Chartered Institute of Internal Auditors

01 February 2023

Audit universe

Chartered Institute of Internal Auditors

Why should organisations take action?

Every organisation is different in terms of structure, processes and risk maturity. The approach to the audit universe needs to be fit for purpose for the organisation, and there is no 'one size fits all'.

While an audit universe is consistent with a risk-based approach, internal audit should not take for granted that listing all auditable areas to form an audit universe will always be necessary or the right thing to do. It would be beneficial to review, on a regular basis, whether you currently have or decide to develop an audit universe. It is also recommended that you review the purpose and value that an audit universe adds to the planning process and its outcomes. If a decision is made to have an audit universe, then this can be a valuable tool for identifying the frequency of required coverage, as a way of checking that coverage is complete (or that coverage has been provided over the key required areas or as planned). This can help with resource.

Top tips

1. Determine whether you need an audit universe or not.
2. If you need one, define the basis that you want to create your internal audit engagements from. The structure of the audit universe should be easy to understand and trackable so that a CAE can monitor coverage.
3. Determine if you want more than one dimension to the audit universe, or if a single lens will suffice, for example only using the structure of the organisation versus using the structure of the organisation as well as an inventory of key change programmes to determine which areas are key and require coverage.
4. Define what you want the audit universe to do for you – for example, drive a risk-based plan, a cyclical plan, or a hybrid plan.
5. Have a clearly documented maintenance and update process in place with defined roles and responsibilities.
6. Have a robust rationale in place for which parts of the audit universe you are not covering, and make sure you can verify that the audit universe if complete.

Introduction/background

An audit universe is the collective grouping of auditable 'components' – sometimes also called auditable areas, units or entities – that support the development of the internal audit plan and help to identify appropriate internal audit coverage that the chief audit executive (CAE) can then prioritise. There are different ways this can be developed. The CAE may also consider whether an audit universe is required at all. The International Standards do not require the CAE and internal

audit activities to develop and maintain an audit universe, but without one how will the CAE be able to demonstrate effective internal audit coverage to key stakeholders? The CAE can choose whether to create and/or maintain an audit universe based on factors such as:

- the organisation's geographical reach
- market sector volatility
- the activities undertaken by an organisation
- the volume of organisational change
- the risk and assurance requirements of an audit committee, board, and other key internal and external stakeholders.

Many organisations have regulatory requirements (for example SR13-1, Basel Committee on Banking Supervision and MaRisk in global financial services) which necessitate an audit universe to demonstrate completeness of coverage (in particular so that lower risk areas are not overlooked for long periods of time). If no such requirements exist, the CAE may consider if it is worth the time and effort to identify and keep up to date all the possible audits that can be undertaken. A CAE may need to revisit this decision from year-to-year. Furthermore, when assurance should be focused on the most significant risks facing the organisation (now or in the future), this may not require a separate inventory of auditable areas. Some organisations instead develop and maintain a risk universe of the risks they are facing, without the formally added dimension of the auditable entities/areas of those risks.

One of the advantages of having an audit universe is that it enables the internal audit activity to be clear about the extent of coverage of the organisation each year. It can also provide a degree of rigour and transparency around areas not being audited and help inform and support decisions over the internal audit activity's resourcing requirements. This guidance will consider the various types of building blocks, and discuss the ways in which an audit universe with multiple dimensions may be advantageous for organisations. It will also assist consideration over whether an audit universe is needed or not, and also provide support for those who choose to create and maintain one.

Types of audit universe segments and perspectives

There is no single way to create an audit universe. However, the audit universe must be divided into units (the names of which can vary, for example being called an auditable unit, entity, area). Each of these are ways in which the internal audit activity can view the organisation for risk assessment and audit planning purposes. Typical ways include business units / teams/areas of stakeholder responsibility, products, service lines or countries, as well as the inclusion of key programmes and projects to represent critical change activities. Each organisation needs to determine what works best for them. A retail organisation may, for instance, want to have separate auditable areas for each of their branches or outlets to enable risk assessment and coverage of operations where local managers are mitigating risks at the front line on a day to day basis.

Irrespective of which way the internal audit activity chooses to view risks, it is advisable that each auditable area is created on the basis of a consistent set of rules or guidance, so that each auditable area is roughly the same size as the others – for example, if the CAE focuses auditable areas on business units, each of the units should be at approximately the same level in the organisational hierarchy. This helps the CAE know that risks are not 'hidden' within one large auditable area and never reviewed. Similarly, it helps the CAE avoid a small auditable area being given greater attention with more detailed work, which may not be of equally high risk. As we will

see later, this is of importance if the internal audit activity chooses to use the auditable areas as the basis for determining audit frequency.

A consistent approach should be used as much as possible. If exceptions are needed, the CAE should make these consciously enabling the internal audit activity to provide better coverage and get a clearer view of risks. Local regulators may also have a view that will drive the CAE's approach to an audit universe for an organisation. For example this will facilitate separate reporting to the regulator.

Some organisations, in particular large international ones, may find it useful to leverage multiple perspectives in their audit universe to enable views through more than a single lens (often the organisational hierarchy). A multi-dimensional universe would give an additional perspective, for example the organisational units in a particular country, or a separate inventory of key change projects, or legal entities applicable to a particular part of the organisation. Each auditable area will then have one or more different additional 'features' that provide relevant information about the scope of the auditable area. This helps the individuals performing the risk assessment and helps scope the associated audit(s). It will also improve the CAE's ability to produce relevant management information and reporting about coverage.

This approach can also be used to help identify which parts of the audit universe are relevant for delivering on coverage requirements that are applicable for the internal audit activity. For example, by creating a separate audit universe 'inventory' of regulatory audit coverage requirements, the CAE could map these to each of the auditable areas.

The number of components

The number of audit universe components will usually depend on the complexity and nature of the organisation and its purpose and strategy. There is no 'one size fits all', but internal audit activities can use an objective measure to support the audit universe design, for example number of FTEs, asset value, impact on Profit and Loss (P&L), or any other metric that exists within the organisation and which is useful to aid the decision.

Auditable areas should not be so large that they 'hide' risks that are not being covered, nor should they be so small that it prevents the internal audit activity from seeing the overall holistic picture (separate top-down macro risk review is also useful to support this). If specific areas are considered so important that they need dedicated attention, the CAE can organise individual engagements in the audit plan, drawn from the audit universe, to address the top risks to the organisation. These engagements could focus on those aspects relevant to the location/business unit – the macro risks do not need to be addressed by the audit universe.

The CAE can use the audit universe to meet the needs of those audit committees and senior managers who value a degree of cyclical assurance, or who have regulatory requirements or industry standards to cover all parts of the organisation at some level and at some frequency.

Although the audit universe is optional, the IIA Standards require the CAE to establish a risk-based internal audit plan (Standard 2010 Planning and Implementation Guide 2010), meaning that there needs to be something on which to perform a risk assessment to determine what the risk-based plan should be. This includes not just the consideration of what we audit, but also the depth of testing that we perform and the type of assurance provided.

Where the organisation has a higher level of risk management maturity (see guidance on risk maturity assessment), there is a high likelihood risks will have been identified, assessed and responses chosen at various levels (strategic, operational in different units and across projects) without direct internal audit input and involvement. In these cases, it may be sufficient for internal audit to review management's monitoring of the key controls and their risk management processes, including reporting and risk judgements made such as risk acceptance and risk tolerance thresholds. In organisations with lower risk maturity, it would be expected that internal audit reviews the detailed key controls.

These are considerations that impact the audit universe. While there is not necessarily a one to one relationship between risks, auditable areas and audits, the CAE needs to be clear on how they interact. Many organisations have a risk taxonomy that is applied to the auditable areas, to support this. It may be convenient to group several risks into a single audit for one part of the organisation, or to focus on one topic across multiple auditable areas in a horizontal/thematic review. In these cases, ie if the relationship between auditable area and audit is not 1:1, the coverage tracking approach needs to be sufficiently mature to enable the necessary monitoring and reporting to take place. The output of the risk assessment over the auditable area is important in this respect, and it is therefore useful to explore in a bit more detail what the CAE may want to do with the auditable areas once they have decided on the design.

What to do with the components

Once the CAE has decided how best to design the audit universe, they also need to determine what they want to do with the output from each of the auditable areas. Many CAEs identify a risk level based on a risk assessment of each auditable area. Those areas within the audit universe with a lower risk ranking are usually audited less frequently than those with a higher risk rating. Indeed, it is possible that some areas within the audit universe will never be audited (where this is permitted by regulators). This highlights the relevance for the CAE to share the risk results with senior management and other key stakeholders. This can help validate the risk results, and drive collaboration across the lines of defence in relation to assurance provision.

The audit universe and the risk assessment results could be used as a basis for discussion with assurance providers from the first and second line (eg compliance or risk management) to determine whether internal audit should be testing all key controls or if it is possible to leverage the work of other assurance providers. Being able to use the work of others would help maximise efficiency, minimise duplication and enable internal audit to focus on the areas of highest risk (see Standard 2050 Coordination and Reliance and Coordination of assurance for more information). This type of collaboration can identify possible overlaps and gaps in assurance as well as opening a wider discussion within the organisation about the nature and extent of the assurance the various providers perform. Internal audit should include undertaking audits of other assurance providers so as to enable an assurance to be provided as to the reliability of their work.

The risk level of the auditable areas helps to determine coverage needs, which many organisations translate to a cycle so that each auditable area is covered at least once within the risk-based cycle it has been given (unless a conscious decision has been made to override this coverage frequency due to other risks being prioritised). Others identify only the high-level auditable areas and focus their efforts on those (with the option, as noted above, that other auditable areas can be covered by other assurance providers). A third option is to divide the audit universe and cover all parts on a

cycle irrespective of the relative risk of the auditable areas, however few organisations leverage this approach today, since it is important to make sure that the internal audit activity focuses on the management of significant risks, which this approach does not easily facilitate.

When determining the risk level and associate coverage cycle, a CAE may consider typical risk factors such as materiality, degree of change, known problems, complexity of operations, date of last audit etc. For all approaches, board/audit committee/senior management requests and regulatory requirements/expectations may override the coverage cycle, so the CAE should build this into the process to ensure completeness of internal and external coverage request considerations.

This means the audit universe can be a useful support to help communicate the amount of coverage by internal audit. This can be invaluable during resourcing and budgeting discussions. The CAE can also find the audit universe valuable when considering what must be covered to enable an 'overall audit opinion' in their annual reporting.

Update and maintenance

Whichever approach a CAE takes to their audit universe, they need to keep it up-to-date, accurate and complete. Usually, an objective measure is chosen as the check, eg all cost centres have been included in the audit universe, that all FTEs are accounted for, and/or that all applications/vendors/projects are included. Selecting more than one of these is possible and will give additional assurance that no key dimension has been missed from the audit universe and therefore excluded from coverage. The CAE should ensure that the update process is efficient to minimise unnecessary administrative overhead and takes account of organisational developments in a timely way.

Those closest to the audit universe (the audit teams) may be expected to be responsible for the content and design of the individual audits, depending on the size of the organisation. For smaller internal audit teams, this may well be undertaken by the CAE. For larger organisations, it can be useful to have a single point of ownership for the audit universe and its framework, to support and co-ordinate the maintenance process. This can include responsibility for initiating updates, confirming completeness, confirming that risk assessments have been completed timely and prior to the planning process, reporting on the adequacy of coverage and determining the design rules and guidance that internal audit teams should follow.

Further reading

IPPF

Standard - 2010 Planning
Standard - 2050 Coordination and reliance
Implementation guidance - 2010 Planning
Implementation guidance - 2050 Coordination and reliance
Supplemental guidance - Developing a risk-based internal audit plan

Technical guidance

How to derive an IT internal audit universe

Coordination of assurance services
Risk maturity assessment
Risk assessments and prioritisation of internal audit work