are mostly used as red flags or alerts. These are targeted algorithms for identifying anomalies in processes. Defining an anomaly is one of the greatest challenges. It can result from a KAI or from the combination of KAIs for which threshold values are to be stored. Even with such a stand-alone CA-System, it is crucial that these conspicuities are analyzed or checked, and appropriate measures/actions are derived. Depending on the collaboration model, an anomaly can be analyzed by internal audit and/or by the responsible departments (jointly). A possible target scenario for the use of independent audit criteria/guidelines is that the RMS/ICS is supported or monitored across departments (Continuous Risk & Control Assessment) to identify risks, among other things, which are ultimately to be controlled in the future through the downstream implementation of measures (risk control and

[41] Cf. Christian Czarnecki, Gunnar Auth: Prozessdigitalisierung durch Robotic Process Automation. In: Digitalisierung in Unternehmen: Von den theoretischen Ansätzen zur praktischen Umsetzung (= Angewandte Wirtschaftsinformatik). Springer Publication Wiesbaden, Wiesbaden 2018, ISBN 978-3-658-22773-9, p. 113-131, doi:10.1007/978-3-658-22773-9_7 (springer.com [retrieved on 14 August 2019]).

minimization). By mapping the implemented ICS, control gaps and weaknesses can be identified. Another objective is to leverage potential for improvement in terms of monetary aspects. A key success factor of a CA approach based on audit criteria is to combine data from different system sources to identify process gaps & weaknesses across departments. Depending on the CA design, it is possible, for example, to monitor anomalies in security levels, logging, incidents, IT configurations, application controls or aspects of functional separation and thus identify fraudulent activities[42] at an early stage.[43]

Fig. 21: Characteristics of CA-Systems[44]



4.2.2 Initiation of ad hoc audits using a CA-System

In addition to the use of KAIs for the audit lifecycle, a CA-System based on audit criteria represents a significant advantage for initiating ad hoc or special

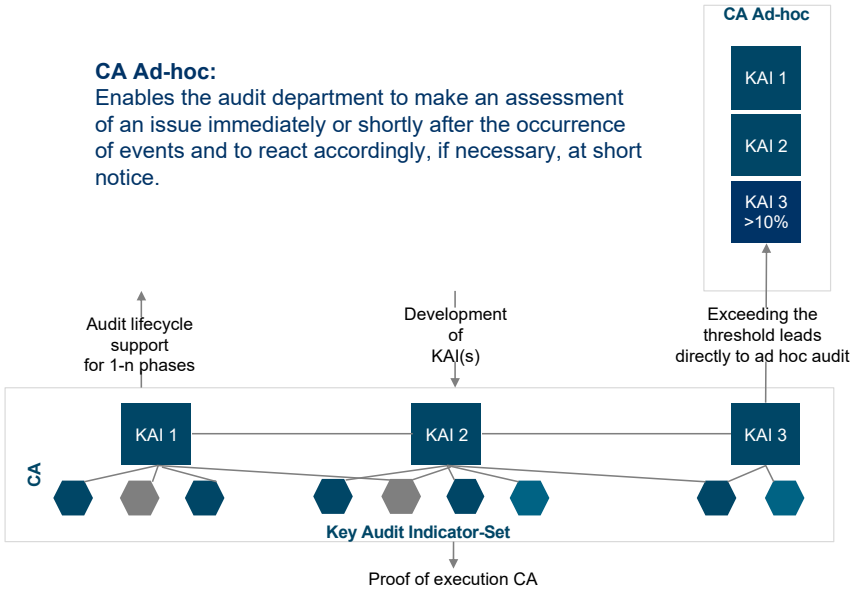
[42] Cf. Chapter 4.2.4 Fraud Prevention & Detection.

[43] Cf. IIA, GTAG Global Technology Audit Guide, Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition, March 2015.

[44] Cf. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Publication Berlin, p. 130 ff.

audits. By developing a system of key performance indicators (e.g., from past audits or data analyses), an internal audit department is enabled, if used continuously, to assess an issue immediately or shortly after the occurrence of events or the identification of anomalies and, if necessary, to react at short notice.

Fig. 22: Interaction of CA with and in addition to the audit lifecycle[45]



This usually occurs when threshold values of certain KAIs or a combination of KAIs are exceeded. Based on such exceedance, an adjustment to the annual plan may be made during the year or an additional audit may be initiated because there is an increased risk value in a certain area or for a particular audit object.

Ultimately, the resources are allocated to the highest-risk audit objects in a timely manner or are used to follow up on suspicious activity-based indications as part of an ad hoc audit. It is not mandatory to initiate an audit. Alternatively, depending on the risk, the department can be asked to check this anomaly via workflow or e-mail notification. For example, if the tolerance level for defaults on payments accounts is exceeded by more than 10%, a request may be made to management for a statement. In the event of an excess of more than 25%, or if other KAIs become conspicuous, the internal audit department may decide on initiating an ad hoc audit.

[45] Cf. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Publication Berlin, p. 237 ff.

4.2.3 News screening/issue management with text mining

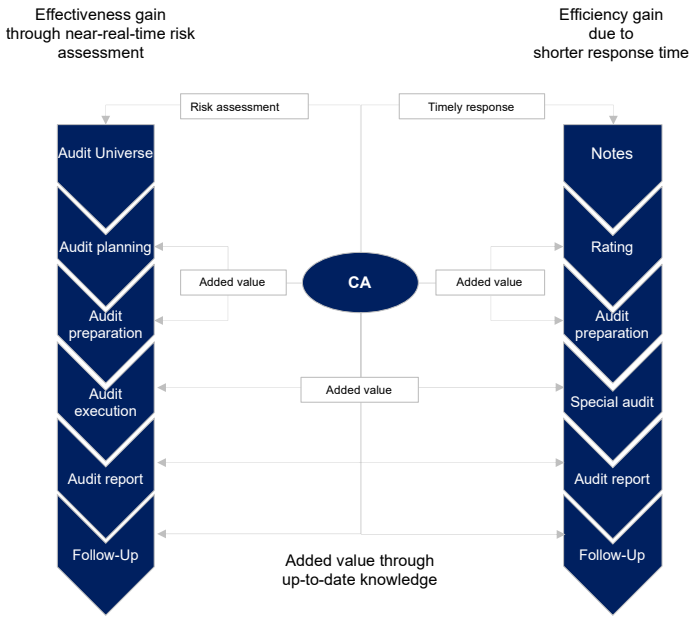
When using CA-Systems, unstructured data such as images, videos, scanned business documents, notes, or PowerPoint presentations can be used in addition to data available in the company. Furthermore, information from the Internet or social media (including news, comments, chats, and forum posts) can be classified as unstructured or semi-structured data. Unstructured data must first be converted into a processable, uniform format with the help of models to be analyzed regarding specific questions. In summary, qualitative data is converted into quantitative data and made analyzable using selected data analysis techniques such as text mining. The automation of news screening and issue management in internal auditing using text mining methods represents a concrete application case.[46]

For the initial, risk-oriented audit planning and the adjustment of this planning during the year due to special situations, news about the own company, its suppliers, customers, the competition, legal changes, or changes in the market situation are significant factors. Issue management is the term used to describe the management of risks and opportunities within an organization. An issue represents a specific topic, aspect, or event (internal or external development/change) that is appropriate for exerting a critical influence on an organization's ability to act or achieve its objectives.[47] Organizationally relevant events should be identified at an early stage to be able to react at short notice. In many internal audit departments, such management is performed manually to incorporate certain aspects into the audit planning.

[46] Cf. „Einsatz von Continuous Auditing: Einsatz von Continuous Auditing: Herausforderungen und Blick in die Zukunft, Bauch, M. et al., ZIR 06/2019, Erich Schmidt Publication Berlin, p. 248 ff.

[47] Cf. Gabler Business Dictionary: https://wirtschaftslexikon.gabler.de/definition/issues-management-52703.

Fig. 23: The added value of CA through current knowledge[48]



Due to the possibility of making internal and external, unstructured data analyzable with the method of text mining, in compliance with data protection laws, this manual process can be automated to carry out a (genuinely) timely risk assessment for audit planning by means of certain information or to initiate an ad hoc audit in the event of an accumulation of textual indications.

4.2.4 Fraud prevention & detection

Fraud prevention & detection aims at the early detection of potential fraud cases and tries to prevent further attempts of fraud. A starting point for this is provided by the Continuous Monitoring of KAIs, which were used to identify process deviations or the occurrence of certain events. An insurance company, for example, can systematically examine submitted damage reports to uncover fraud attempts. In this context, it may be necessary to collect further details and to form subject complexes/aggregations of damage reports. The aggregation procedure, i.e., the deliberate, targeted combination of individual information modules, is crucial for the validity of the analysis results. For instance, an increase in the number of damage cases just beneath existing release limits may be an initial indicator that

[48] Cf. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Publication Berlin, p. 130 ff.

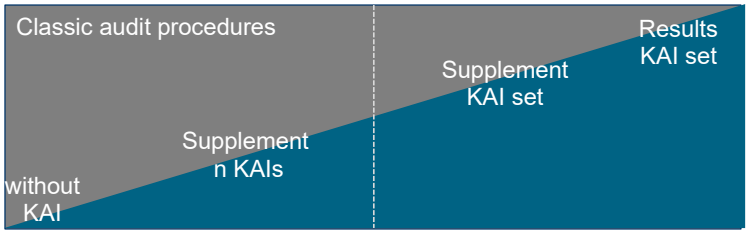
requires closer examination. By adding processing or transaction times and, if necessary, pseudonymized requestors and/or clerks, further target-oriented indicators can be generated.

The various data analysis tools on the market offer standardized evaluation options already, e.g., gap analyses (document or sorting gaps), Benford analyses (deviation analysis as comparison of digit patterns in data sets with the expectation of Benford's law) or double-booking analyses. Some tool providers and consultants have also already developed a variety of fraud indicators, which are mostly based on ERP system data and the standard workflows in ERP systems. If a high number of specific adjustments to ERP standard processes and settings have been realized in the corporate environment, these standardized analyses may not be able to be used without adjustments that are also necessary.

4.2.5 Fully automated CA-System without interaction with the audit lifecycle

It has already been explained in the presentation of the collaboration models that there are different scenarios. Furthermore, the number of existing KAIs in a CA-System and the relationship between the use of KAI results and the classic audit activities of an internal audit function vary.

Fig. 24: Degree of automation and use of a CA-System[49]



Increasing the level of automation and the use of existing KAIs means that traditional - often manual and time-consuming - individual audit procedures can be reduced.

[49] Bauch, M., Kriegelstein-Sternfeld H., Die inverse Beziehung zwischen Continuous Auditing und der Digitalisierung, Specialist lecture DIIR Digitale Tage 2019,16.05.2019.

It is thus possible for KAIs developed by internal audit to be carried out fully automatically based on a schedule. Certain analyses can be built on each other and previous results can be used in subsequent analyses. One example is audit routines that are performed automatically at fixed, regular times and forwarded for processing. Subsequently, the results are supplemented with further information regarding time and process flow. Clarification of who should be the recipient of the results generated in this process should be made in advance (internal audit or the specialist department). In case of exclusive use of the results by addressees in the business department, there is a need for the latter to be responsible for contents of the analyses and results (also in the form of quality assurance) (cf. chapter 3.3 Collaboration models). It must be ensured that the department is familiar with the audit methodology to be able to interpret the results properly. In this process, they can and must be regularly checked. Adjustments to the processes or the data models of the supporting systems may require an adjustment of the KAIs. As there may be no feedback of information to internal audit, or the results may not be used by internal audit as a supplement, they cannot have any influence on the audit lifecycle. Depending on the responsibility for the process, the boundaries between CA and CM may be crossed here (see also chapter 1.3 General Definitions).

A fully automated CA without any interaction with the audit lifecycle therefore means that a comprehensive KAI system is fully and independently implemented and that analysis results are automatically generated and directly delivered to the recipients for implementation via workflow. The implementation or the actions performed are then reported to the CA-System.

The following changes can consequently occur using a fully automated CA for internal auditing:

- Continuous and thereby largely automated monitoring of a company's controls and processes
- Real-time mapping of key business indicators
- KAIs replace traditional audit procedures 100%
- Workflow and/or e-mail notification when threshold values are exceeded
- Audit reports/results are generated automatically and addressed in digital form
- Implementation of workflow-based approvals
- Performing audits on site is not always necessary, travel time and travel expenditure can be reduced. The audit can be performed partially or entirely remotely.

As a limitation, it should be emphasized that the higher the degree of automation and use of a CA-System, the more knowledge and transparency will be lost regarding the business processes due to a lack of observations and interviews. At present, even the best CA-System cannot replace the professional and social skills of an auditor, despite the experience gained in the special situation during the pandemic. The disposition and control skills as well as the judgment of the qualified auditor are presumably indispensable.

4.2.6 Early risk detection/preventive approaches

As described in various previous sections, the Continuous Monitoring of KAIs also serves to identify risks at an early stage. For example, an underlying problem can be identified by evaluating customer complaints if an issue occurs more frequently or more frequently than before. For this purpose, it might again be necessary to gather further details and aggregate customer complaints. This will most likely involve unstructured data (e.g., from free-text fields), which needs to be converted first.

In a comprehensive field analysis, the complaints can be referred to specific product groups, products, or even more finely granulated to specific components, for example. By aggregating information on measurable environmental factors (e.g., service life, temperatures, batch numbers, supplier numbers, points in time), targeted clusters can be established. This can serve as a preventive starting point for a quality check, in which raw materials and supplies, vendor parts, or even process flows, and controls can be focused on the quality assurance of a manufacturing company. However, corresponding analyses can also be implemented in trade or at service providers.

The applied risk indicators and the increase in the corresponding risk values also prompt internal auditing to make an adjustment to the audit planning, if necessary. The results of these investigations also serve to reduce possible legal and regulatory violations as well as economic and reputational damage.

5 Software support in CA-Systems

5.1 Software architecture models

The development of a CA-System in one's own company depends, among other things, on the governance structure, the interpretation of the role of internal auditing in the company, the existing IT infrastructure, IT systems, data sources, data volumes, and the established CM systems in the first and second line. It is important to emphasize that a CA-System can be developed differently at each company. Given the individual framework conditions and a cost/benefit analysis, a CA-System can be built on Excel, data analysis or data mining tools, database queries, and even process mining tools or custom programmed systems. Depending on the amount of data to be processed, e.g., in the Big Data scenarios and the conversion of unstructured data into structured data, appropriate software frameworks, hardware, and architectures must also be built or existing IT infrastructures, databases and/or data lakes[50] must be used.

To take full advantage of CA-Systems, the use of appropriate software is recommended. Automation in this context is not only limited to the analysis of data, but may also extend to possible upstream steps, such as data extraction. Due to the wide range of applications, there are many different IT solutions on the market that are suitable for automating CA-Systems. Despite this variety, both theory and practice essentially differentiate between two main system architectures for the technical implementation of CA-Systems: Embedded Audit Modules (EAM) and Monitoring Control Layer (MCL).

- **EAM-Architecture:** The core of the EAM architecture is an audit module that is embedded in an existing IT system (which digitally maps the audit subject) and is thus part of this system. To ensure technical compatibility, the same programming language and logic must be used when embedding the system. This enables very short processing times even with large data volumes. From the user's point of view,

[50] Cf. Gartner.com: “A data lake is a concept consisting of a collection of storage instances of various data assets. These assets are stored in a near-exact, or even exact, copy of the source format and are in addition to the originating data stores.” (https://www.gartner.com/en/information-technology/glossary/data-lake).

audit modules in an EAM architecture integrate relatively seamlessly into the existing system, so that the user only needs a comparatively short orientation period due to the functional and visual similarity to the existing system. Data access and data extraction are performed according to known procedures.

In EAM architectures, the data to be analyzed does not usually leave the actual IT system and therefore does not have to be subjected to any additional security or data protection requirements. However, the operation of the IT system and consequently the authority over access rights and security parameters is often in the responsibility of specialist departments.

- **MCL- Architecture:** MCL architectures, on the other hand, include as an essential component an independent auditing system located outside the existing IT system, which extracts relevant information from the existing IT system and analyzes it externally. In this architecture model, the auditing system represents a separate layer that can perform tasks such as data extraction, data filtering, data harmonization, data analysis, and results processing. Due to its independent character, the auditing system can more easily utilize data from different sources and is therefore particularly suitable for companies with a large number of IT systems or with a heterogeneous IT landscape. For the auditor himself, an independent auditing system (e.g., an auditing DWH) offers the opportunity to define certain parameters and other settings.

  MCL architectures, in addition, often fall under the responsibility of internal auditing and thus allow a higher degree of independence and self-determination on part of the auditors. However, due to their "external" location, they often require consideration of stricter data protection and security requirements, especially when data is stored or processed outside existing IT infrastructure (e.g., directly at the provider or in an external cloud). Many systems offer corresponding data security and encryption functionalities.

In addition to these two architecture models, several hybrid variants with different characteristics can be found in practice. The choice of architecture or specific application should therefore generally depend on the situation. Factors to be considered include the nature of the existing IT infrastructure, the objectives and scope of the planned CA activities, as well as the auditor's experience with such IT applications. Any requirements, such as regarding the availability of data, the encryption of data and compliance with security parameters, should be fully identified and taken into consideration.

5.2 Application scenarios of data analysis for internal auditing

For auditor's auditing and consulting activities, the company's data represent a reliable source of information in addition to documents and evidence. Data analysis supports the auditor in auditing, consulting, and determining threshold values of Key Audit Indicators (KAIs) that can be applied for Continuous Auditing. In the subsequent section, the methods and applications of data analysis in the CA-System are described, following its definition.

Definition of the data analysis

Data analysis[51] is defined as a method of obtaining summarized information (characteristics) from individual data and documenting it in tables or graphs. Data analyses can be divided into the following areas:

- **Descriptive data analysis**: In the case of a complete survey or data set, descriptive data analysis can condense information and present key points with tables, graphs, and key statistical measures.
- **Inferential data analysis** enables results from samples to be generalized to the overall population.
- **Exploratory data analysis** is used to process data sets to show and discover structures and correlations.[52]
- **Confirmatory data analysis** can be used to test relationships (e.g., regression analysis).

Auditing methods of data analysis

Manual ad hoc data analysis

Auditors can use ad hoc data analysis for both regular and special audits along with topics that can only be addressed by examining the data at hand. The ad hoc data analysis enables the auditor to determine reliable results

[51] https://wirtschaftslexikon.gabler.de/definition/datenanalyse-30331, 02.09.2019.
[52] Cf. Chapter 7. Process Mining.

and findings for the specific subject matter to be examined. Given that the analysis is usually performed on a single occasion or for a specific purpose, the analysis is a conventional, non-standardized data analysis.

Ad hoc data analysis may alert auditors by identifying issues that are valuable as KAIs for a CA-System. For example, a data analysis from the Accounts Payable area shows that suppliers submit invoices to bank accounts not only in their country of domicile, but also in potential tax havens. Hence, information might flow into a CA-System and a KAI might show the number and amount of invoices per quarter that have been transferred to possibly critical bank accounts.

Possible software tools for manual data analysis are IDEA, ACL or standard macros, e.g., from Excel.[53]

Semi-automated data analysis

Semi-automated data analysis is characterized by a combination of manual actions, such as a manual start of the process by a person, and automatically executed data analysis logics, such as scripts. For example, auditors can have an automatic script available for defined subject areas (e.g., purchasing processes that do not follow the standard process), which enables them to perform a well-founded and useful analysis. During the auditing process, auditors manually request the required data, such as payment or purchasing data, either from the department to be audited or by directly accessing the system. After the necessary data preparation, the automated scripts provide the results of the data analysis related with the obtained data.

One of the main reasons or advantages of using semi-automated data analysis compared to fully automated data analysis is the lower complexity of scripting. Even though the analysis execution is partly dependent on manual steps performed by human, this variant is considered to be cost-effective and more suitable for certain purposes (e.g., for smaller companies, specific process requirements). Numerous internal audit functions, which are of a certain size due to the complexity of the company, implement central data analysis departments for the creation of data analysis logics and modules and, if necessary, for the preparation of analysis results, to provide auditors with data in the course of audits.

[53] This list is not exhaustive and should not be interpreted as a recommendation.

Fully automated data analysis

In fully automated data analysis, the execution of time-controlled data analysis logics such as scripts takes place. This method of data analysis is fully integrated into the IT process environment. Due to the usually complex implementation, this is a more cost-intensive solution for which a cost/benefit analysis is useful in the conception phase to be able to determine the added value.

Fully automated data analyses take place in a completely independent process. The retrieval of the data to be analyzed is done, for example, on a monthly basis. For defined key figures such as thresholds being exceeded, not met, or current status, the information is shared with the relevant persons via e-mail or dashboard. For example, auditors are shown the results of a particularly high-risk process of the company at defined intervals to make the results of the analyzed data easier to evaluate.

Data analysis in CA-Systems

To apply CA methods, manual and automated data analyses, as described below as examples, are relevant for the auditor.

Identification of KPIs and calculation of their threshold values

The auditor or creator of a CA-System applies manual data analysis to create the identified KPIs for a defined subject area. By evaluating specific data, relevant metrics and thresholds can be determined for the identified KPIs. This yields metrics and thresholds that represent a corresponding target value. Within the CA-System, current figures are compared with the predetermined target value, indicating a positive result (within the target range) or a negative result (outside the target range).

Regular data analysis in the CA-System

An implemented CA-System enables the continuous comparison of KPIs based on defined metrics and thresholds. In the process, the company data is analyzed, aggregated, and processed. The aim is to determine the actual KPIs and, accordingly, the actual state of the company data.

6 Development and validation of KAIs including thresholds

This section describes how KAIs, including their thresholds, can be developed and validated.

Fig. 25: Definition of Key Audit Indicators (KAI)

Definition of key audit indicators (KAI)
KAIs are quantitative metrics whose current values, trends, and developments are causally linked to the probability of audit field risks and/or the likelihood of achieving audit field performance goals.

Exceeding defined thresholds triggers appropriate activities for root cause analysis (e.g., further data analysis, document review, discussions with business units, or special audits) and, if necessary, the identification of a deficiency. Business units should be aware of the KAIs and the currently defined thresholds.[54]

Thresholds represent the target values against which the KAI-based CA-System regularly checks. Frequent and regular calculation of the KAI value (actual value) and comparison with the threshold (target value) essentially constitute an (automated or automatable) continuous audit activity.

The greater the influence of KAIs and their thresholds on internal audit activities, the more transparent and justified the choice of threshold should be. In particular, the definition of the threshold values indicates the responsibility that the internal audit has taken with regard to a risk-oriented and balanced cost-benefit ratio in the CA-System.

[54] Cf. Chapter 2.2 Content and methodological framework and 4.1.1 Audit Lifecycle-Support.

When suitable for the CA-System, internal audit can use indicators already used by business units (e.g., Key Risk Indicators, Key Performance Indicators) as KAIs—possibly modified or combined to fit audit objectives. The choice of threshold reflects the independent assessment of internal audit regarding the importance of the subject for the company. Typically, the internal audit threshold (for early warning) is set below the business unit threshold. It is recommended to consider audit field risks and performance goals when developing KAIs.[55]

Along with the definition, the description of a KAI must particularly contain the specification of a threshold value, which determines the point at which the above-mentioned probability of occurrence or chance is assumed to be increased or decreased to such an extent that an activity needs to be started on the part of the internal audit function.[56]

A quantitative KAI can be defined in several ways:

Absolute (number, amount, other unitized quantities), e.g.:

- Number of overdue invoices, e.g., 13
- Number of employees in dept. 4711, e.g., 8
- Total double payments, e.g., 1000 EUR
- Mean value of double payments, e.g., 500 EUR
- FX rate, e.g., 1.0 EUR/USD

Relative, e.g.:

- Average number of employees per team in the last quarter, e.g., 12
- Return on equity (ROE) in the last year, e.g., 10%.
- Scoring: combination of several individual indicators to form a KAI.

A KAI may be formed based on (aggregated) (risk) indicators, e.g., "conspicuous jump in mean probability of default".[57]

The use of relative values (e.g., indices) offers the decisive advantage over absolute values that the KAI values can be compared even if

[55] Cf. Appendix 2: Consideration of audit field risks and audit field performance targets.
[56] Cf. Appendix 3: KAI Description.
[57] Cf. Appendix 4: KAI based on key figures.

the absolute reference value changes over time. Relative indicators are therefore generally preferable to absolute values when forming KAIs.

A quantitative KAI is preferable to a qualitative KAI to ensure the possibility of automating the determination of the current KAI value in the medium to long term. For example, the risk of an improperly performed quality control in the department, which intuitively can rather be described by a qualitative KAI, could be represented by a quantitative KAI, which measures the duration of the performance of the quality control, provided that a causal relationship can be assumed between duration and quality of this activity.

When using a quantitative KAI, data quality should be regularly reviewed or assessed as part of the KAI validation process.[58]

If data of a historical period is used for the calculation of the KAI value (e.g., short-term vs. long-term average), the effect of the duration of the considered historical period on the KAI values has to be assessed and the choice of the duration of the period (e.g., 1 quarter, 1 year, 2 years, ...) has to be reasonably justified. In particular, if a time series of data included in the KAI calculation shows a sudden change over time, it has to be analyzed to what degree older values may be taken into account. The completeness of the data must be ensured.[59]

Even when using a qualitative KAI, the quality of the information on which the KAI is based must be adequate, i.e., there must be transparency regarding the reliability, correctness, accessibility, availability, and timeliness of the required information.

The content of the KAI definitions should necessarily be reviewed with the respective departments, since the level of acceptance necessary for the success of the KAI-based CA approach can only be achieved in the department if the procedure is adequately transparent.[60]

For the precise operationalization of the CA-System, an indicator value is defined for each KAI of an audit field, above which the probability of occurrence of the risk is assumed to be significantly increased (and therefore critical).[61] This value is referred to as the threshold value. Conversely, if the current indicator value is below the threshold, the probability of

[58] Cf. Appendix 5: KAI Data Quality.

[59] Cf. Appendix 6: Data completeness in the historical period.

[60] Cf. Chapter 3.3 Collaboration models.

[61] The representation of exceeding a threshold value applies analogously to falling below a threshold value, if lower indicator values (instead of higher values) mean higher probabilities of occurrence of the risk.

occurrence of the risk is not assumed to be significantly increased. Exceeding (or falling below) a threshold value is often referred to as a threshold value breach or a "red flag".

In practice, no ideal situation generally exists in which a good indicator value range can be exactly distinguished from a bad range and a threshold value can therefore be easily determined. In principle, this means that occasional misjudgments occur, because

- situations with an increased likelihood of a risk occurring may exist in which the current value of the KAI is (possibly just) below the threshold value. The KAI therefore falsely does not strike (false negative).
- situations with a low likelihood of a risk occurring may exist in which the current value of the KAI is (just) above the threshold value. The KAI therefore falsely strikes (false positive).

A threshold value is therefore usually not necessarily unambiguously definable. This non-uniqueness offers a margin that requires careful consideration/decision-making, because

- a threshold value that is too low means: only a few (or even no) situations with increased likelihood of occurrence of the risk are missed, but many threshold value exceedances cause a lot of effort/high processing costs.
- too high a threshold means: few threshold violations cause little effort/low processing costs, but many (perhaps most or even all) situations with increased likelihood of occurrence of the risk are missed.

Weighing criteria for threshold determination may include:

- Conservatism: Better (too many) false alarms than one missed loss.
- Progressivity: Better missed losses than (too) much effort (in internal audit and in the specialist area).
- Balanced ratio: Misjudgments occur with approximately equal frequency in both directions.

The selected weighing criterion in the concrete determination of a threshold value must be documented.[62]

[62] Cf. Appendix 7: Types of thresholds.

The frequency with which a threshold value is set or adjusted can be defined statically, event-related, or automatically.[63]

In addition to the simple thresholds for a KAI, the following options are possible in threshold setting and application:

- A corridor can be defined, i.e., a combination of a lower and an upper threshold value. An activity would therefore be started by internal audit when the KAI assumes a value that lies outside the corridor.[64]
- Several threshold values can be defined. Exceeding them can trigger different activities one after the other. For example, the KAI value 13 would result in a different activity than the KAI value 11, if the value 10 was set as the first threshold value and the value 12 as the second threshold value.
- A threshold value must be exceeded several times in succession before an activity is started. For example, an activity would only be triggered if the KAI exceeds the threshold twice in a row (e.g., in two consecutive months with monthly observation frequency).
- If the threshold value is exceeded for a longer period and activity has already taken place, no further activity will be carried out in a subsequent period.[65]
- A KAI can be the threshold of another KAI (e.g., the 6M Euribor can be defined as the threshold of the 3M Euribor. Then there would be an anomaly if the 3M Euribor becomes larger than the 6M Euribor).

KAI thresholds to be applied in the CA-System, as well as their derivation, should be discussed with the affected department, just like the KAIs themselves.

The use of a threshold value obtained by an expert estimate[66] is generally considered permissible, especially when introducing a new KAI. [67] However, the aim should be to determine threshold values (at least in the long term) by means of data analysis.

[63] Cf. Appendix 8: Frequency with which a threshold value is set.

[64] The reverse case is also conceivable: The KAI is to move outside the corridor, i.e., a conspicuity is present if the KAI lies within the corridor.

[65] The length of such a period can be fixed or dynamically determined, e.g., by the time required by the department to correct a defect.

[66] For example, the person responsible for the corresponding audit field in internal audit is considered an expert here.

[67] Cf. Appendix 9: Advantages and disadvantages of expert estimation.

There are various reasons for determining the threshold value of a KAI.[68] In order to be able to define a KAI for an audit field with reasonable effort and in a timely manner, the following applies:

- A causal relationship between an audit field-specific risk and an assigned KAI must be qualitatively traceable. The amount of the correlation does not have to be quantified.
- In many cases, number and volume considerations represent a target-oriented approach for KAIs to define a KAI, e.g.:
  - Number of claims,
  - Number of new business,
  - Volume of claims in EUR,
  - Volume of new business in EUR.
- Number and volume considerations can target two types of changes, as a deficiency could be their cause:
  - Comparison with the longer past (1 year or more): A significant change compared to the longer past represents an abnormality worthy of investigation.
  - Comparison with the recent past (1 month to 1 year): A strong change (jump) compared to the recent past represents an abnormality worthy of investigation.

For each audit field, a validation should be performed and appropriately documented once per calendar year, in the context of which

- the main audit field-specific risks, the KAIs and their thresholds are to be reviewed regarding several aspects,
- any necessary changes to the KAIs and/or their thresholds are to be identified,
- appropriate measures are to be derived, and
- the status of the measures of the previous validation is to be reflected.

The resulting plan of measures, if any, must be able to identify,

[68] Cf. Appendix 10: Occasions for determining a threshold.

- which measures are not to be implemented and why not, and what risks are associated with non-implementation of the measures,
- which measures are to be implemented by when and how, and which risks or weaknesses exist during the implementation period.

To achieve these goals, a regular validation must include at least certain validation actions.[69]

If the validation has shown a need for change for a KAI and/or its threshold value and the KAI is also used in another audit field, it must be checked whether the changes should or even must also apply to the application in the other audit field. If necessary, the auditor responsible for the other audit field must be informed about the possible need for change.

At the end of a regular validation, each KAI can be assessed by assigning a color from the color scale[70] shown in the appendix.

Documentation is required for the design and validation of the KAIs. Generally, the documentation should take place in the audit system using the audit concept of the CA audit engagement (standing order or annual engagement). A separate comprehensive order can be used for documenting of the validations.[71]

[69] Cf. Appendix 11: Validation actions.
[70] Cf. Appendix 12: Color scale for result of a validation.
[71] Cf. Appendix 13: Documentation of the validation.

7 Process mining

The input and processing of data in digital systems are recorded in the form of a technical activity log. The activities thus leave behind digital footprints. Process mining is a procedure that visualizes these digital traces in such a way that the user can draw conclusions about the internal sequence of business processes.

The goal is to identify the actual business processes and their variants within an organization. Process Mining can be used in various phases of an internal audit:

- It helps auditors gain an overall view of the processes in the area to be audited. Auditors can see not only the typical and most frequent activities and process flows but also rare or very rare activities (e.g., reactivation of canceled documents) and unusual process flows (e.g., invoices received before the creation of a purchase order).

- During the audit, Process Mining allows auditors to gain an overall overview of the processes, compare the identified actual state with the target state and to explore the details of transactions in depth.

- The graphics generated from Process Mining can usually be exported and included in the audit report.

Relationship between process mining and continuous auditing

Process mining is an exploratory tool with very flexible applications. It can also be implemented independently of well-known process mining tools.

In Continuous Auditing, the typical approach is to continuously monitor predefined KAIs (Key Audit Indicators) to react during the year if critical thresholds are exceeded or not met. The key aspect here is the ongoing observation of the same KAIs.

The process mining method is useful in the run-up to the implementation of a CA-System for identifying critical process risks and defining appropriate KAIs. The insights gained through process mining provide a basis for identifying effective KAIs. It is therefore particularly well suited to audit activities.

Importantly, Process Mining tools can also be used to implement continuous CA-Systems, as deviations between actual and target processes can be defined as KAIs and monitored continuously.

8 Machine Learning

Machine Learning (ML) is the idea of allowing machines to learn via appropriate algorithms through data and experience. Machines derive a statistical model from the information provided. A machine thus learns from the data and can generalize after the training phase.

In this process, the machine does not simply memorize examples but recognizes patterns and regularities in the training data, allowing it create a model of its environment and perform assigned tasks better.

Ideally, the machine can assess unknown data and transfer what it has learned. In the worst case, it may fail to learn from unknown data. ML methods can therefore not operate independently, but must be set up, applied, and evaluated by specialists.

The implementation of ML occurs in three phases:

- Phase 1 - Learning/Training Phase (Modelling),
- Phase 2 - Testing Phase (Quality Assurance and Evaluation)
- Phase 3 - Application to Unknown Data (Prediction)

The different applications of ML can be grouped as follows:

- Data types: Text, speech, and image data.
- Learning tasks: Classification, regression, and clustering.
- Algorithms: The technical solution to the problem.

These categories are often interdependent; for example, different learning tasks can be solved with similar algorithms, and specific algorithms may be suitable only for certain data types.

Typical applications of Machine Learning, for example in the financial sector, include:

- Credit scoring (creditworthiness assessment)
- Credit card fraud detection

- stock market analysis,
- customer segmentation.

ML can be used to identify anomalies and irregularities in these and other areas. Thus, it may serve as a control instrument and is particularly suitable as a tool for the first line.

However, in practice, there are several challenges for internal auditing when using ML:

- Large data volumes are required for ML.
- Technical and personnel resources are needed (powerful servers, data science-trained staff).
- High implementation effort compared to traditional methods.
- Uncertain success: The outcome of ML projects cannot always be predicted.
- High false positive rate: ML often produces more false alarms than traditional methods.
- Lack of explainability: When a case is flagged as anomalous, it is often unclear why the machine classified it as such.

In CA, the main goal is to regularly determine well-defined KAIs, compare them to target values, and take action in case of significant deviations. ML can be used to extend a metrics-based CA-System after its implementation.

9 Appendices

9.1 Possible data sources

Fig. 26: Data sources[72]

Data source	Examples of collected information
IT-Asset-Register	Designations/IDs of IT assets, their life cycle, and process-based deadlines; dependencies between IT assets (information network).
Electronic organization charts/organizational structures	Changes to organizational structure, ReOrg measures, changes to designations; roles and responsibility changes
Risk management systems	Changes to (process-based) risk assessments; occurrence and processing status of risks, damage levels if applicable, process assignments
Internal and external reporting	Findings and measures from annual reports or reports from external supervisory/control bodies (BaFin, ECB, state or federal data protection, audit reports from service providers)
Project management systems	Projects and their framework data (budget, approvals, bodies, goals, milestones, roles, responsibilities, risk assessments, cost-effectiveness assessments)
Knowledge management systems	Process information, vulnerabilities, assessments, improvements, solutions, various analyses
Product databases/catalogs	Products and their data (designations, dependencies, links to legal framework, life cycle, descriptions, links to controlling information)
Protocols of meetings with specialists and managers	Planned changes to processes and responsibilities, risk assessments by departments, identification of audit objects, audit, and consulting requests

[72] The list is not complete. It will be updated in the course of further revisions of the guide.

Electronic process documentation	Processes and their data (designations, dependencies, responsibilities, life cycle, descriptions, controls, control objectives, if applicable results and evidence of performed first and second line control actions); if applicable results from process mining analyses
ERP systems/DWHs	Process and product information, control information, analyses/evaluations, if necessary, results from process mining analyses, controlling information, various analysis options by combining different data sources
Provider management systems	Providers with their contact data, contact persons, risk assessments, emergency information, information from the monitoring process, audit reports, if applicable own audit reports, call logs, KPIs from monitoring, contract information
Security Information and Event Management	Use cases, security events with their risk assessment and status of processing
Personnel management systems	Personnel data, entry and exit dates, salary information, training information
Master data management systems	Personnel data, authorization information, user accounts and their status, entry and exit dates
Identity and Access Management	Authorization information and compositions, user accounts and their status, time limits, recertifications, release levels, applications, and changes with associated framework data

9.2 Consideration of audit field risks and audit field performance targets

In order to develop KAIs, it is recommended that for each audit field that is to be taken into account in the CA-System of internal auditing, the **audit field risks** and **audit field performance objectives** are first set out as a written statement and then divided into "material" and "non-material" and into "audit field-specific" and "audit field-non-specific". The associated visualization of the material risks and performance objectives supports the auditor in defining the KAIs and establishing the KAI-based CA-System quickly.

First, KAIs should be formed for the **key audit field-specific risks** and performance objectives. Over time, additional KAIs can then be used to define the other risks and performance objectives, e.g., in the following sequence

I. material audit-field-topic-unspecific risks (e.g., inadequate staffing, insufficient IT availability) and material audit-field-topic-unspecific performance targets,

II. non-significant audit-field-topic-specific risks and non-significant audit-field-topic-specific performance targets,

III. and non-significant audit field-specific risks and non-significant audit field-specific performance targets are continuously reviewed.

The content of the formulation of the (material) risks and performance targets should be discussed with the departments involved to achieve a common understanding of the audit field contents and their weighting.

9.3 KAI description

A KAI description should contain the following information:

- **Indicator name:** The KAI should be given a meaningful name.
- **Area:** The area in which the KAI is used should be stated (e.g., finance).
- **Audit frequency:** The frequency with which the KAI is to be viewed is to be specified (e.g., monthly).
- **Risks, performance targets:** The relationship to the covered (material) risk or performance objective shall be established.
- **Dependencies:** Possible dependencies of the KAI on other KAIs should be mentioned.
- **Points to note:** It should be noted what needs to be considered when using the KAI.
- **Specifics:** The sources from which the information/data required for the KAI is obtained should be mentioned, along with alternative sources, if available.
- **Aggregation level:** If the KAI can be used for different aggregation levels (e.g., organizational unit, continent, product type), this must be indicated.

9.4 KAI based on key figures

Example of a KAI: In the rating procedure audit field, the risk "The rating procedures do not provide valid and thus objective results for the probability of default of a borrower" exists. The KAI "conspicuous jump in the average probability of default (of all or part of the portfolio)" is defined.

This KAI is motivated by the fact that a significant change (jump) in the average probability of default of all exposures rated with a specific rating module is rarely to be expected and therefore a conspicuity exists in the event of a significant change in this ratio. In addition to natural causes, there may be various reasons for such an anomaly, e.g., deficiencies in the rating calculation or in the proper application of the rating. Thus, a significant change in the indicator value is conspicuous both upwards and downwards.

The principle of this KAI, i.e., the reaction to a significant change in a key figure where no jumps are to be expected, is very well transferable to other audit fields.

9.5 KAI data quality

When using a quantitative KAI, the following should be considered regarding the quality of the data needed for the KAI calculation:

- Completeness of the required data,
- Reliability of the required data (i.e., is the origin of the data traceable, e.g., by means of a business concept or a process map)?
- If applicable, consistency of the required data across different systems or sources,
- Correctness and, if applicable, exactness of the required data,
- Accessibility of the required data (current and long-term), e.g.:
  - own system or database authorization,
  - Supply from the business department or IT,
  - Internet (www.destatis.de, ...),
- Availability of the required data (current and long-term, i.e., will the required data be produced in the long term?),

- Timeliness of the required data (i.e., are the required data produced in time and/or are they available exactly when they are needed for the KAI calculation? And if not, is the use of data that is already of a certain age acceptable, i.e., can the CA goals be achieved)?

9.6 Data completeness in the historical period

In particular, if a time series of data included in the KAI calculation shows a jump over time, it must be analyzed to what extent older values may be taken into account. Regarding the completeness of the data, proceed as follows:

- A KAI value may only be used with completed data or data that has been completed appropriately.
- If data gaps exist in the selected time period, the data quality may still be adequate, specificaly if the existing data remains correct and the data gaps can be filled appropriately.
- Filling the data gaps can be done in several ways:
  - Ideally, the missing data can be obtained after all (with reasonable effort) (e.g., from other sources) or produced.
  - By expert estimation, for which, however, assured expert knowledge must be available in the specialist department and/or in internal auditing.
  - By constant continuation at the margins in case of a time series: If data is missing at the beginning and/or at the end of the selected time period, the data series can be completed by using the last available date in each case, provided this is appropriate and can be comprehensibly justified.
  - Per Interpolation:
    - Piecewise linear interpolation: all dates between which data are missing will be connected by means of a straight line, resulting in the missing values.
    - Other interpolation methods such as higher degree polynomials, cubic spline interpolation or Gaussian process regression are usually costly. They should only be used if a linear interpolation definitely leads to inappropriate results.

9.7 Types of thresholds

Examples of types of thresholds are

- for qualitative KAIs:
  - Yes/No or 0/1.
- for quantitative KAIs:
  - 0, if zero tolerance.
  - Specification from
    - Law, regulation,
    - Business strategy,
    - Written regulations/instructions, specialist concepts.
  - Threshold value from a target minus (or plus) an expert-estimated (usually conservative) add-on (absolute or relative).
  - Expert-estimated quantitative value.
  - Average of KAI values of a relevant/expertly appropriate long period in the past.
  - Average minus (or plus) n standard deviations of the KAI values of a relevant/expertly appropriate long period in the past.
  - Quantile, if it is known how the historical KAI values are distributed (e.g. 95% quantile in the case of a normal distribution).

9.8 Frequency with which a threshold value is set

Regarding the frequency with which a threshold value is set, the following variations are possible:

- Static: The threshold value is set and remains constant. A review, which can lead to a change, takes place in any case within the framework of the KAI validation, i.e., the review or adjustment frequency corresponds to the validation frequency.
- Occasion-related adjustment: In addition to the review, which takes place regularly as part of the KAI validation, the threshold value can be changed on an occasion-related basis, which must be justified and documented. Occasions can be, for example:

- A KAI has exceeded its threshold, but the follow-up activity (e.g., discussion with the department) has shown that the probability of occurrence of the risk has not (significantly) increased. Then the threshold could be adjusted (in this case increased).
- Internal audit has become aware of the (significant) increase in the probability of occurrence of a risk, but the associated KAI has not exceeded its threshold. Then the threshold value can be adjusted (in this case lowered).

- Dynamic/automatic adjustment: If the threshold value is determined by observing a historical course of the KAI values in a period, two options are possible:
  - The historical period consists of n whole calendar years before the current calendar year. In this case, the threshold value is always determined at the beginning of a calendar year based on the KAI data of the new period (during a calendar year, the threshold value is then constant).
  - The historical period (e.g., l months, m quarters, n years) always starts directly before the currently considered period (e.g., current month, current quarter), i.e., the threshold value is re-determined and immediately applied at each consideration point (calculation point of the KAI).

The advantage of a dynamic adjustment of the threshold value or the application of a dynamically determined threshold value is that the most recent past and thus the current development of the situation represented by the KAI are always taken into account. However, this variant must be applied with caution, since a trend that could be associated with an increase in the probability of occurrence of the risk may be missed.

In the case of a time series, it must be checked - e.g., by means of visualization of the data - whether there is a trend and/or seasonality in the selected historical period that should be taken into account when determining a threshold value.

9.9 Advantages and disadvantages of expert estimation

Advantages of an expert estimate:

- From a practical point of view, procedures for the quantitative determination of an optimal threshold are often non-trivial. If the effort is disproportionate, expert estimation is initially a cost-effective alternative that allows the immediate application of a KAI.

- If the necessary data for the application of a quantitative or visual method for threshold determination are not available at all or not in sufficient quantity or quality,[73] expert estimation is initially a cost-effective alternative. If the necessary data can only be obtained with disproportionate effort or not at all, expert estimation may initially be the only way to determine a threshold value.

Disadvantages of expert estimation:

- People often overestimate the probability of rare events and underestimate the probability of frequently occurring events. In contrast, deriving a threshold from a data analysis yields results that are not biased or are less subjectively biased.
- Due to the subjective part in an expert estimate, the comprehensibility of the result is usually lower than in a calculation.
- In contrast to the derivation of a threshold value from a data analysis, an expert estimate cannot be automated.

Due to the disadvantages mentioned above, the aim should be to determine threshold values (at least in the long term) by means of data analysis.

9.10 Occasions for the determination of the threshold value

There are various occasions for determining the threshold value of a KAI:

- Start of the CA-System: With the start of the CA-System, all KAIs are de facto new KAIs. → The determination of a threshold values is necessary.
- New KAI in an existing audit field: The KAI set of an existing audit field is augmented by a new KAI. → The determination of a threshold value is necessary.
- New audit field: A new audit field is added to the audit universe.

[73] The fact that historical data is not available at all, or not available in sufficient quantity or quality, will be a relatively frequent occurrence with a new KAI (i.e., with many KAIs at the time the CA-System is launched). Over time, this situation should improve significantly, as the introduction of a KAI will result in the production of the necessary data by the department (or by internal audit itself).

- The main risks of the new audit field are completely or partially mapped by new KAIs. → The determination of threshold values is necessary.
- The material risks of the new audit field are fully or partially represented by KAIs that are also used in other audit fields. → The determination of a threshold value is necessary if the threshold values used in the other audit fields for the existing KAIs are not also to be used in the new audit field.

- Changed KAI in an existing audit field: Due to circumstances beyond control, it is necessary to change a KAI (e.g., production of the required data is discontinued), i.e., its data basis and/or its calculation logic is changed (then it may even be a new KAI). → The determination of a new threshold value is necessary.
- Validation: From the regular validation of a KAI and its threshold value, the necessity for the new determination of the threshold value arises.

If necessary, new KAIs are added to the CA-System. The initial period after a KAI is added to the CA-System is referred to as the introductory phase. In this phase, which may last up to one year, reduced formal requirements may apply about the adjustment of the threshold value of a KAI.[74]

- In principle, the threshold value may be the result of an expert estimate, even if the data situation would allow a threshold value determination by data analysis.
- The threshold value may be adjusted several times by expert estimation, especially if the analysis of the cause of a threshold value exceedance leads to the conclusion that an incorrect estimation has occurred.
- The reason for the adjustment must be documented in each case. This must include the reason for the direction of the adjustment (higher or lower threshold value than before).
- The amount of a change must be justified only qualitatively.

After the introductory phase, the expert estimate should - if possible - be replaced by a data analysis.

[74] The validation cycle is generally 1 year (see section 9.11 Validation actions), i.e., a regular validation of the KAI including a review of its threshold value takes place no later than 1 year after the introduction of the new KAI.

9.11 Validation actions

To verify the KAI results, a rotational validation must include at least the following actions:

- regarding the main audit subject-specific risks:
  - It must be examined whether the audit topic-specific risks have been fully identified, i.e., whether
    - Risks and thus, if applicable, KAIs need to be supplemented,
    - risks (and thus KAIs, if applicable) that are no longer material are omitted.
  - It should be investigated whether the phrasing of the material audit subject-specific risks needs to be adjusted or at least sharpened.
- with regard to the KAIs:
  - It is to be examined whether causality can still be assumed between risk and KAI.
  - It should be investigated - considering the threshold exceedances that occurred during the validation period - whether the observation frequency of the KAI should be changed (i.e., more frequent or less frequent KAI calculations).
  - Investigate whether the quality of the data used to calculate the value of a quantitative KAI remains appropriate. More specifically, it should be ensured that the completion of data in case of incomplete data continues to be carried appropriately.
  - Examine whether the quality of the information on which qualitative KAIs are based remains appropriate.
  - Investigate whether the KAI calculation logic would need to be changed. A change has to be weighed carefully, since this means de facto the introduction of a new KAI with the corresponding consequences (coordination with the department, new threshold value, ideally calculation of historical KAI values, etc.).
  - If a tool (e.g., an Excel spreadsheet with formulas) is used for the calculation and visualization of a KAI, a tool review must be performed to ensure the correctness of the calculations. For this purpose, it must be examined, among other things, whether the test cases contained in the tool continue to ensure sufficient test coverage or whether additional test cases must be added. In the case of an Excel sheet, a tool review should also include the following activities:
    - Investigate whether formulas output error values that are not processed with proper error handling.

        - Investigate whether copied formulas have been copied correctly (e.g., if data series have been extended to cover the following period).
        - Check whether the cell ranges addressed in the formulas are correct (e.g., if cell ranges have been extended to cover the following period).
        - Check if all relevant data are shown in graphs (e.g., if data series have been extended to cover the following period).
- Regarding the thresholds of the KAIs:
    - Investigate whether the number and amount of threshold exceedances that occurred during the validation period was appropriate. If necessary, the threshold value should be adjusted.
    - Examine whether the response of internal audit was appropriate for the threshold violations that occurred during the validation period. If necessary, the planned response should be adjusted and/or several thresholds could be introduced, each with a different response.
    - Investigate whether the method by which the threshold is determined should or could be changed (e.g., data analysis instead of expert estimation).
    - The time course of the KAI (including a representation of the threshold value) should be visualized - if reasonable and possible and not already done - to increase the traceability regarding all activities performed during the validation period and based on the KAI observations or all activities not performed.
    - If circumstances have come to light where an internal audit response would have been appropriate or necessary but has not occurred and no threshold exceedance has been measured, investigate whether the threshold should be adjusted.
    - If a tool is used to determine the threshold value, e.g., an Excel sheet with formulas, a tool review must be carried out to ensure the correctness of the calculations.

If there are different views between the department and internal audit regarding the main risks specific to the audit field, the KAIs and/or their threshold values, the validation should again be used as an opportunity to reflect on the view of internal audit with the department and, in the best case, to reach a consensus with the department.

The following applies to every validation action

- that it must be documented in a comprehensible manner why it is not carried out, if necessary,
- that comprehensible reasons must be formulated (e.g., "risk X is no longer material because ...", "the calculation logic of a KAI is changed because ...").

If there is a need for further validation a relatively short time after a regular validation (i.e., before 9 months have elapsed since the validation), the following procedure can be followed (event-based validation):

- A shortened validation is performed, e.g., only for one KAI instead of for all KAIs. For this purpose, it must be decided which validation actions of a regular validation (see above) are at least necessary to ensure the CA-System for the audit field by means of KAIs in the future as well. These are documented. The reference time for the start of the next regular validation is not the end of the event-related validation, but the end of the last regular validation.
- A validation is performed that corresponds to a regular validation in terms of its scope. In this case, the reference time for the start of the next regular validation is not the end of the regular validation, but the end of the event-related validation.

9.12 Color scale for result of a validation

At the end of a periodic validation, an assessment can be made per KAI by assigning a color from the following color scale:

Green

- KAI is still used,
- Calculation logic unchanged or adapted,
- Threshold value unchanged or adjusted.

Yellow

- KAI can still be used, but use is suspended until the necessary changes or corrections (e.g., appropriate data quality must be established, threshold value must be recalculated and adjusted) have been implemented (action plan),
- renewed use planned from ...

Red

- KAI can/should no longer be used because ...

Blue

- New KAI,
- Use from now or use from ...

9.13 Documentation of the validation

The documentation of the KAIs and thresholds should always be included in the audit concept of the CA audit engagement (standing order or annual engagement). A separate overarching order can be used for the documentation of the validations. This results in the following possible breakdown:

Documentation of KAIs and thresholds in the audit concept of the CA audit engagement.

KAIs

- In addition to the definition of a KAI, the documentation of the design of the KAIs must contain comprehensible justifications for the specific design.
- The characteristics of a KAI[75] can be presented in an annex to the audit concept.
- In doing so, the connection to the risks/performance objectives to be considered of the audit field to be assessed by CA should be established.

Thresholds

- The documentation of the threshold values must contain comprehensible reasons for the concrete design.

- In this context, the criteria for the determination of threshold values should be considered (conservatism, progressivity, ...).

[75] Cf. Appendix 3: KAI description.

- Occasion-related changes during the year.

Documentation of the validation in a separate overarching order.

- This order is divided into the audit fields considered in the CA. For each audit field, the performance and results of the necessary validation actions as well as any resulting measures are to be documented for all CAs.
- Files from which validation results are derived (e.g., Excel files) are annexes to the validation order.

Publisher

This guideline was developed by the DIIR working group “Continuous Auditing” and published by DIIR - Deutsches Institut für Interne Revision e.V.

Website the working group.

Published: 26.04.2021 on www.diir.de. English version: 5.06.2026.

DIIR would like to thank the members of the working group in Continuous Auditing and the working group leader, Mr. Michael Bauch, for preparing this publication.

Frankfurt am Main, 26.04.2021

DIIR – Deutsches Institut für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main
Germany