Paul Gascoigne
K10VISION

How to deliver real value from your investment in Audit Management Software...
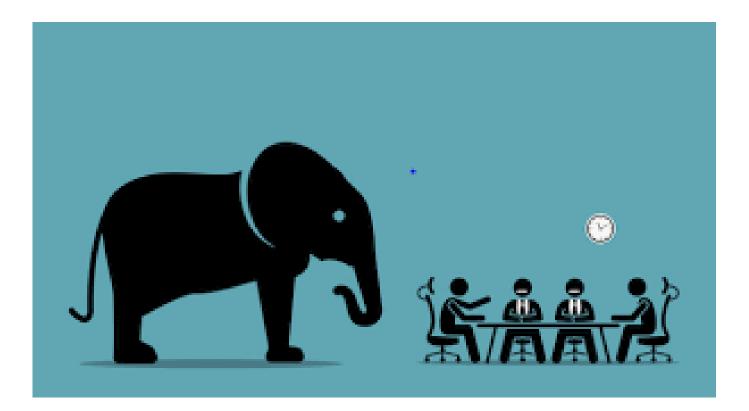
...a practical guide

The elephant in the room:

- I am a software company owner talking to you about software …

Establishing realistic expectations of yourself and your software:

- What are you REALLY expecting

    - Efficiencies, dashboards, reporting, standards compliance etc…

- How IT savvy is your team – will your audit staff pick up working with new technology very easily

- Has your Audit Committee stated their expectations

- Remember the true investment is never cash … it is always time

- Create a realistic timeline – the day job doesn't disappear

    - Ensure your software provider clearly understands your timelines

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Establishing realistic expectations of yourself and your software:

- Your expectations should not be routed in software you used 5, 10 or 15 years ago

  - Technologies have advanced rapidly

  - Address where your software selection is in its lifecycle

    - Will it still be current and relevant in 10 to 15 years time?

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Leveraging "your" value:

- No-one ever said I want to spend thousands building a documentary repository
  - If your aspiration is nothing more than working outside your AMS and then adding documents back in as you go then please do not waste your money

Leveraging "your" value:

- No-one ever said I want to spend thousands building a documentary repository

  - If your aspiration is nothing more than working outside your AMS and then adding documents

    back in as you go then please do not waste your money

- If your AMS is not integral to your core auditing processes then the value collapses

Leveraging "your" value:

- No-one ever said I want to spend thousands building a documentary repository

    - If your aspiration is nothing more than working outside your AMS and then adding documents

        back in as you go then please do not waste your money

- If your AMS is not integral to your core auditing processes then the value collapses

- Let's discuss – best practice – is this the domain of the software companies?

Avoid being blinded by sales tactics:

- Be aware to make use of month, quarter and year ends – real savings are available for some

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Avoid being blinded by sales tactics:

- Be aware to make use of month, quarter and year ends – real savings are available for some

- Still surprising when you hear:

  - I didn't realize it had a limited number of fields

  - We didn't realize there wasn't any Annual Planning

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Avoid being blinded by sales tactics:

- Be aware to make use of month, quarter and year ends – real savings are available for some

- Still surprising when you hear:

  - I didn't realize it had a limited number of fields

  - We didn't realize there wasn't any Annual Planning

- Watch out for LOADED RFI's – all industry players have their own version

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Avoid being blinded by sales tactics:

- Be aware to make use of month, quarter and year ends – real savings are available for some

- Still surprising when you hear:

    - I didn't realize it had a limited number of fields
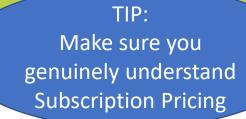
    - We didn't realize there wasn't any Annual Planning

- Watch out for LOADED RFI's – all industry players have their own version

- Beware of false expertise:

    - ESG, GRC, working papers, frameworks etc (the latest buzz words have a habit of appearing front and centre of software companies' sales materials)

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Getting the pace of rollout right for maximum impact:

- Most important – keep training as close to go live as possible

- Get everyone to work and deliver an audit as soon as humanly possible – get started

  - If you wait until everything is "perfect" you have wasted an opportunity to get going

- Decide on the "process must haves", for example:

  - Audit Planning

  - Conducting Tests

  - Review Of Working Papers

  - Etc…

How does Pareto apply to your investment:

- 20% of the functionality you purchase will deliver 80% of the value
  - Therefore be careful how you weight your functional requirements
  - Focus functional requirements on what you will actually benefit from
    - E.g. robust electronic working papers vs auto transcription

Lessons from the coal face:

- Crazy calculations do not automatically mean brilliant procurement

The Recurrent Costs (R) are reduced to net present value and determined using the following formula:

$$R \equiv \sum_{X=1}^{N} \frac{R_x}{(1+I)^x}$$

where

N = number of years of evaluated recurrent costs

x = an index number 1, 2, 3, … N.

R_x = total Recurrent Costs for year "*x*," as recorded in the Recurrent Cost Sub-Table.

I = discount rate to be used for the Net Present Value calculation, as specified **in the TDS for ITT 33.3.**

or Option 2:

*[specify **alternative recurrent cost evaluation scheme** or state **"none"**]*

(b) The score for each feature (i) within a category (j) will be combined with the scores of features in the same category as a weighted sum to form the Category Technical Score using the following formula:

$$S_j = \sum_{i=1}^{k} t_{ji} \times W_{ji}$$

where:

t_{ji} = the technical score for feature "i" in category "j"

w_{ji} = the weight of feature "i" in category "j"

k = the number of scored features in category "j", and

$$\sum_{j=1}^{n} W_j = 1$$

(c) The Category Technical Scores will be combined in a weighted sum to form the total Technical Tender Score using the following formula:

$$T = \sum_{j=1}^{n} S_j \times W_j$$

where:

S_j = the Category Technical Score of category "j"

W_j = the weight of category "j" as specified in the TDS

n = the number of categories, and

ARAC

Lessons from the coal face:

- Profit vs the profession ...

  - *Remember ... software companies absolute focus is profit, growth and market share*

  - *Never confuse their interest in your profession to be something even close to yours*

    - *You are the custodians of your profession*

    - *You are the true audit professionals*

  - *Learn about the players in the software market – become educated on their DNA*

    - *What is their customer service really like?*

    - *What is their culture?*

    - *What does a 15 year relationship really look like?*

UAE Internal Auditors Association
JOIN, LEARN & SHARE

ARAC

Lessons from the coal face:

- Subscription …

  - *Only exists to make software companies more money*

  - *Has underpinned the move to CLOUD and has eliminated a lot of on-premise options in the marketplace*

    - *So much so that we have some of the larger players literally ignoring whole segments of the market*

UAE Internal Auditors Association
JOIN, LEARN & SHARE

ARAC

Lessons from the coal face:

- Proximity is not the same as competence (this is 2023) …

  - *So many audit teams want their software company to have employees, agents or resellers close by*

    - *Just because a living, breathing human lives near you does not necessarily equate to the reality of high quality local support*

Lessons from the coal face:

- Large = simpler ...

  - *Time and time again the large audit teams place less pressure on the software companies than the small audit teams*

  - *Once a team gets larger than 50 the complexity often rapidly decreases*

    - *This applies to all industries and all sectors*

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Lessons from the coal face:

- How valuable is your business …

    - *If you pay $20,000 per annum in fees for your AMS this increases the value of the software company by ?????*

Lessons from the coal face:

- How valuable is your business …

    - *If you pay $20,000 per annum in fees for your AMS this increases the value of the software company by:*

        - *$80,000 to $220,000 (dependent on whether the company is quoted or not)*
        - *This is why your business is so valuable*

ESG – audit management software's role. Reality or myth:

- Audit Management Software is like a car – it will take you from A to B, however the route you take and how fast you get there is still determined by the driver

- AMS technology is NOT the holy grail for ESG auditing … brilliant, smart, intellectually adept auditors is the real solution

- Be very careful of software companies claiming to be EXPERTS in ESG, GRC, Framework XYZ etc…

- Also – be very careful of consultants who suddenly rebrand themselves!!!

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

How Can Internal Auditors Drive Change
Towards Sustainable Supply Chain?

Session Code

301122

Volkan Pekince
Group Chief Internal Audit, DIB

Face with the Reality

- Every auditor should understand and acknowledge that nobody wants to be audited: Think about the External QA Reviews you have been subject to.

- Being audited is inherently tense / annoying experience for all parties involved, everybody behaves like this is not the case.

- You will never be the most popular person / team in the organization.

    - Do your job properly and highlight many risks   :   you are unpopular bad person

    - Don't do your job and a fraud happens / regulator highlight issues   :   you are unpopular bad person

Face with the Reality

It is very difficult to build an effective and healthy relationship with the auditee due to common perceptions:

AUDITOR

What they say	How it is perceived
- We are here to help	- I need to prove myself
- We would like to work with you to identify opportunities for improvement	- I should raise at least 5 High Risk, 8 Medium Risk issues
- We are not policemen	- If no issue, my capabilities will be questioned
- We don't have any KPI linked to # of issues we identify	- Hope I will identify some fraud cases so that I can get a promotion
- We will respect the ongoing workload of your teams	- Tell me your problems and I will make them audit findings against you
	- I can not delay the completion of this audit, would impact my annual plan

AUDITEE

What they say	How it is perceived
- We value the view of audit to see our gaps from a third eye	- A bad audit report would create a dent in my career / bonus
- We benefited a lot from the last audit. It is very important for us to understand our gaps and close them immediately.	- Whatever I am aware of as problems / gaps, I will keep them to myself
- We will provide every data / information requested	- No, you can not see our confidential data
- We will help auditors understand our business	- Last audit was a proper waste of time
	- These guys are like bunch of teenagers and no clue about the business. We can pacify them with lots of technical jargon.
	- We will disagree with anything they say. Even if factually correct, we will disagree with ownership

Good Communication requires / involves:

- Good writing skills

- Effective verbal communication skills

- Advanced presentation skills (this doesn't mean Power Point wizardry)

But it is much more than that; Good Communication requires / involves good and reliable attitude and behavior.

As internal auditors, you continuously live with your auditee. **Talking the talk** might be good enough for consultants, but you will need to be **walking the walk** as well.

Your auditee at every level should know that:

- You do what you say you would do
- They can trust you and can be open with you without any hesitation
- You looking good will not be at the expense of how they look
- You will understand and digest all necessary technical details of the subject before commenting on them
- You will be able to give the right messages with the right context to the right audience (line management, CEO, Board, Regulators etc.)
- You don't exaggerate non-worthy subjects
- You are happy to except when you are proven to be wrong

But also,
- You won't downplay important things
- You won't mix personal relationship with professional relationship
- Audit is a serious business requiring discipline on both sides
- Audit reports are "exception based", not designed to praise people
- Once an issue is raised, it won't disappear magically

Without all these, your communication will never be fully effective.

Message 1

Audit is not something done **to** the Auditee; It is done **with** the Auditee

Message 2

Audit execution is Agile and do not create unnecessary workload

Message 3

Audit issues / reports will be disclosed to the wider audience only after full alignment (no necessarily full agreement)

Message 4

Internal Audit's independence is for you, not against you

Message 5

Internal Audit is able to derive an objective and concise message out of the audit report

Message 6

Audit issues to be taken seriously and require proper discipline for their follow-up and closure

ZERO TENSION

ZERO SURPRISE

FULL TRANSPARENCY

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

SIMPLIFY

Audit universe:

- You don't need to replicate the organizational structure of the company. Be **product / process based.**

- Rank the entities based on their inherent risks, **not the residual risks.**

Annual planning

- Big excel files with loads of formulas / macros calculating how important and entity is and how much manpower needs to be allocated for each audit are complete waste of time.

- Just rank the entities based on their inherent risks, define the frequency based on the risk ratings and you have the annual plans for the next 3-4 years.

❑ Create the (draft) Audit Universe and the Annual Plan via internal workshops with all internal auditors.

   Now, everybody in Internal Audit owns the plan

❑ Discuss the audit universe, entity risk assessments and annual plan for the year with all business areas in the form of workshops (Chiefs and their direct reports) to get their feedback / input.

   Now, everybody in the management contributed to the plan

❑ Once finalized, share the entire plan with the entire senior management.

   Now, everybody in the organization knows the plan with full transparency

AGILE EXECUTION

Working in isolation / behind a mystic cloud during the audit fieldwork is not necessary. Sharing a "very" draft issue quickly is a healthy check, even if it is proven inaccurate and can save a lot of time.

- The purpose of the Factual Accuracy Confirmation is to confirm with the auditee that what we are working on as a potential observation is accurate.

- At this point, you don't have a solid idea about the extend, full relevancy, applicability, risk involved, control quality etc. Therefore, the wording of the document should be very simple, without any judgement or indication about the **risk level.**

- You don't need to provide too much information or context or background.

- The auditee should be able to respond in a very simple way; ideally Yes / No.

- No need to ring the alarm bells yet.

The profit calculation is done outside the system via excel files. Excel files are stored in a shared folder that could be accessed by 7 people with read / write privileges (6 product team, 1 IT).

The applications can be processed by one person without system approval. The system does not have detailed maker / checker profiles.

Some of the Policies were not approved by Legal (9) and Sharia (13); see the list below.

Circa 180 documents (original) in relation to the customer applications are pending to be sent to the Central Operations for 3 months.

The users can select the GL accounts manually during the vendor payments (i.e. the system does not assign the relevant GL automatically).

The internal blacklist name matching is not always effective (see examples which were missed) and the results can be overwritten by the users.

AGILE EXECUTION

- Critical Issue escalation: Serious gaps should be escalated immediately, after alignment with the auditee, rather than waiting until the full completion.

- Fluid / flexible scope: your scope should expand or contract easily, without any bureaucracy.

- Draft observation sharing very frequently: Share draft issues **without risk ratings** until full agreement is reached.

    Issue Risk Rating Mechanism:

    - Every audit department has a complicated matrix with parameters and calculations.

    - But everyone knows that the risk rating is 90% judgmental. If you are having to calculate the risk rating to justify what you say, it means you could not properly explain what the issue is.

    - Clearly tell everyone that the risk ratings are judgmental and will not be assigned until the full final draft report is created.

    - Be flexible and pragmatic. High or Medium, every audit issue has to be fixed.

- Close out Meetings:

    - You are an important function of your organization. Your interaction approach and level should reflect this. Your close out meetings should be attended by all relevant and most senior people (direct reports of the CEO).

    - This would help with the ownership arguments.

    - Tension is your enemy. It makes even the simple thing complicated and difficult.

EFFECTIVE AUDIT REPORTS

- Audit Reports can easily be very boring, unattractive and unreadable.

- Making use of visual effects (animations, photos, videos) will not help with this. You must have seen;

    Internal Audit reports

    - in MS Word format with no color, table, diagram, pure "Times New Roman" verbiage.

    - starting with a number of boring sections (Background, objective and scope of the audit etc.).

    - followed by a series of repeating titles (finding, risk, recommendation, management response, finding …).

    - Difficult to get the main / condensed message out of the report.

    or

    Consultant reports

    - in PDF with eye wateringly colorful pages,

    - explaining how great their company has been for a century,

    - their experience of dealing with mighty clients like Google, Microsoft, Pentagon, and you should feel so lucky that they also kindly spared some of their valuable time for you mortals,

    - and a few valuable information successfully hidden on the 67th page of the document, followed by a hefty invoice to be paid immediately.

Obviously, neither of these is a good example of an attractive readable end result.

EFFECTIVE AUDIT REPORTS

The best format I found for audit reports is MS Power Point (converted into PDF at the formal submission time) with few colors and tables where needed, and without animation.

For Whom	Characteristic of Readers	Which Section
??	??	**Background** section may not be required (the management will not need an audit report to understand, say, which departments are involved in Credit card, their organization charts, the financials etc.),. **Audit Objective and Scope** section may not be necessary; I don't remember seeing any unusual audit objective, needing to read the scope to understand what is being covered. The above 2 sections have a big potential to distract / repel the readers and they would not survive until the real sections of the reports.
CEO, Board Audit Committee and Board	Limited Time Limited Attention span (10 minutes max) No direct execution responsibility	**Executive Summary** explains what is being highlighted in the report
CEO Direct Reports	Ultimate Accountability	**Table of Contents** contains high level summaries of all issues raised in the report.
Executioners	Real doers	**Detailed Findings** section is the main place the people will read to fix the issues

1. EXECUTIVE SUMMARY
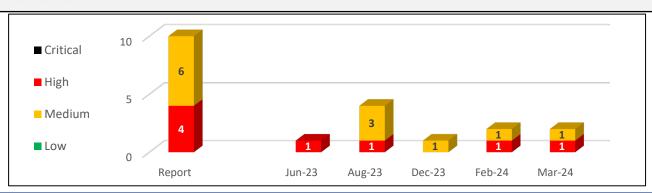
Entity Audited
Xxxxxx Xxxxxxxxx

Group Internal Audit's Overall Opinion on the Control Environment

3 - Needs Significant Improvement

Controls are not operating consistently and/or effectively, as relevant weaknesses in specific processes were noted. Weaknesses either individually or taken together have or could have a substantial impact on the related operations. Priority should be given by management to necessary remedial actions to enhance the control environment *(See the last slide for definitions).*

Key Themes Highlighted in the Report

This report contains the results of Yyy yyyyyyy audit review covering yyy yyyy yyyy. Yyy yyyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

The audit review highlighted that yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy ue to various deficiencies which are summarized below;

- Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy **yyy yyyy yyyy**.

- Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

- Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

- Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

- Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

- Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy..

In addition, Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

Audit identified **18 issues** in total (**6 High** and **12 Medium** risk rated), many of which have been addressed and closed (**2 High** and **6 Medium**) during the 2022-23 xxx reporting and outstanding issues are planned to be actioned by Mar 2024.

- Start the audit report with the **Executive Summary** explaining what is being highlighted in the report.

- The Executive summary should not be more than 1 slide. Any report, regardless of how many issues are in it, could be summarized in 1 slide. But this slide should be telling a coherent story.

- Start with a **impactful / strong / blunt** statement condensing the full message of the report, to grab the attention of the reader and lure them into reading the entire page, and even more; as long as the content / message deserves big attention.

    The audit review highlighted that the company will not be able to restore its services in a timely manner incase of even a minor disaster impacting a small portion of the data center due to various deficiencies which are summarized below;

    In its current format, the RCSA related activities, due to the approach followed, are no more than a bureaucratic burden, creating a significant amount of workload without generating any real / tangible benefit. Specifically; …

- Everybody who received the report will read this section (junior or senior).

- However, you are mainly talking to the CEO or Board members in this section, who:
    - have maximum 10 minutes to understand what the entire report is talking about
    - did not attend the close-out meeting
    - will not have any one to explain things to them verbally
    - are not familiar with (and probably not interested in) all details you have in the report
    - have great power and authority over the staff and could use this power based on your report
    - are looking for clues to know how they should respond (what to tell and to whom to tell)

- if you cause them to misunderstand, then things will be very complicated to restore.

TABLE OF CONTENTS

AUDIT REPORT: Table of Contents

- Table of Contents is the section high level summaries of all issues are given so that the relevant people can get a gist of what each issue is all about, along with which departments will need take part in resolution, an the timelines committed. The wording of this section should be short enough to keep the readers interested but comprehensive enough to let them understand.

- They will decide whether they want to / need to read this section based on how interesting they will find the executive summary.

- Summaries, as the name suggests, are supposed to explain what the issue is about in a couple of sentences without loosing the message.

- It doesn't have to be a copy / paste of some sentences from the original observation.

- In most cases, you would need to come up with different sentences than the ones in the original observation.

- Don't try to give all details of the observation in the summary.

- But also, try not to miss the real essence of the observation.

2. DETAILED OBSERVATIONS

2.1 Aaaaa Aaa Aaaaaaa and Aaaaa

2.1.4 Bbbb Bbb Bbbbbb	High

Observation

Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy **yyyy yyyy**. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

Secifically:

► Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy

► Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy

  ► Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy

  ► Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy

► Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy **yyyyyy** yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy

Internal Audit acknowledges that Xxxxxx xxxx xxxxx xxx xxxx xxx xxxxx xxx.

Risk

► Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

Management Action Plan

► Yyy yyyyyy department will yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

Action Owner: Xxxxxx Xxxx, Head of Xxxx Xxxxxx   **Target Date**: AUG 2023

► Yyy yyyyyy department has yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

► Yyy yyyyyy has already been yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy. Yyy yyyyyy yyy yyyy yyyy.

Action Owner: Xxxxxx Xxxx, Head of Xxxx Xxxxxx   **Target Date**: CLOSED

AUDIT REPORT: Language

- Do not focus on the individuals, but draw attention to process gaps allowing people to make mistakes.

- Unless there is a clear / almost proven fraud suspicion, **never blame** people.

- You will highlight many control gaps / risks which have never been exploited or materialized.

  - Use the word "**potentially**" when you talk about what could go wrong.

  - Give a clear message from the beginning that the risk rating of an issue is not about what has happened, but it is about what **could happen.**

- Audit reports should include minimum or **zero judgmental** opinion. They should be factual.

- Do not use phrases like "Internal audit believe, think, assume, feel, informed etc.". If really necessary, say "IA is of the opinion that…"

- Do not try to **soften** an issue with your wording. Do not try to **exaggerate** the issue with your wording.

- Do not start with '**this circular, this policy states that**…'. It is not a checklist audit, it should be a risk based audit. you can mention that there is also a regulation in relation to the issue you are raising in the observation.

  - Not complying with a policy can not be the only risk. Policy should be there to mitigate a risk and that risk should be explained in the risk section.

  - In the same way, not complying with a regulation can not be the only risk. Risk which the regulation is trying to mitigate should be mentioned along with the risk of getting regulatory attention and fines.

- If the auditee will come up with an **excuse / explanation / historic detail**, and if valid, incorporate this in the observation (GIA acknowledges that …), rather than allowing them to mention this in the management response or action.

- Think about questions any reader might ask and try to answer all within the observation.

AUDIT REPORT: Language

- No long stories, Very direct and to the point.

- Never start the observation with **bullet** points. Have a short paragraph explaining at a high level what the issue is about along with the risk / impact. 'Internal Audit identified the following deficiencies, in relation to the ….., which could potentially expose the Bank to significant financial, regulatory and reputational risks;

- Tables can be more readable than paragraphs. Charts can be more readable than tables. Use them where they are relevant.

- Story of the observation should be complete:

    • If we are talking about excessive access rights given to some staff, we should take one more step and check if this access was used for unauthorized activities. The result of this check should also be mentioned in the observation. Where this wasn't possible, then this should be mentioned and should become a management action.

    • Same thing should be done for potential for fraud cases.

- Risk/impact should be very obvious. If a reader can ask "so what" then it is not a well written observation. Via numbers where relevant, give a good idea about the impact.

- When you mention the exceptions identified, make sure you explain whether these were identified as part of a sample or via review of the entire portfolio. If it is a sample, clearly explain the sample size and the overall size of the portfolio the sample was taken from and if relevant, period the portfolio belongs to. Even if the exceptions are identified via an MIS, state the size of the overall portfolio.

- You don't need separate sections called Recommendation and Management Response. Only the Management Action Plan. This is another way of showing that this report is an output showing collaboration, not argument.

- Do not give the impression that management actions and the target dates are enforced by Internal Audit; but rather decided and owned by the auditee.

AUDIT REPORT:

- Internal Audit will never have enough resources to cover every area every year. That's why we have a responsibility to encourage all staff in the organization to identify and manage their own risks.

- One of the best ways of doing this is to recognize / acknowledge / reward formally.

- Where possible, as long as certain conditions are met, have a separate section to report the issues which were already identified (and being managed)by the auditee, Management Self Identified Issues.

- When the full maturity is reached; 2 overall ratings could b e given in the audit reports: Control Environment, Management Awareness.

- Audit Report Overall Ratings are used as staff KPIs in many organizations. If this is not done properly, this has the potential to KILL your relationship with your auditee.

- The reasonable / constructive KPIs could be defined as;

  • Timely resolution of highlighted issues (e.g. # of extensions / overdues)

  • Percentage of self identified issues

Robust Follow-up and Periodic Reporting

- Follow up and closure of audit issues is as important as the audits themselves.

- This is also important to maintain the profile of Internal Audit and the discipline around the audit issues.

- The open issues / actions to be reported to the owning business areas periodically (monthly) to prevent surprises at every level.

- Any target date extension request should not be treated lightly;

  - justifications should be provided by the highest authority in the owning area, and
  - extensions should be subject to approval from the CEO where relevant.

- High / Medium: 1st extension; Chief of the business area | 2nd extension; CEO

- Every issue / action should be subject to proper validation, like a mini audit, before full closure.

Be Pragmatic

- Appreciate the power / impact of your voice :: Utilize this for the benefit of the organization.

- Do not mechanize auditing. Hold and monitor the pulse of the organization.

- Keep the motivation and energy of the management for fixing issues up. Do not saturate their senses, but do not become invisible either.

- Every standard approach may not be applicable to every organization at all times. Take the maturity level of the organization into account.

- Appreciate the difference between what SHOULD be done and what COULD be done. Always push for the full solution, while appreciating milestone achievements

- Recognize what is happening in the organization, Change the annual plans / schedules accordingly.

- When to and how to say could be more important than what to say.

- Optics should be managed properly; how **you / your department / the organization / the management** look in front of others.

None of the above means you need to hide / ignore important things.

Your Audience

Direct Reports of the CEO

- These are not your rivals in the organization you issue reports against

- They are your partners to improve the control environment of the organization.

- If you give the impression that you are trying to expose them, you will not have a healthy relationship. And you will get resistance even for the easiest, most obvious issues you try to raise.

- Your success is not measured based on how many high risk issues you identified or how many good / bad audit reports you published; it is measured with what kind of changes you were able to trigger in the organization to make it better, more secure, more risk aware, and more controlled.

- And this could not be done without proper buy-in from your partners.

- Make sure that what ever you are highlighting / escalating to the higher levels, these are done after full alignment (not necessarily full agreement) with your partners.

Your Audience

Chief Executive Officer

- CEO is your main stakeholder and main receiver of your services.

- An Internal Audit Function can not be successful or can not have good profile in the organization despite the CEO.

- This can only happen with the support of CEO.

- Independence of Internal Audit does not mean that you don't need to have a good relationship with the CEO.

- Your independence from the CEO does not make you equal with him / her; but when things are done properly, it makes your function a Trusted Partner for the CEO and the management.

- When you are escalating anything to him, the CEO should trust that you have already aligned with all parties.

- Never share / escalate anything to the Board before aligning with the CEO.

Your Audience

Board Audit Committee:

- BAC members are not working for the organization. They are not familiar with the day to day activities.

- We also meet with them once every 2-3 months at best for a couple of hours.

- That's why communication with the BAC should be very accurate, to the point and succinct. This means there are a lot of opportunities to create misunderstanding which might cause a lot of unnecessary problems.

- They have only three expectations from you:

    1. you know what you are doing, are able to highlight the major risks impacting the organization.

    2. they are properly informed about what's happening in the organization, adequate for them to be able to talk about.

    3. and all known issues are being dealt with by the management with full alignment with Internal Audit.

- Time to time, make sure you take the senior management (CEO and / or his directs) to BAC sessions to demonstrate the alignment.

Conclusion

- Communication is important only when you have good things to communicate. Make sure you do the ground work without any gap.

- Communication happens in both ways. Show your stakeholder / audience that you listen, are open to hearing their views, ready to change your opinion when you see new facts and have no problem with accepting when you are wrong.

- Always have a good guess of what people want to hear. You don't have to say what they want to hear, but you can shape what you will say accordingly.

- The same thing can be / should be told to different people at different levels. For this, knowing your audience is the key.

- Tension and surprise are your enemy. Transparency and alignment are your best friends and most powerful weapons.
  - Tension gives the impression that you are not confident, not sure about what you are saying and vulnerable
  - When you are relaxed and cool, you give the impression that you have all the facts and are fully confident.

Show people that you:

- Always do your homework and know what you are talking about

- Be very open, direct, honest, even blunt in your comments without being rude and disrespectful

- Do not aim for or try to put people into difficult position in front of others

- You, the auditor, and you, the real person, can be 2 different people. The auditor you could / should be very thorough and direct, real person you could be very friendly.

- The most common and most justified complaint about auditors is "they do not listen". So, listen!

From Boring to Brilliant - How to Make

Your Audit Communication Engaging and Impactful

(Concurrent session)

Session Code

238166