White Paper

IMPLEMENTING COMBINED ASSURANCE

Galvanize

About the author: Anil Jogani

Anil Jogani is a senior executive with considerable international experience in the IT industry throughout the UK, India, and Europe. A GRC, security, audit, and ERP software solutions professional, Anil regularly presents at international events and writes about IT governance, security, data privacy, audit, and control topics.

www.linkedin.com/in/jogan1

Special thanks: Liz Sandwith

Special thanks to Liz Sandwith, Chief Professional Practices Advisor, Chartered Institute of Internal Auditors, for reviewing this paper and providing additional feedback and content during its development.

https://www.linkedin.com/in/liz-sandwith-14b9879/

Contents

Implementing combined assurance

“Every time you insert another level of management in an enterprise’s hierarchy, the noise is doubled and the message cut in half.”

—Peter F. Drucker

This white paper is the second in a series on combined assurance. The first part, *What is combined assurance?*, gave an overview of the combined assurance model, detailed the main assurance providers, explored how the model complements the Three Lines of Defense, and explained how combined assurance provides a more holistic view of risk throughout the organization.

In this second white paper, we want to build on that foundation by examining how an organization could implement a combined assurance program.

It’s common for audit and other GRC professionals to struggle with implementing combined assurance because of a lack of the right tools or support. Also, combined assurance is a complex topic, and the dynamic nature of organizations makes it difficult to put it into practice.

That’s why we want to provide a method for implementing combined assurance—along with some tools and techniques—to help you get started.

Implementation process

Figure 1 breaks down the complexity of the implementation process for combined assurance.

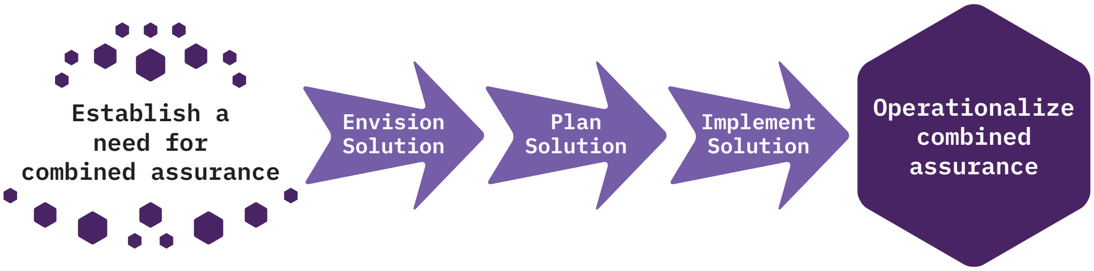
Establish a need for combined assurance
Envision Solution
Plan Solution
Implement Solution
Operationalize combined assurance

Figure 1: *The combined assurance implementation process.*

Establishing the need

You know the challenges that can arise when multiple assurance projects are carried out by many different assurance providers. In fact, we covered many of them in our earlier paper. Now, in this first stage, think about your specific challenges and take a methodical approach to establishing the need for a combined assurance program. In this first stage, we'll show you how to:

1. Assess impact and create an assurance map.
2. Define implementation risks.
3. Define resources and deliverables.
4. Raise awareness and get management commitment.
5. Assign accountability.

CRITICAL OUTPUT

There are two essential outputs that will help you.

1. **Impact assessment:** Analysis of your current state and the desired combined assurance state.
2. **Assurance map:** Details of assurance providers involved, as well as frequently audited business areas.

ASSESS IMPACT & CREATE AN ASSURANCE MAP

The impact assessment and assurance map are interdependent—and the best possible starting point for your combined assurance journey. An impact assessment begins with a critical look at the current or "as is" state of your organization. As you review your current state, you build out your assurance map with your findings. You can't really do one without the other.

The map, then, will reveal any overlaps and gaps, and provide insight into the resources, time, and costs you might require during your implementation.

Looking at an assurance map example will give you a better idea of what we're talking about. The Institute of Chartered Accountants of England and Wales (ICAEW) has an excellent template (reproduced in Appendix 1). The ICAEW has also provided a guide[1] to building a sound assurance map. The institute suggests you take the following steps:

1. Identify your sponsor (the main user/senior staff member who will act as a champion).
2. Determine your scope (identify elements that need assurance, like operational/business processes, board-level risks, governance, and compliance).
3. Assess the required amount of assurance for each element (understand what the required or desired amount of assurance is across aspects of the organization).
4. Identify and list your assurance providers in each line of defense (e.g., audit committee or risk committee in the third line).
5. Identify your assurance activities (compile and review relevant documentation, select and interview area leads, collate and assess assurance provider information).
6. Reassess your scope (revisit and update your map scope, based on the information you have gathered/evaluated to date).
7. Assess the quality of your assurance activities (look at breadth and depth of scope, assurance provider competence, how often activities are reviewed, and the strengths/quality of assurance delivered by each line of defense).
8. Assess the aggregate actual amount of assurance for each element (the total amount of assurance needs to be assessed, collating all the assurance being provided by each line of defense).
9. Identify the gaps and overlaps in assurance for each element (compare the actual amount of assurance with the desired amount to determine if there are gaps or overlaps).
10. Determine your course of action (make recommendations for the actions to be taken/activities to be performed moving forward).

Just based on the steps above, you could understand how your desired state evolves by the time you reach step 10. Ideally, by this point, gaps and overlaps have been eliminated. But the steps we just reviewed don't cover the frequency of each review and they don't determine costs. So we've decided to add a few more steps to round it out:

11. Assess the frequency of each assurance activity.
12. Identify total cost for all the assurance activities in the current state.
13. Identify the total cost for combined assurance (i.e., when gaps and overlaps have been addressed, and any consequent benefits or cost savings).

[1] https://www.icaew.com/technical/audit-and-assurance/assurance/assurance-mapping/10-steps-to-prepare-your-assurance-map

Use risk across the business as the tool to decide which areas require assurance. This will give you a more complete assessment of assurance, and makes the assurance map a more valuable and strategic tool to the board and audit committee. You'll also get a better understanding of the level of assurance provided by each line of defense.

DEFINE THE RISKS OF IMPLEMENTATION

Implementing combined assurance is a project, and like any project, there's a chance it can go sideways and fail, losing you both time and money. So, just like anything else in business, you need to take a risk-based approach. As part of this stage, you'll want to clearly define the risks of implementing a combined assurance program, and add these risks, along with a mitigation plan and the expected benefits, to your tool kit.

As long as the projected benefits of the project outweigh the residual risks and costs, the implementation program is worth pursuing. You'll need to be able to demonstrate that a little further down the process.

DEFINE RESOURCES & DELIVERABLES

Whoever will own the project of implementing combined assurance will no doubt need dedicated resources in order to execute. So, who do we bring in?

On first thought, the internal audit team looks best suited to drive the program forward. But, during the implementation phase, you'll actually want a cross-functional team of people from internal control, risk, and IT, to work alongside internal audit. So, when you're considering resourcing, think about each and every team this project touches.

Now you know who's going to do the work, you'll want to define what they're doing (key milestones) and when it will be delivered (time frame).

And finally, define the actual benefits, as well as the tangible deliverables/outcomes of implementing combined assurance. (The table below provides some examples, but each organization will be unique.)

BENEFITS OF COMBINED ASSURANCE	TANGIBLE DELIVERABLES OF COMBINED ASSURANCE
Consolidated, single source of truth	Accessible and harmonized data
More informed audit committee	Integrated, holistic assurance reporting
Streamlined workflows/time savings	Automated, standardized process

RAISE AWARENESS & GET MANAGEMENT COMMITMENT

Congratulations! You're now armed with a fancy color-coded impact assessment, and a full list of risks, resources, and deliverables.

The next step is to clearly communicate and share the driving factors behind your combined assurance initiative. If you want them to support and champion your efforts, top management will need to be able to quickly take in and understand the rationale behind your desire for combined assurance.

Critical output: You'll want to create a presentation kit of sorts, including the assurance map, lists of risks, resources, and deliverables, a cost/benefit analysis, and any supporting research or frameworks (e.g., the King IV Report, FRC Corporate Governance Code, available industry analysis, and case studies). Chances are, you'll be presenting this concept more than once, so if you can gather and organize everything in a single spot, that will save a lot of headaches down the track.

ASSIGN ACCOUNTABILITY

When we ask the question, "Who owns the implementation of combined assurance?", we need to consider two main things:

- Who would be most impacted if combined assurance were implemented?
- Who would be senior enough to work across teams to actually get the job done?

It's evident that a board/C-level executive should lead the project. This project will be spanning multiple departments and require buy-in from many people—so you need someone who can influence and convince. Therefore, we feel that the chief audit executive (CAE) and/or the chief revenue officer (CRO) should be accountable for implementing combined assurance.

The CAE literally stands at the intersection of internal and external assurance. Where reliance is placed on the work of others, the CAE is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity. And the CRO is taking a more active interest in assurance maps as they become increasingly more risk-focused.

The Institute of Internal Auditors (IIA), Standard 2050, also assigns accountability to the CAE, stating:

> *"The chief audit executive should share information and coordinate activities with other internal and external assurance providers and consulting services to ensure proper coverage and minimize duplication of effort."* [2]

So, not only is the CAE at the intersection of assurance, they're also directing traffic—exactly the combination we need to drive implementation.

[2] *Institute of Internal Auditors, 2016, International standards for the professional practice of internal auditing*

Envisioning the solution

You've summarized the current/"as is" state in your assurance map. Now it's time to move into a future state of mind and envision your desired state. What does your combined assurance solution look like? And, more critically, how will you create it?

This stage involves more assessment work. Only now you'll be digging into the maturity levels of your organization's risk management and internal audit process, as well as the capabilities and maturity of your Three Lines of Defense. This is where you answer the questions, "What do I want?", and "Is it even feasible?" Some make-or-break capability factors for implementing combined assurance include:

1. Corporate risk culture

Risk culture and risk appetite shape an organization's decision-making, and that culture is reflected at every level. Organizations who are more risk-averse tend to be unwilling to make quick decisions without evidence and data. On the other hand, risk-tolerant organizations take more risks, make rapid decisions, and pivot quickly, often without performing due diligence. How will your risk culture shape your combined assurance program?

2. Risk management awareness

If employees don't know—and don't prioritize—how risk can and should be managed in your organization, your implementation program will fail. Assurance is very closely tied to risk, so it's important to communicate constantly and make people aware that risk at every level must be adequately managed.

3. Risk management processes

We just stated that risk and assurance are tightly coupled, so it makes sense that the more mature your risk management processes are, the easier it will be to implement combined assurance. Mature risk management means you've got processes defined, documented, running, and refined. For the lucky few who have all of these things, you're going to have a much easier time compared to those who don't.

4. Risk & controls taxonomy

Without question, you will require a common risk and compliance language. We can't have people making up names for tools, referring to processes in different ways, or worst of all, reporting on totally random KPIs. In the words of Sam C. J. Huibers in his research paper for The IIA Research Foundation on Combined Assurance,[3] the result of combined assurance should be "one language, one voice, one view" of the risks and issues across the organization.

5. System & process integrations

An integrated system where there is one set of risks and one set of controls is key to delivering effective combined assurance. This includes:

+ Risk registers across the organization
+ Controls across the organization
+ Issues and audit findings
+ Reporting.

There shouldn't be duplicate issues and findings, and all relevant data and findings should be conveyed in one integrated report. To achieve this, organizational silos have to be broken down and cross-functional teams must work together. The degree of integration reflects the risk maturity within the organization. Low integration equals low maturity. High integration equals high maturity.

[3] *The IIA Research Foundation, 2015, Combined assurance: One language, one voice, one view*

6. Technology use

Without dedicated software technology, it’s extremely difficult to provide a sustainable risk management system with sound processes, a single taxonomy, and integrated risks and controls.

How technology is used in your organization will determine the sustainability of combined assurance. (If you already have a risk management and controls platform that has these integration capabilities, implementation will be easier.)

7. Using assurance maps as monitoring tools

Assurance maps aren’t just for envisioning end-states; they’re also critical monitoring tools that can feed data into your dashboard. They can inform your combined assurance dashboard, to help report on progress.

8. Continuous improvement mechanisms

A mature program will always have improvement mechanisms and feedback loops to incorporate user and stakeholder feedback. A lack of this feedback mechanism will impact the continued effectiveness of combined assurance.

We now assess the maturity of these factors (plus any others that you find relevant) and rank them on a scale of 1-4:

+ **Level 1:** Not achieved (0-15% of target).
+ **Level 2:** Partially achieved (15-50%).
+ **Level 3:** Largely achieved (50-85%).
+ **Level 4:** Achieved (85-100%).

This rating scale is based on the ISO/IEC 15504 that assigns a rating to the degree each objective (process capability) is achieved.

An example of a combined assurance capability maturity assessment can be seen in Figure 2.

	Current maturity level				Desired level
Factor/attribute	**Level 1**	**Level 2**	**Level 3**	**Level 4**	
Corporate risk culture			X		3
Risk management awareness		X			4
Risk management processes		X			3
Risk & controls taxonomy		X			4
Extent of integration		X			4
Use of technology		X			3
Use of assurance map		X			4
Continuous improvement		X			4

Figure 2: *Combined assurance maturity assessment.*

GAP ANALYSIS

Once the desired levels for all of the factors are agreed on and endorsed by senior management, the next step is to undertake a gap analysis. The example in Figure 2 shows that the current overall maturity level is a 2 and the desired level is a 3 or 4 for each factor. The gap for each factor needs to be analyzed for the activities and resources required to bridge it. Then you can envision the solution and create a roadmap to bridge the gap(s).

SOLUTION VISION & ROADMAP

An example solution vision and roadmap could be:

- We will use the same terminology and language for risk in all parts of the organization, and establish a single risk dictionary as a central repository.
- All risks will be categorized according to severity and criticality and be mapped to assurance providers to ensure that no risk is assessed by more than one provider.
- A rolling assurance plan will be prepared to ensure that risks are appropriately prioritized and reviewed at least once every two years.
- An integrated, real-time report will be available on demand to show the status, frequency, and coverage of assurance activities.
- The integrated report/assurance map will be shared with the board, audit committee, and risk committee regularly (e.g., quarterly or half-yearly).
- To enable these capabilities, risk capture, storage, and reporting will be automated using an integrated software platform.

Figure 3 shows an example roadmap to achieve your desired maturity level.

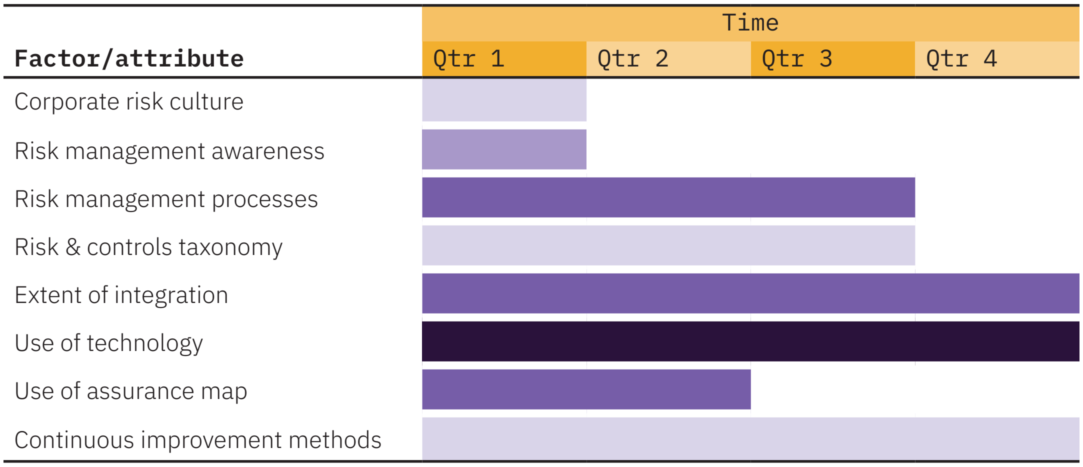

Figure 3: *Maturity level roadmap.*

You can easily adapt these examples to suit your needs. Based on the solution vision, gap analysis, and roadmap, you can now plan the solution.

Planning the solution

Your solution to achieve combined assurance needs to be broken down into projects and activities. These can then be implemented properly, in line with the objectives of your solution. The roadmap already highlights the various projects and timelines. These projects should now be further broken down into either sub-projects or tasks that can be assigned. Each task should have a task owner and timeline. This is also called a work breakdown structure (WBS). (For an example of a WBS for implementing the assurance map, see Appendix 2.)

The plan should contain a WBS for each factor/attribute mentioned in the solution vision and roadmap.

WAYS TO INTEGRATE YOUR ASSURANCE ACTIVITIES

Assurance activities across the lines of defense can be combined in a few different ways. For the ideal outcome, you need to assess what works best for your organization.

Internal audit often plays the part of the coordinator and would also perform reviews of certain activities on its own or jointly with another provider. However, it's essential that internal audit retains its core independence function so that it's able to provide an objective and impartial view.

Here are some ways that the assurance activities could be coordinated and combined:

1. **Joint audits.** Different teams across the lines of defense carry out audits together and issue a joint report (e.g., internal controls and SOX teams can review the state of controls together).
2. **Coordinated activities.** The different teams carve out areas among themselves and carry out the reviews separately. Each produces a separate report that may or may not be consolidated.
3. **Integrated reporting.** Audits are carried out separately, but teams get together to produce a single report.
4. **Integrated functional processes.** In this technique, processes are integrated so that only one report is necessary (e.g., risk management and internal controls could be integrated, and a risk-based control status report produced).

Implement your combined assurance plan

Now is the time you set your plan into motion. It's here where you kick off the implementation of combined assurance by:

- Executing all of the tasks, activities, and projects detailed in the plan.
- Monitoring the projects during implementation, keeping stakeholders informed, taking any corrective action, and ensuring activities are completed as planned.
- Monitoring implementation performance.
- Communicating the availability of combined assurance to stakeholders, as well as across the organization, and informing them of the benefits.
- Appointing skilled and knowledgeable people to provide training to the stakeholders and users of combined assurance tools.
- Reviewing plan effectiveness to ensure that objectives are being met. (Here you would carry out a post-implementation review, assess results and experience gained, and record and share lessons learnt. Then compare results with your original criteria for success.)
- Gathering feedback from the implementation team and stakeholders via interviews or surveys.

Operationalize your combined assurance program

Once combined assurance has been implemented, you need to make it sustainable. This involves establishing mechanisms for:

- Providing support for combined assurance and its components, including the software platform.
- Regularly reviewing your combined assurance program to assess its effectiveness, especially when there are changes to organizational structure or the introduction of new regulations.
- Capturing user and stakeholder comments and feedback.
- Kicking off improvement projects so that the program evolves and improves over time.

Implementing a combined assurance program is an ongoing process. It’s impacted by organizational, socio-political, governmental, and societal influences. Using a program management approach and established project management techniques helps ensure that the implementation is successful.

Fortunately, software solutions are available that have the flexibility to incorporate these changes and provide data-driven integrated assurance reports. Organizations that have implemented combined assurance have experienced many benefits. One example is FirstRand, South Africa,[4] which:

- Reduced duplicate work and eliminated assurance fatigue.
- Shifted its assurance approach to focus on the most critical risks.
- Developed a common view of risks and issues across the organization.
- Implemented a common taxonomy, which has resulted in more value-added discussions.
- Delivered more precise and insightful reports.
- Realized cost savings through better resource allocation and greater assurance coverage.
- Established a commitment to enhance controls.

[4] *The IIA Research Foundation, 2015, Combined assurance: One language, one voice, one view*

Conclusion

By now, you should have a pretty good idea of how you can implement a combined assurance program.

From developing an impact assessment and assurance map to guide your activities and define your stakeholders, to detailing how to get management approval and defining deliverables, we've detailed all of the necessary steps.

We've also discussed the tools—including gap analysis, maturity assessments, and solution roadmaps—that will help you throughout your implementation process.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 6,300 customer organizations in 130 countries, Galvanize is connecting teams in many of the Fortune 1,000 and S&P 500 companies, and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Learn more about what you can accomplish with Galvanize
1.888.669.4225 | wegalvanize.com | info@wegalvanize.com

APPENDIX 1: ASSURANCE MAP TEMPLATE (ICAEW)

		Management (first line)				Management (second)			Management (third)				Management (fourth)			
Objectives of assurance activity: Confidence in effectiveness of governance, risk management, & controls	Desired/ required amount of assurance	Policies	Control framework	Management review	Current amount of assurance	Board 1	Board 2	Current amount of assurance	2 Authorities	Operating Committee	Audit Committee	Current amount of assurance	External 1	External 2	Current amount of assurance	Current amount of assurance
GOVERNANCE: Objective of assurance activity 4																
Conduct, culture, & behavior	L	GOV2			L			NONE				NONE			NONE	L
Vision & strategy setting	M	GOV3		GOV4	M	GOV5		L				NONE			M	L
	M	GOV7			M	GOV8		L				NONE			M	L
OPERATIONAL TASKS																
Operational tasks	H	DEF1		GOV1	H	GOV1		H				H	N/A	N/A	N/A	H
BOARD RISKS: Objective of assurance activity																
Output risk 1	H	RSK1			L	GOV1		H	RSK20			H			NONE	H
Output risk 2	M	RSK2		RSK3	M	GOV1		H	RSK20			H			NONE	H
	M			RSK4	M	GOV1		H	RSK20			H			NONE	H
Input risk 1	H		RSK11	RSK12	M	GOV1		H	RSK20			H			L	H
	H			RSK13	M	GOV1		H	RSK20			H			L	H
	H			RSK14	M	GOV1		H	RSK20			H			L	H
Input risk 1	H		RSK11	RSK13	L	GOV1		H	RSK20			H			L	H
PROCESSES/RELEVANT AUTHORITIES: Objective of assurance activity																5
P3M	M	PRO1		PRO2	L			L		PRO4	PRO5	M		PRO7	M	M
	M			PRO10	L			L				M		PRO11	M	M
Personnel administration	M	PRO30		PRO31	L		PRO32	L				L			NONE	L
	M				L		PRO34	L				L			NONE	L
Inclusion & diversity 1	M			PRO35	M			NONE				NONE			NONE	L
	M			PRO36	M			NONE				NONE			NONE	L
	M			PRO37	M			NONE				NONE			NONE	L
	M			PRO23	M			NONE				NONE			NONE	L
Finance	H	PRO38	PRO39	PRO40	H		PRO41	M	PRO42		PRO43	M	PRO47	PRO48	H	H
	H		PRO49	PRO50	H	GOV1	GOV1	M	PRO51			M	PRO53		H	H
	H			PRO54	H			M	PRO55			M	PRO56		H	H
	H			PRO40	H			M				M	PRO57		H	H
Health & safety	M	PRO77	PRO78	PRO79	H	PRO80		L	PRO82		PRO83	M			M	H
	M			PRO85	H			L	PRO86			M			M	H
	M		3	PRO8	H			L				M			M	H
Business resilience	L			PRO89	L	GOV1	GOV1	L	PRO91		PRO92	L			NONE	L
Security	H	PRO93	PRO94	PRO95	H			L	PRO97		PRO98	M			L	M
	H	PRO102	PRO103	PRO104	H	GOV1	GOV1	L	PRO105			M			L	M
	H		PRO107	PRO108	H			L	PRO109			M			L	M
	H			PRO110	H			L				M			L	M
Fraud	M			PRO135	L		PRO136	L				L			L	L
	M				L		PRO117	L				L			L	L

KEY

1 Elements requiring assurance are the headings for each row.
2 Assurance providers are the headings for each column, grouped by line of defense.
3 Activities are detailed for each element (row) and assurance provider (column). These can be presented as references, linking through to a reference key, or as descriptions of what the activity was (e.g., monthly health & safety audits).
4 Desired/required amount of assurance for each element (high, medium, low).
5 Current amount of assurance at each line of defense and then overall for each element (high, medium, low, none).

■ No assurance desired/provided.
■ Low amount of assurance desired/provided.
■ Moderate amount of assurance desired/provided.
■ High amount of assurance desired/provided.

Quality of the assurance activity is depicted by the shade of the color of the activity in the body of the map.

■ Broad and deep scope of assurance activity. Activity is performed by subject matter experts frequently throughout the year, following recognized and appropriate methodology/standards.

■ Narrow and shallow scope of assurance activity. Activity is performed by generalists or on an ad hoc basis throughout the year and doesn't follow recognized and appropriate methodology/standards.

APPENDIX 2: WORK BREAKDOWN STRUCTURE

Work breakdown structure		
Project name	**Implement the use of assurance map**	**Project owner**
Activities	**Tasks**	**Task owner**
Identify areas/elements that need assurance. (Elements can include business processes & resilience, fraud, & regulatory compliance).	➡ Identify sources of information for the areas that need assurance. For example: previous audit reports, board papers, risk reports, corporate plans, etc. ➡ Confirm the sources with senior management/project sponsor.	
Assess the required amount of assurance for each element.	➡ Assess complexity & criticality of the element. ➡ Assess risks. ➡ Review past assurance reports for each element, as well as their coverage & frequency. ➡ Determine the amount of assurance required. ➡ Get approval from chief audit executive (CAE).	
Identify the assurance providers.	➡ Check whether assurance is being provided in each of the areas it's required. ➡ Identify the providers & any gaps. ➡ If not already done, review past assurance reports of each provider & their coverage and frequency. ➡ Note the coverage, duration, & frequency of their activities.	
Interview assurance providers.	➡ Assign interviewer from project team. ➡ Identify the individuals to interview. Interview and find out: the depth, breadth, & frequency of the scope. ➡ Determine who carries out the review and their competency, as well as which line of defense. ➡ Identify who consumes the report. ➡ Determine follow-up activities & current status.	
Assess the actual amount of assurance received for each element.	➡ Review interview notes & other sources of information. ➡ Note the actual amount of assurance received from each provider for each element in terms of frequency, timing, depth, & breadth of activities (as well as whether it's internal or external), & line of defense.	
Record in the assurance map.	➡ For each element requiring assurance, record the desired amount/level of assurance & the actual amount received. ➡ Break them down according to the lines of defense for each element.	
Analyze the gaps and overlaps in assurance for each element.	➡ For each element requiring assurance, identify deviations from your desired amount of assurance. ➡ Identify areas with excess assurance. ➡ Identify areas that have insufficient or no assurance. ➡ Discuss findings with your CAE & other users of the assurance map.	
Recommend the course of action.	➡ Based on the findings above, provide recommendations to reduce excess assurance & increase where it's insufficient.	