



FP Consultants

SOX – Current Trends and Developments

Andrew Olding, FCCA

Your Premier Corporate Training Provider In Asia
www.fp-consultants.com

FP Consultants YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

Agenda

- Initial approaches under SOX 404 and AS 2
- Costs and resources required, criticisms and reactions
- SEC and PCAOB findings and responses
- How AS 5 should help – (Scotts)
- Reduction in testing – (Avid)
- Potential to reduce audit fees
- Deloitte survey – (Time Warner)
- Self-assessments / walk-through reviews
- Risk assessment review / fraud considerations
- Automation potential – SAP / Articles
- Recent developments – US and Singapore
- Practical examples / exercises



FP Consultants YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

2

So what exactly is SOX?

It is not a baseball team....



And it is definitely not a movie....



The Sarbanes-Oxley Act of 2002

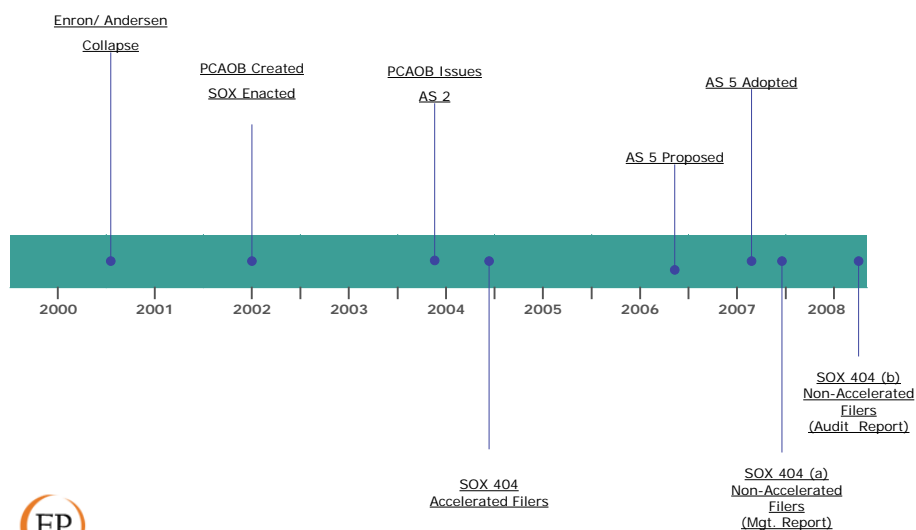
"To protect investors in US securities by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes."



YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

3

SOX Timeline



YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

4

Initial approaches under SOX and AS 2

- Section 404 is made up of only 180 words!
- Creation of the Public Company Accounting Oversight Board (PCAOB)
- Public companies must evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting each fiscal year
- Independent auditors "attest" (i.e., agree or qualify) to such disclosure
- CEO and CFO must publicly certify financial reports
- Auditor independence, including outright bans on certain types of work for audit clients
- Companies must have fully independent audit committees that oversee the relationship between the company and its auditor
- Ban on most personal loans to any executive officer or director
- Accelerated reporting of insider trading
- Enhanced criminal and civil penalties for violations of securities law, including the willful misstatement of financial statements
- Protections for corporate whistleblowers



Initial approaches under SOX and AS 2

- Little guidance issued by PCAOB or SEC
- Audit firms unwilling (unable) to help set scope and tone
- Auditor attestation/qualified opinions weighed heavily on companies
- Companies tended to overreact to 404
- Risk was not adequately assessed or addressed
- Scopes were set widely
- Attempts made to cover every major account, policy, process
- New controls often established to ensure coverage
- Companies underestimated time required for documentation and testing



Costs and resources required

- Cost of Section 404 Compliance
 - Year 1: \$3.14 million per US company (2004 average)
 - Mainly for consulting, software, and fees paid to external auditors
 - Internal resources exceeded these costs, in some instances
 - Highest cost of compliance was in the first year
 - External auditors “encouraged” to rely on the work of a company's internal auditors – but are instructed to obtain a “meaningful portion” of evidence through their own testing
- Per the PCAOB, costs were related to:
 - The adequacy of the company's IC in previous years
 - Whether the company has international operations
 - The complexity of the company's corporate structure and business operations



Criticisms and reactions

- Legislation was rushed through Congress
- Lack of guidance on 404
- High compliance costs
- Diversion of internal resources
- Concerns over personal liability
- Stifles entrepreneurs / growth
- Redirects talent to private companies
- Companies delaying IPO's / going private
- Foreign issuers delisting / listing on non-US exchanges
- Does not provide the assurances investors hoped for (Lehman, Societe Generale, Northern Rock)



SEC / PCAOB Findings and responses

- Audit firm inspections found:
 - Audits of ICFR and financial statements were not integrated
 - Top-down, risk based approaches were not followed
 - Unnecessary testing performed
 - Neglected to use the work of others
 - 404 reviews not scaled to the company
- Companies complained of high compliance costs – internal and external costs



FP Consultants

YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

9

How AS 5 should help

- Risk Assessment and Scoping
- Integrated Audit Approach and Methods
- Entity-Level Controls
- IT Controls
- Control Self Assessment / Walkthrough Reviews
- Multi-Location Scoping



FP Consultants

YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

10

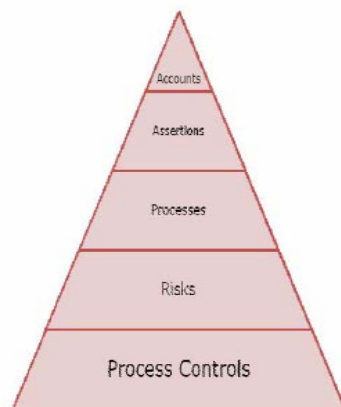
Major differences between AS2 and AS5

1	Management ICFR assessment reviewed	Deemed unnecessary and inefficient
2	Material classes of transactions and processes required to be reviewed without a clear definition – resulting in more controls	Waived assessment of processes or transaction classes without material impact
3	Annual assessment of all significant accounts	Auditors to use past experience and the nature of an account when determining what needs to be tested
4	No requirements to assess risk based on size and complexity	Auditors should use a risk based approach and scale reviews accordingly.
5	Covered all locations where any significant accounts or processes existed	Eliminated locations or divisions which individually or when aggregated did not present a reasonable possibility of a material misstatement
6	Required auditors to obtain principal evidence for applicable ICFR items	Allows auditors to rely on the independent work of others
7	Required auditors to perform all walk-through reviews independently	Allows auditors to rely on walk-through reviews performed by others as long as the auditor provides supervision
8	Assessment of ELC would not provide sufficient evidence of ICFR effectiveness	If ELC sufficiently addresses the risk, no further testing is required to assess that risk



YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

Old AS2



New AS5



Strategy: Shift focus from bottom-up to top-down



YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

Scott's

New definition of significant deficiency

- SEC revised the definition of Significant Deficiency to:
 - A deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the registrant's financial reporting.
 - No longer includes reference to likelihood of occurrence or magnitude of misstatement
- Deficiencies evaluated using qualitative and quantitative measures:
 - Reasonable Possibility exists that the company's controls will fail to prevent or detect a misstatement of an account balance or disclosure; and
 - the magnitude of the potential misstatement resulting from the deficiency or deficiencies.
 - Not a comparison to a benchmark, but in relation to financial statement amount; dollars and volume of transactions exposed to the deficiency;
 - Qualitative
 - Risk Factors - Nature of accounts/disclosures; susceptibility to fraud; subjectivity, complexity, judgment in calculations; transaction volume and amounts; interaction of controls and deficiencies
 - Any mitigation provided by compensating controls



RISK ASSESSMENT

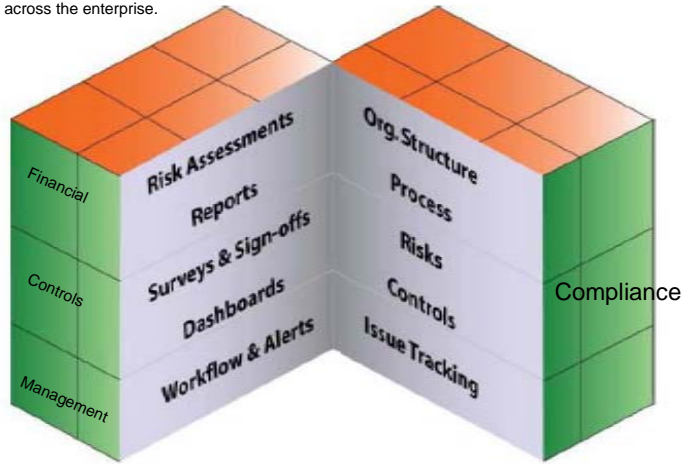
- Risk assessment describes the way management identifies, summarizes, and controls the organization's key risks. The following areas describe how risk assessment is organized and formalized in an organization:
 - Management assesses the likelihood and impact of risks (e.g., analyze, plan, and perform the assessment; check and act on the risk)
 - Meetings with the board, operating group control, legal, and IT are held to discuss the implications and impact of changes in the business
 - These controls acknowledge that effective risk assessments--including assessments of financial reporting risk--reduce the risk of material misstatements in the organization's financial statements



Monitoring - A Way to Keep Score

Look for precise controls – monitoring and risk assessment

- Identify, design and assess entity level controls.
- Document and test entity level controls.
- Identify and remediate gaps.
- Push monitoring and risk assessment down through the organization.
- Keep score consistently across the enterprise.



• Assess risk at the significant account level – not the account balance level

Significance	Extreme	Significant 5	Major 10	High 15	Severe 20	Severe 25
	Very High	Moderate 4	Significant 8	Major 12	High 16	Severe 20
	Medium	Low 3	Moderate 6	Significant 9	Major 12	High 15
	Low	Trivial 2	Low 4	Moderate 6	Significant 8	Major 10
	Negligible	Trivial 1	Trivial 2	Low 3	Moderate 4	Significant 5
		Rare	Unlikely	Moderate	Likely	Almost Certain
		Likelihood				

LEVELS OF RISK

Severe Risk: Must be managed by senior management with a detailed plan.

High Risk: Detailed research and management planning required at senior levels.

Major Risk: Senior management attention is needed.

Significant Risk: Management responsibility must be specified.

Moderate Risk: Manage by specific monitoring or response procedures.

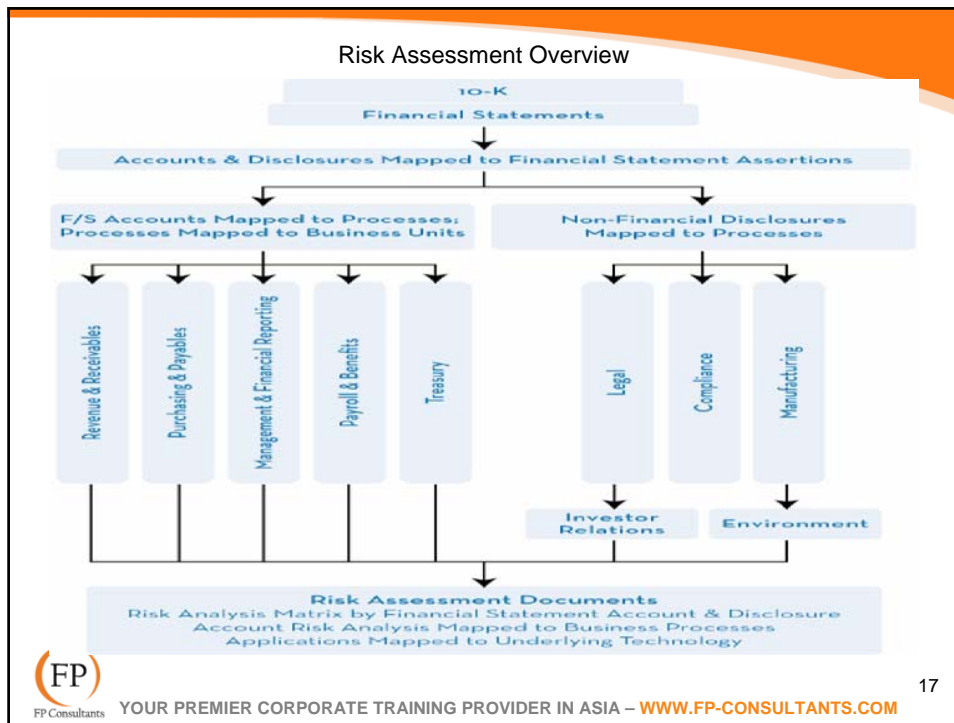
Low Risk: Manage by routine procedures.

Trivial Risk: Unlikely to need specific application of resources.

LEVELS OF SIGNIFICANCE

- Extreme:** The consequences would threaten the survival of not only the process, but also the department, possibly causing major problems for clients and for a large part of the business.
- Very High:** The consequences would threaten the survival of continued effective function of the process or project, and require top level management intervention.
- Medium:** The consequences would not threaten the process, but would mean that the process could be subject to significant review or changed ways of operating.
- Low:** The consequences would threaten the efficiency or effectiveness of some aspect of the process, but would be dealt with internally.
- Negligible:** The consequences are dealt with by routine operations.





17

Risk Assessment Approaches

Management should evaluate the design of controls:

- Top-down, risk-based approach focuses on the controls necessary to prevent or detect material misstatements
- This approach presents the opportunity to focus the company and its auditors on what is most important to the company and its investors
- No requirement to identify all internal controls in a process
- Management’s evaluation must have “reasonable support.”
- Evidence and methodology may take a variety of forms
- Nature and extent will depend upon level of complexity of control, judgment involved with control and risk of misstatement
- Use self-assessments in lower risk areas
- Reliance on entity-level controls
- Increase the use of monitoring of activities through automation
- Walkthroughs performed by management may be used to update narratives perform application testing and provide evidence for auditors

FP
 FP Consultants YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

18

Common Period-End Risks

- Improper or incorrect application of GAAP risk
- Improper or incorrect valuation risk
- Cut off error – accidental
- Cut off error – intentional - unauthorized entries
- Incorrect system calculation
- Unauthorized change to formulae or standing data
- Incomplete or missing transactions
- Invalid transactions – accidental
- Invalid transactions – intentional
- Incomplete description of situation or event
- Unaware of disclosure item
- Incorrect interpretation of regulation

Identify all risks to period-end reporting



YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

Boeing⁹

Entity Level Controls

- AS5 gives the following examples of entity-level controls:
 - Controls within the control environment, including management culture, assignment of authority and responsibility, consistent policies and procedures, and company-wide programs, such as codes of conduct and fraud prevention, that apply to all locations and business units.
 - Senior management's risk assessment processes.
 - Centralized processing and controls, including shared services.
 - Controls to monitor operating results – budget reviews
 - Controls to monitor other controls, including activities of the internal audit function, audit committee, and self-assessment programs.
 - The organization's period-end financial reporting process.
 - Board-approved policies that address significant business control and risk management practices.



YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

20

Entity Level Controls

Three Broad Categories

AS 5 describes three broad categories of entity-level controls, which vary in nature and precision:

- **Some have an important but indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis.**
- For example: The general operating environment, policies and IT controls
- These controls might affect the other controls the auditor selects for testing and the nature, timing, and extent of procedures the auditor performs on other controls.
- **Some monitor the effectiveness of other controls.**
- Such controls might be designed to identify possible breakdowns in lower level controls, but not at a level of precision that would, by themselves, sufficiently address the assessed risk that misstatements to a relevant assertion will be prevented or detected on a timely basis.
- These controls, when operating effectively, might allow the auditor to reduce the testing of other controls. For example, close process, budget reviews / variance analysis
- **Some might be designed to operate at a level of precision that would adequately prevent or detect on a timely basis misstatements to one or more relevant assertions.**
- If an entity-level control sufficiently addresses the assessed risk of misstatement, the auditor need not test additional controls relating to that risk. For example, ERP access controls



Fraud Risks

Risk Assessment

- Assessment of fraud risk and anti-fraud controls is critical to ensuring an effective top-down approach.
- A discussion of fraud risk and fraud-risk controls was placed at the front of AS5 to emphasize the importance of assessing fraud risk throughout the audit process.
- Even the strongest internal control frameworks cannot provide absolute assurance that fraud will be prevented or detected.
- However, a strong control environment will help to reduce instances of fraud.
- The focus on fraud controls in the internal control audit should enhance investor protection.
- Management fraud is an area of higher risk and the auditor should focus more attention on this area.



Fraud - Face the Potential

Where are the biggest risks of fraudulent financial reporting

- Use common fraud risk scenarios
- Use statistics on restatements
- Use data on reported deficiencies
- Assess inherent, residual risk and related controls
- Identify all plausible fraud scenarios then describe controls in place to mitigate risk



Example of Scenarios to Consider



Walkthroughs - *Key Changes:*

- Walkthroughs only required for significant processes, as opposed to each major class of transactions
- Not required to be performed by an auditor.
- Should be able to reduce the number of walkthroughs.
- Allow auditors to use management to perform walkthroughs.
- Auditors can now focus on the objectives and not the mechanics of the walkthrough.
- Less work will be needed in testing the design of controls, as a sufficient evaluation of design is done during the walkthrough.



Use of the Work of Others - *Key Changes:*

- Auditors are able to use the work of others to obtain evidence on the design and operating effectiveness of controls. Others are defined as:
 - Sufficiently competent and objective company personnel
 - Internal auditors
 - Third parties working under the direction of management or the audit committee
 - AS5 eliminates the principal evidence provision.
 - Now, frameworks for the use of other's work are the same for audit of internal control and the audit of financial statements.



Communication and Coordination is Key

- AS 5 opens the door for many improvements and allows management to focus on what is most important.
- The key to success is a high level of communication and coordination with the client and their auditors.
- Evaluating entity level controls to identify monitoring controls that can reduce or eliminate testing at the transaction level.
- Identification of areas where the auditors are relying on management's work.
- Identification of ways to provide better evidence and perform additional work that can be relied on by the auditors.



FP Consultants

YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

Deloitte

27

Automation potential

- Centralized management of policies and compliance initiatives
- Moving away from spreadsheets
- Integrating automated controls into ERP systems – three-way PO matching process, credit limit reviews, slow moving inventories
- Segregation of duties assessments
- Building effective monitoring controls (CCM) – management dashboards to highlight exceptions, require reviews & approvals



FP Consultants

YOUR PREMIER CORPORATE TRAINING PROVIDER IN ASIA – WWW.FP-CONSULTANTS.COM

SAP/CW

28

Board Proposes New Auditing Standards Related to the Auditor's Assessment of and Responses to Risk

Washington, DC, October 21, 2008 – The Public Company Accounting Oversight Board voted today to propose for public comment a suite of seven new auditing standards related to the auditor's assessment of and responses to risk and related conforming amendments. The proposed standards would supersede the Board's interim auditing standards related to audit risk and materiality, audit planning and supervision, consideration of internal control in an audit of financial statements, audit evidence, and performing tests of accounts and disclosures before year end.



Overview of the Proposed Standards

The proposed risk assessment standards are as follows:

Audit Risk in an Audit of Financial Statements. This proposed standard describes the components of audit risk and the auditor's responsibilities for reducing audit risk to an appropriately low level in order to obtain reasonable assurance in an audit of financial statements.

Audit Planning and Supervision. This proposed standard describes the auditor's responsibilities for planning the audit, including assessing matters that are important to the audit, and establishing an appropriate audit strategy and audit plan. The proposed standard also describes the responsibilities of the engagement partner and other engagement team members for supervising and reviewing the work of the engagement team.

Identifying and Assessing Risks of Material Misstatement. This proposed standard describes the auditor's responsibilities for identifying and assessing risks of material misstatement. The risk assessment process discussed in the proposed standard includes information-gathering procedures to identify risks (e.g., obtaining an understanding of the company, its environment, and its internal control) and analysis of the identified risks.



- *The Auditor's Responses to the Risks of Material Misstatement.* This proposed standard sets forth the auditor's responsibilities for responding to the risks of material misstatement in the general conduct of the audit and specific audit procedures.
- *Evaluating Audit Results.* This proposed standard describes the auditor's responsibilities regarding the process of evaluating the results of the audit in order to form the opinion(s) to be presented in the auditor's report. This process includes evaluating uncorrected misstatements and control deficiencies identified during the audit.
- *Consideration of Materiality in Planning and Performing an Audit.* This proposed standard sets forth the auditor's responsibilities for applying the concept of materiality, as described by the federal securities laws, in planning the audit and determining the scope of the audit procedures.
- *Audit Evidence.* This proposed standard sets forth the auditor's responsibilities regarding designing and applying audit procedures to obtain sufficient appropriate evidence to support the opinion(s) in the auditor's report. In particular, it discusses the principles for determining the sufficiency and appropriateness of audit evidence.



Improvements to Audits

The Board believes that the proposed standards, if adopted, would result in improvements to audits of issuers, such as the following:

The proposed standards would update the existing requirements to take account of the improved risk-based audit methodologies currently in use by some auditors.

The proposed standards should enhance integration of the audit of the financial statements with the audit of internal control over financial reporting, resulting in more effective audits. Auditing Standard No. 5 describes a risk-based audit of internal control over financial reporting that should be fully integrated with the audit of financial statements. The proposed standards describe the auditor's responsibilities for assessing risk, responding to risk, and evaluating audit results in the context of an integrated audit of financial statements and internal control over financial reporting, which should help auditors better understand how certain procedures required by Auditing Standard No. 5 can be integrated with financial statement audit procedures.

The proposed standards would integrate the auditor's current responsibilities for considering fraud during the audit. This integration would emphasize that consideration of fraud is a central part of the audit process and should prompt auditors to make a more thoughtful and thorough assessment of fraud risks and develop appropriate audit responses.



PCAOB, Singapore Agree on Cooperation

- PCAOB has reached a reciprocal regulation agreement with the Accounting & Corporate Regulatory Authority in Singapore (Apr 2008)
- The PCAOB has 850 non-U.S. audit firms from 86 different countries on its registration rolls, including 20 located in Singapore
- The PCAOB does not assess foreign firms' compliance with applicable local standards and will not assess compliance with Singaporean audit standards
- The PCAOB will monitor audit firms in the U.S. doing business in Singapore, and ACRA will monitor Singapore firms registered to audit public companies listed on U.S. exchanges



Conclusions:

- Use a top-down, risk-based approach.
- Implement a solid risk assessment methodology
- Look for fraud potential.
- Emphasize entity level controls.
- Emphasize the use of internal audit to reduce risk on high risk areas.
- Implement self-assessment programs, particularly for lower risk areas.
- Establish frequent meetings with external auditor.
- Develop a “challenge the process” mentality.
- Link all audit efforts (External and Internal).
- Reduce number of controls to be tested.
- Understand the benefits / requirements before implementing technical tools.
- Anticipate the hardest problems and toughest judgment calls.



Conclusions:

- Develop a Change Management Strategy / Mentality:
 - Determine areas where management testing is relied on by external auditors and areas which should not need to be relied on at all - and understand why
 - Low risk – External auditor should not look at these areas at all. These are opportunities for greatly reduced testing or self assessment.
 - High risk – External auditor may retest these areas and put limited reliance on management's testing. Explore ways management can address these areas by increasing entity level controls.
- Identify the types of issues:
 - Which ones can be addressed without the concurrence of external auditors?
 - Which ones require the concurrence of external auditors?
 - Get buy-in from the external auditors on the approach for these issues.

