Chartered Institute of Internal Auditors

acl™

Live Webinar

Delivering Impactful Internal Audit Reports for Maximum Effectiveness

Wednesday 13th February 2019

Speakers

Ben Kaye
European Senior IA Manager
Kellogg's

Nichol Deaddis
GRC Adoption Manager
ACL

Liz Sandwith
Chief Professional Practice Advisor
Chartered IIA

Larry Sawyer Quote

"Few sources of friction within the auditing department exceed that caused by the process of report writing. The most brilliant of analyses and the most productive of audit findings seem to be forgotten in the trauma of report writing"

Agenda

What do the standards say?

How can objectives and scope be incorporated?

Constructing and reporting audit findings - the 5C approach

Audit report formats

Options for grading rating an audit finding

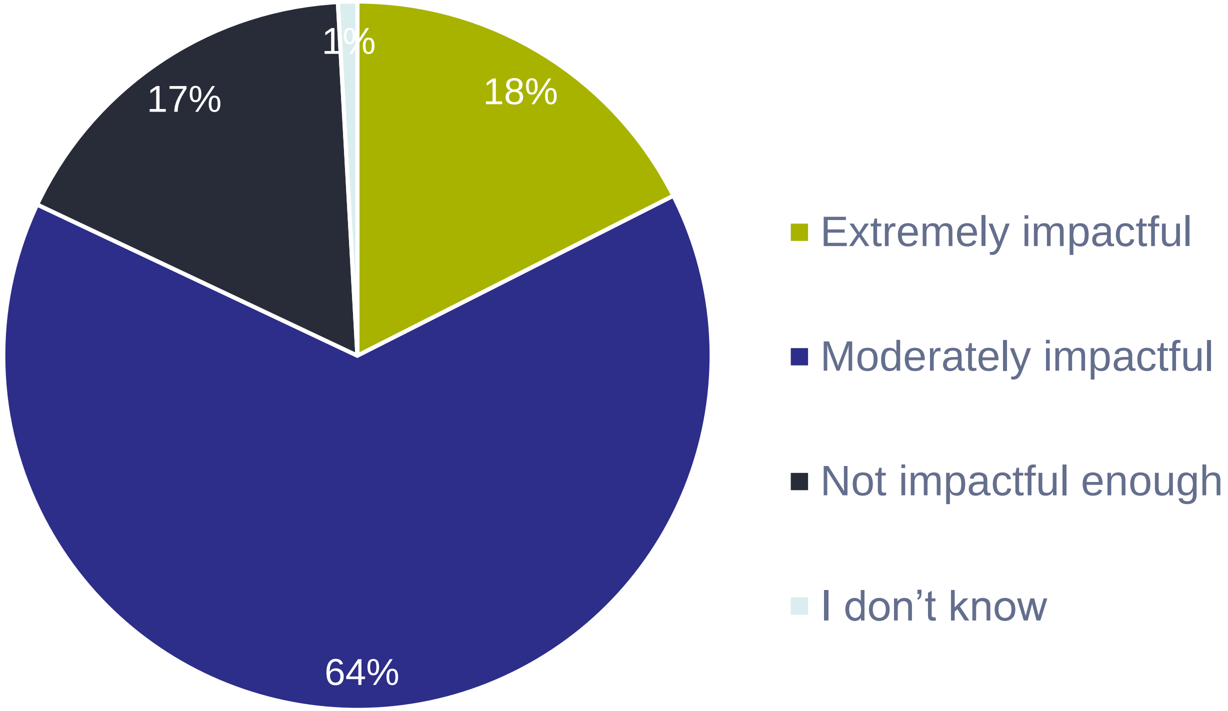
Offering an opinion in the report

Key Take Aways

Live Polling Question #1

How impactful would you say your internal audit reports are?

- Extremely impactful
- Moderately impactful
- Not impactful enough
- Negligible or zero impact
- I don’t know



WHAT DO THE STANDARDS SAY?

What do the standards say?

Implementation Guides (Recommended)

- IG2400 Communicating results
- IG2410 Criteria for communicating
- IG2420 Quality of communications
- IG2421 Errors and omissions
- IG2430 Use of 'conducted in conformance with the International Standards for the Professional Practice of Internal Auditing'
- IG2431 Engagement disclosure of nonconformance
- IG2440 Disseminating results
- IG2450 Overall opinion

Supplementation Guidance (Recommended)

- Audit reports: Communicating assurance engagement results

What do the standards say?

The IIA’s Integrated Professional Practices Framework (Mandatory) Performance Standard 2400 states: “Internal auditors must communicate the results of engagements.”

- Communications must include the engagement’s objectives, scope, and results
- Results must include applicable conclusions, as well as applicable recommendations and/or action plans
- Where appropriate, the internal auditors’ opinion should be provided
- Encouraged to acknowledge satisfactory performance in engagement communications
- Communication of the results of consulting engagements will vary in form and content
- Communications must be accurate, objective, clear, concise, constructive, complete and timely
- The chief audit executive must communicate results to the appropriate parties
- When an overall opinion is issued, it must take into account the strategies, objectives and risks of the organisation; and the expectations of senior management, the board and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant and useful information

The 7 dimensions of a report

The IIA's implementation guide 2420-1 Quality of Communications advises:

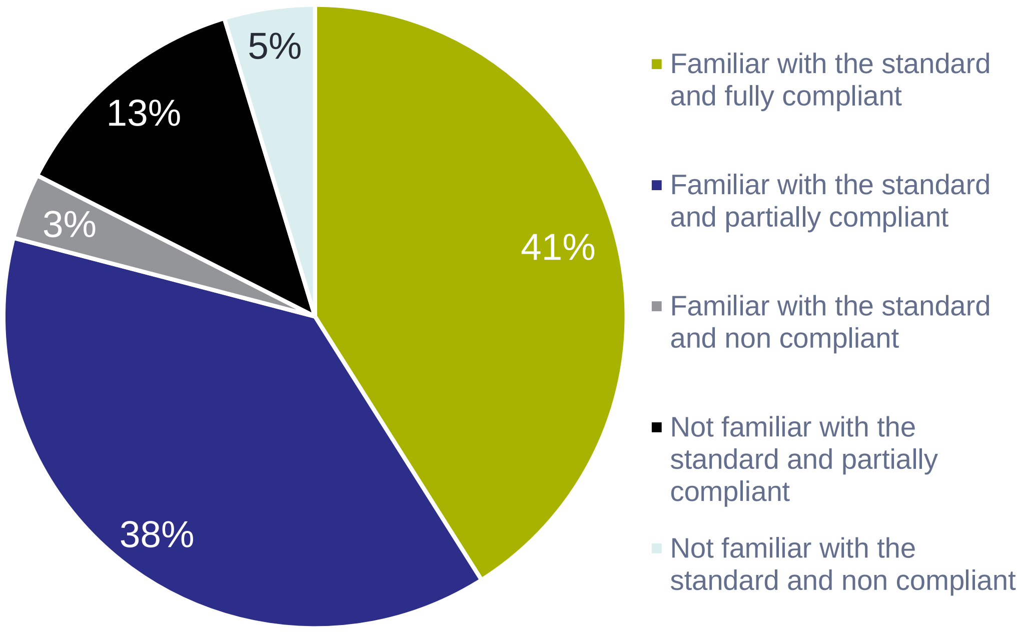
Communications must be:

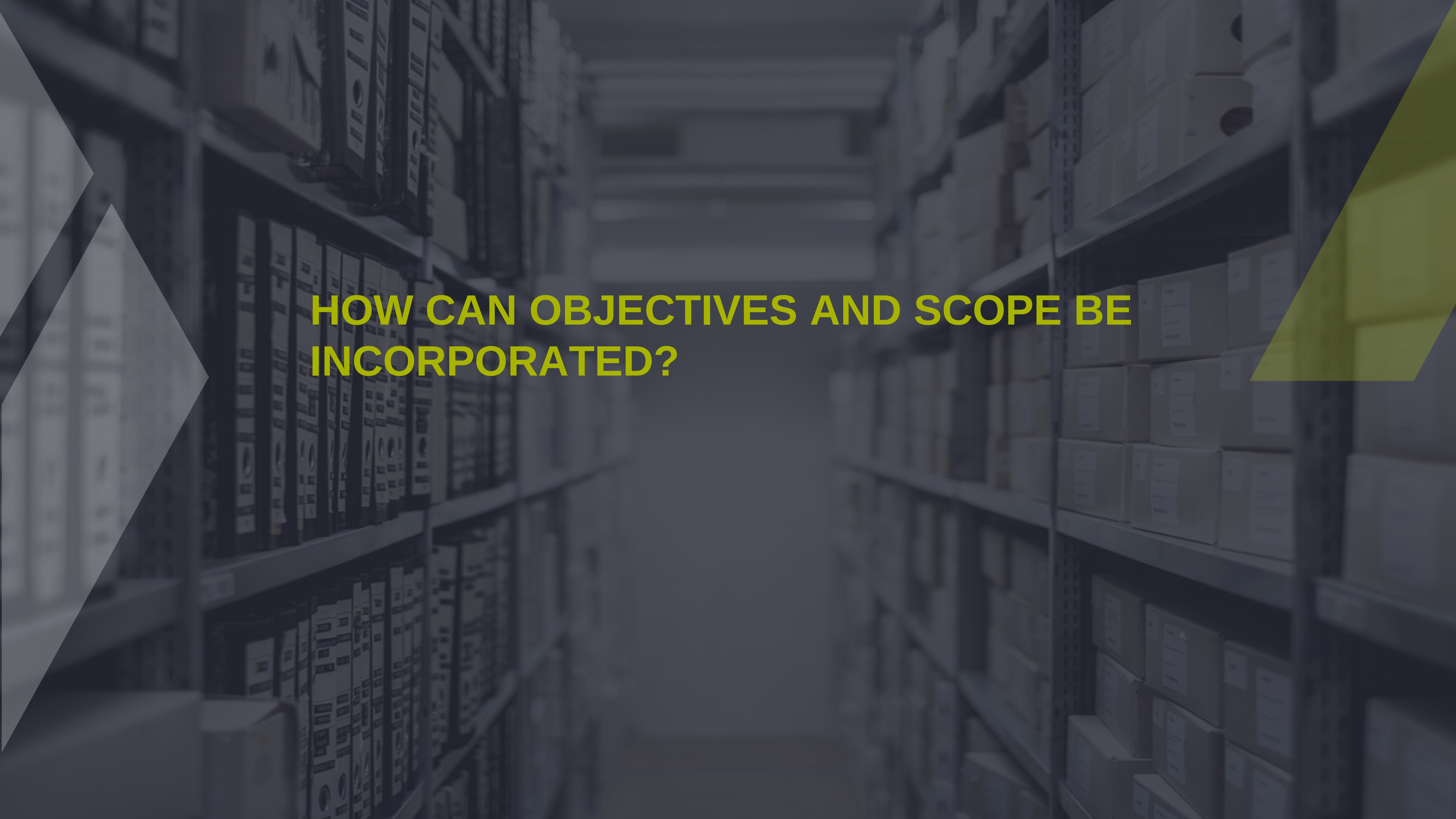
- Accurate
- Objective
- Clear
- Concise
- Constructive
- Complete
- And timely

Live Polling Question #2

How familiar with performance standard 2400 just discussed is your internal audit function and how compliant are you with it?

- Familiar with the standard and fully compliant
- Familiar with the standard and partially compliant
- Familiar with the standard and non compliant
- Not familiar with the standard and partially compliant
- Not familiar with the standard and non compliant





HOW CAN OBJECTIVES AND SCOPE BE INCORPORATED?

How can objectives and scope be incorporated?

The objectives and scope of the audit should be included in the audit's terms of reference / audit planning memorandum. That way they have been agreed and can then referred to / duplicated in the final internal audit report

ACRES is a useful tool for considering objectives.

- **A**ccomplishment of goals and objectives
- **C**ompliance with policies, plans, procedures, laws and regulations
- **R**eliability and integrity of information
- **E**conomical and efficient use of resources
- **S**afeguarding of assets

CONSTRUCTING AND REPORTING AUDIT FINDINGS - THE 5C APPROACH

Constructing and reporting audit findings - the 5C approach

Criteria

- Standards, measures, or expectations used in making an evaluation and/or verification of an observation (what should exist). E.g. policies & procedures (internal), laws and regulations (external) and industry best practice or professional guidance (best practice)

Condition

- Condition: Factual evidence identified during the course of the engagement (what does exist). Condition is the key issue the internal auditor considers, and it can be measurable or observable

Cause (Root Cause)

- Underlying reason for the difference between the criteria and condition (why the difference exists)

Consequence

- Risk or exposure encountered because the condition is not consistent with the criteria (the consequence of the difference). Consequence can be existing or potential.

Corrective Action

- Recommendations and / or Management Action Plans (“MAPs”), Agreed Remediation Plans (“ARPs” etc. These are agreed between the auditor and auditee for correcting conditions, and identifying the cause to prevent recurrence (or the creation of new conditions)

Constructing and reporting audit findings - the 5C approach

<table>
<tr><td rowspan="2">2</td><td>Scope Area:</td><td>Windows Security</td><td rowspan="2">Finding Rating: Moderate</td><td>Management Action Plan (“MAP”)</td></tr>
<tr><td>Finding Title:</td><td>Domain Account Policy Weaknesses</td><td>MAP Owner: John Smith, VP IT</td></tr>
<tr><td colspan="3">Finding / Observation Description</td><td>Risk</td><td>MAP Date: April 30, 2019</td></tr>
<tr><td colspan="3"><b><u>Criteria:</u></b>
In accordance with best practice, strong domain account policies should be configured to increase the security of the network.
<b><u>Condition:</u></b>
During the course of the audit, it was identified that:
• Password changes are only required every 90 days (leading practice is 30 to 60);
• The password history size is only 10 (leading practice is 22 or greater);
• The lockout threshold is set to five unsuccessful attempts (leading practice is three);
• The lockout duration is set to five minutes (leading practice is zero); and
• The reset lockout counter is set to five minutes (leading practice is 1440 minutes).
<b><u>Root Cause:</u></b>
Active Directory was not implemented and configured by a suitably qualified individual.</td><td><b><u>Consequence:</u></b>
Unauthorised access to data and network resources may occur.
<b>Impact:</b> High
<b>Likelihood:</b> Moderate</td><td><b><u>Corrective Action:</u></b>
Management will adjust the noted domain account policies to ensure that they are aligned with best practice. Where applicable, the requirements defined in the company’s ‘Access Control Procedure’ will be updated to reflect this.</td></tr>
</table>

AUDIT REPORT FORMATS

Audit Report Formats

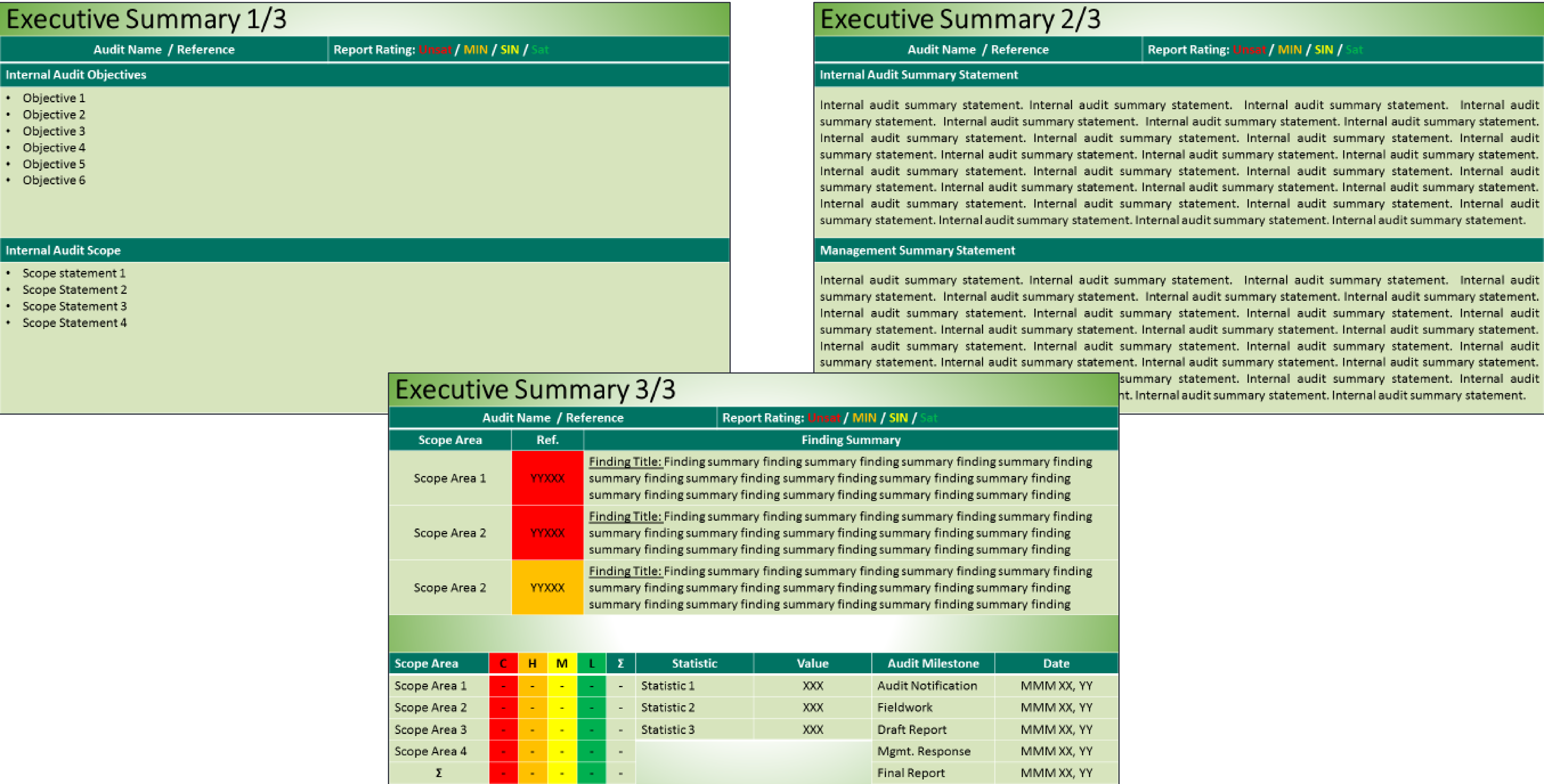
What does good look like?

- Executive summary - grab readers attention, target audience, clear headline, themes, overall rating
- Detailed observations - fact-based observations / findings, root cause analysis, articulate risk and impact, issue rating, recommendations / management action plans linked to root cause, pragmatic and specific

Top Tips:

- Write the report in one sitting don't stop and start; and
- Put it in your "draw" for 48 hours then read it again you will make changes!

Executive Summary - Example



Executive Summary 1/3

Audit Name / Reference	Report Rating: Unsat / MIN / SIN / Sat

Internal Audit Objectives

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5
- Objective 6

Internal Audit Scope

- Scope statement 1
- Scope Statement 2
- Scope Statement 3
- Scope Statement 4

Executive Summary 2/3

Audit Name / Reference	Report Rating: Unsat / MIN / SIN / Sat

Internal Audit Summary Statement

Internal audit summary statement. Internal audit summary statement.

Management Summary Statement

Internal audit summary statement. Internal audit summary statement.

summary statement. Internal audit summary statement. Internal audit

nt. Internal audit summary statement. Internal audit summary statement.

Executive Summary 3/3

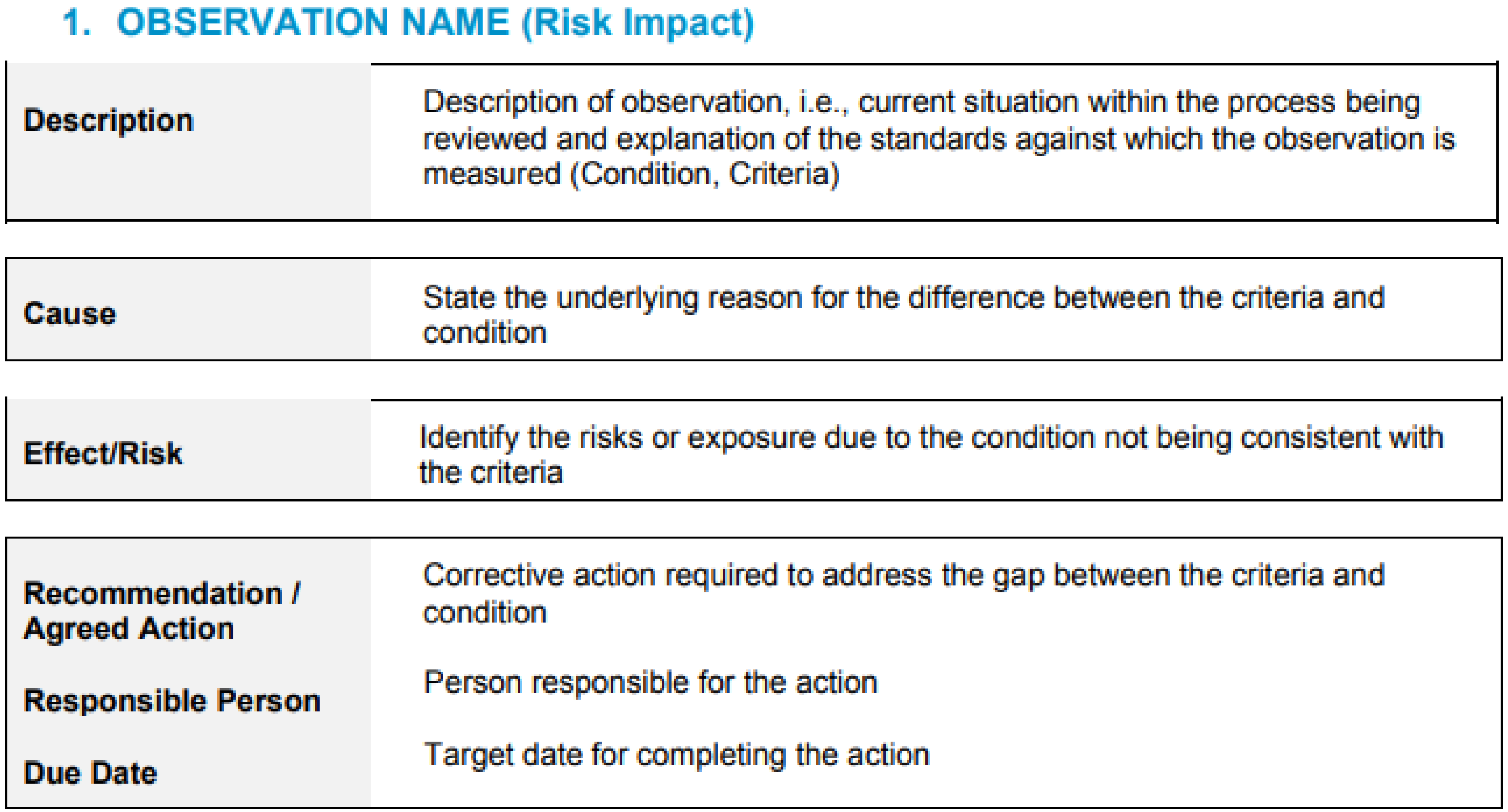
Audit Name / Reference	Report Rating: Unsat / MIN / SIN / Sat

Scope Area	Ref.	Finding Summary
Scope Area 1	YYXXX	Finding Title: Finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding
Scope Area 2	YYXXX	Finding Title: Finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding
Scope Area 2	YYXXX	Finding Title: Finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding summary finding

Scope Area	C	H	M	L	Σ	Statistic	Value	Audit Milestone	Date
Scope Area 1	-	-	-	-	-	Statistic 1	XXX	Audit Notification	MMM XX, YY
Scope Area 2	-	-	-	-	-	Statistic 2	XXX	Fieldwork	MMM XX, YY
Scope Area 3	-	-	-	-	-	Statistic 3	XXX	Draft Report	MMM XX, YY
Scope Area 4	-	-	-	-	-			Mgmt. Response	MMM XX, YY
Σ	-	-	-	-	-			Final Report	MMM XX, YY

Audit Report Formats

IIA Template From Supplemental Guidance Practice Guide



1. OBSERVATION NAME (Risk Impact)

Description	Description of observation, i.e., current situation within the process being reviewed and explanation of the standards against which the observation is measured (Condition, Criteria)
Cause	State the underlying reason for the difference between the criteria and condition
Effect/Risk	Identify the risks or exposure due to the condition not being consistent with the criteria
Recommendation / Agreed Action	Corrective action required to address the gap between the criteria and condition
Responsible Person	Person responsible for the action
Due Date	Target date for completing the action

Audit Report Formats

When preparing a report you should ask yourself the following questions:

- Who will receive this?
- Does it contain significant findings?
- Are the findings fully supported by sufficient, trustworthy and relevant information?
- What level of discussion is likely to be needed to reach agreement?
- What speed of communication is necessary?

Audit Report Formats

The Reporting Environment

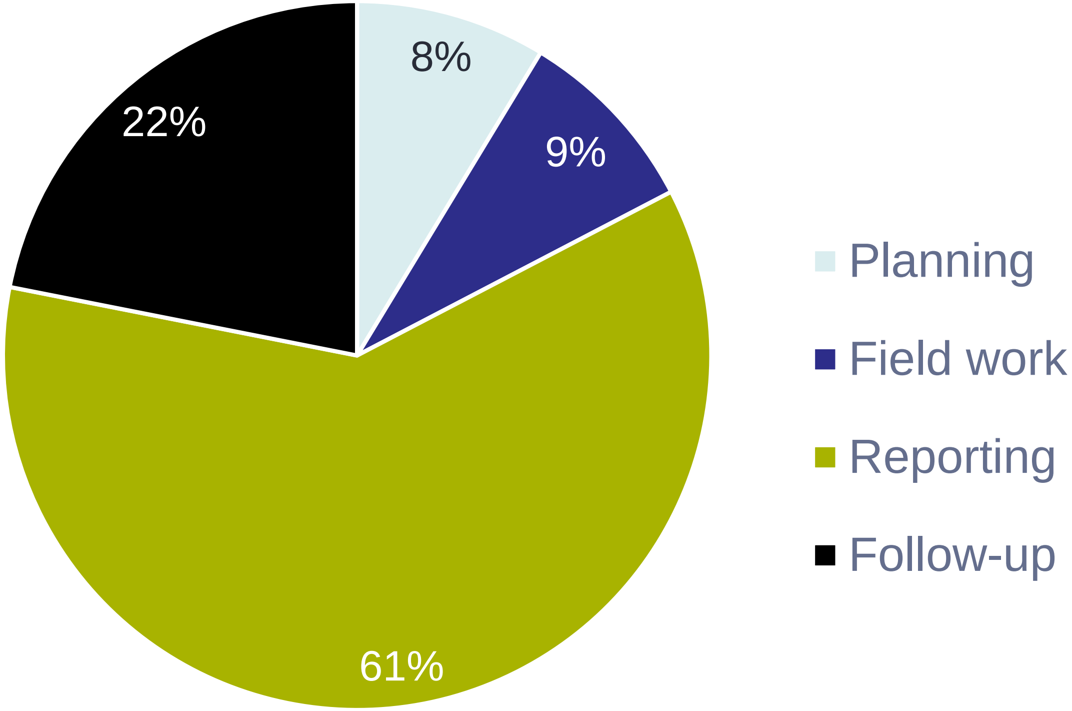
A good environment will be fostered where:

- The presentation of findings is tailored to the needs of the recipients
- Findings are presented in a simple, accurate and factual way
- There has been on-going and effective communication with the auditee throughout the process
- Recommendations / management action plans are SMART, in line with business risks and objectives, cost-effective and solve the problem
- And reports are issued promptly!

Live Polling Question #3

Which stage of the internal audit process causes the most friction with stakeholders and / or the most challenge for auditors?

- Planning
- Fieldwork
- Reporting
- Follow-up



Audit Report Formats

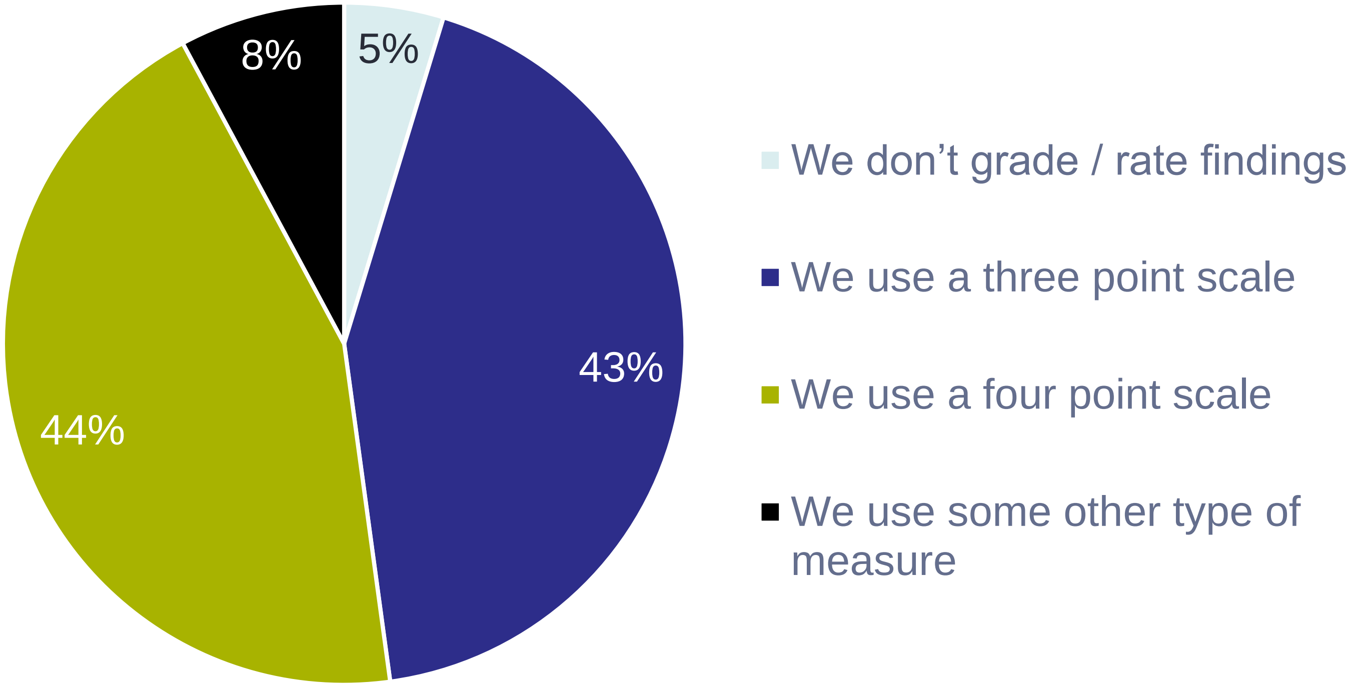
- PowerPoint vs Word
- Assurance vs advisory
- Video reports
- Executive summary
- Graphics and visuals (analytics / analysis)
- Finding on a page
- Conclusions and recommendations / management action plans
- Distribution of findings by grade / rating and scope area
- Objectives, scope and results
- Accurate, objective, clear, concise, constructive, complete and timely

OPTIONS FOR GRADING / RATING AN AUDIT FINDING

Live Polling Question #4

How do you grade / rate your individual findings?

- We don't grade / rate findings
- We use a three point scale
- We use a four point scale
- We use some other type of measure



Finding Rating Example (Impact x Likelihood)

Impact	Non Financial Indicators				Financial Indicator
	Health & Safety	Business Continuity	Compliance	Reputation	$
High	Fatality or permanent personal injury or sickness.	Disruption to critical business process and / or system.	Critical non compliance with law, code of ethics, corporate policy or process.	Significant brand / market share / share price impact due to international media coverage.	> US$ 1 million
Moderate	Long term major mobility injury / sickness.	Long / medium disruption to significant business process and / or system.	Significant non compliance with law, code of ethics, corporate policy or process.	Brand / market share / share price impact due to regional / national media coverage.	US$ 50k < x < US$ 1m
Low	Temporary minor injury or sickness.	Medium / short disruption to significant business process and / or system.	Minor non compliance with law, code of ethics, corporate policy or process.	Minor brand / market share / share price impact due to media coverage.	< US$ 50k

Likelihood	Interpretation of Occurrence	Time	
		Next 12 Months	Occurrence
High	Likely	50% – 100%	Every 2 years or shorter
Moderate	Possible	26% – 50%	Every 2 to 5 years
Low	Unlikely	0% – 25%	Every 5 years or longer

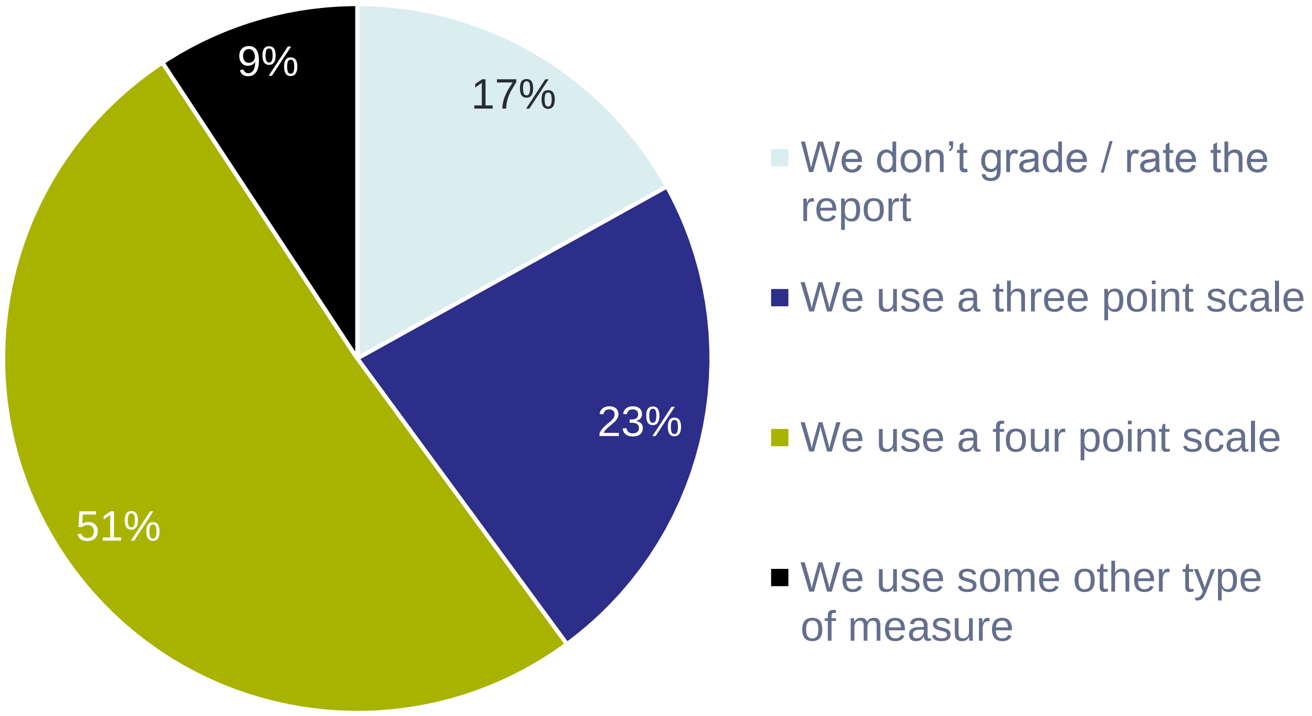
Likelihood	Impact		
	Low Impact	Moderate Impact	High Impact
High Likelihood	Moderate Risk	High Risk	Critical Risk
Moderate Likelihood	Low Risk	Moderate Risk	High Risk
Low Likelihood	Low Risk	Low Risk	Moderate Risk

OFFERING AN OPINION IN THE REPORT

Live Polling Question #5

How do you grade / rate your audit report?

- We don’t grade / rate the report
- We use a three point scale
- We use a four point scale
- We use some other type of measure



Offering an opinion in the report

- Engagement reports are unlikely to provide observations only. They usually include opinions on some or all aspects of the area reviewed
- There are two ways to express an internal audit opinion, by using positive or negative assurance statements
- In providing positive (or reasonable) assurance, the internal auditor takes a definite position
- Negative (or limited) opinions use negative forms of expression
- An opinion may address the whole scope of or may be limited to specific aspects of the engagement

Offering an opinion in the report

- Self declaration of control weaknesses, lack of efficiency / effectiveness pre-audit
- Audit report grade / rating
- Overall assessment of the control environment
- Risk culture assessment
- Assessment of auditee's receptiveness to audit process, findings and management action plans
- Each audit report will contribute towards the annual opinion provided to the Audit Committee by the Chief Audit Executive

Report Rating Example

Report Grade	Description	
Unsatisfactory	• Total non compliance • Appropriate authority levels not in place • Fundamental internal controls are not being performed	• No monitoring of performance • A critical level of risk is present • Typical profile of findings is 'Grade 4‘ - Critical
Significant Improvement Needed	• Substantial non compliance • Some authority levels in place • Most fundamental internal controls are not being performed	• Poor monitoring of performance • A significant level of risk is present • Typical profile of findings is 'Grade 3‘ - High
Some Improvement Needed	• Some compliance • Most authority levels in place • Some fundamental internal controls are being performed	• Limited monitoring of performance • A moderate level of risk is present • Typical profile of findings is 'Grade 2‘ - Moderate
Satisfactory	• Substantial compliance • Appropriate authority levels in place • Fundamental internal controls are being performed	• Adequate monitoring of performance • A minor level of risk is present • Typical profile of findings is 'Grade 1‘ - Low

Offering an opinion in the report

An alternative approach…

Objective	Measure	Non Existent	Initial	Repeatable	Defined Process	Managed	Optimised
Controls Maturity	TBD	🟦	🟦	🟦			
Management Culture	TBD	🟦	🟦	🟦	🟦		
Policy Maturity	TBD	🟦	🟦				
Information and Comms	TBD	🟦	🟦	🟦	🟦	🟦	
Risk Assessment	TBD	🟦	🟦				
Commitment To Audit	TBD	🟦					
Prior Audit Actions	TBD	🟦					

Key Take Aways...

Key Take – Aways...

- The audit report is the culmination of the audit assignment. It is the means by which internal audit communicates findings to management. Internal audit reports must be based on facts derived from our evaluation and testing of the area under review, and be presented in such a way that they convince management to act on our recommendations / observations and / or management action plans
- Connect the dots – what is the view across the business, learning good pratices from other areas of the business, or other assurance providers, assurance mapping / alignment etc.
- Visualisation – a picture (or video) paints a thousand words, easy to read, understand and digest!
- External support – establish models, benchmark, maturity assessments from co-sourced partners, networking with IA peers, consulting publications etc.

Chartered Institute of Internal Auditors

acl™

Thank you for your attention!

Questions?

Feel free to reach out to:

liz.sandwith@iia.org.uk

ben@benkaye.net

Nichol_Deaddis@acl.com

Key Take – Aways...

- Practice Guide – Audit Reports Communicating Assurance Engagement Results
  https://www.iia.org.uk/media/1688799/audit-reports.pdf
- Practice Guide – Formulating and Expressing Internal Audit Opinions
  https://www.iia.org.uk/media/97442/Formulating%20and%20Expressing%20Internal%20Audit%20Opinions.pdf