Material weakness and significant deficiency remediation

January 30, 2024

Your speakers

Ryan Pierson
Principal, Technology Risk Consulting

Peoria, IL

Ryan.Pierson@rsmus.com

Eliot Mitchell
Partner, Business Risk Consulting

McLean, VA

Eliot.Mitchell@rsmus.com

Bob Herman
Managing Director, ERP Risk and Automation Services

Charlotte, NC

Bob.Herman@rsmus.com

Agenda

Learning objectives

- Learn about the typical symptoms and root causes for material weaknesses
- Learn about misconceptions for remediating material weaknesses
- Learn about the impacts of a material weakness on a business
- Learn about solutions for remediating material weaknesses with precision and efficiency

Common causes of weakened control environments

Significant deficiencies and material weaknesses are driven by breakdowns within one or several of the **people, process, technology, and data** supporting an organization's control environment.

People
In a strong internal control environment, people are well-trained, competent, and aware of their roles and responsibilities in maintaining control over business processes.

Process
Internal control processes are designed to ensure the reliability of financial reporting, effectiveness and efficiency of operations, compliance with laws and regulations, and safeguarding of assets.

Technology
In a strong internal control environment, technology is leveraged to automate and streamline processes, enhance data accuracy, and facilitate timely reporting.

Common causes of weakened control environments

While there are many potential breakdowns of the People, Process, Technology, and Data supporting an organization's control environment, here are some of the more common themes we're seeing from our clients –

1. **Poor accounting organization structure:** Unqualified or inadequate staffing to process the volume and complexity of transactions; inability to drive consistency and sustainability in decentralized environments.
2. **Improper valuation of Long-Lived Assets or Liabilities:** Overreliance on valuation specialists to aid in determining the fair value of long-lived assets or liabilities. Management must own the ultimate valuation and they may not adequately understand and validate key valuation considerations in some cases.
3. **Improper technology implementation or integration:** Poor change management and system development lifecycle (SDLC) processes, poorly configured access controls, lack of data governance controls and processes, and inadequately trained staff are common implementation challenges.
4. **Inadequate use of tools to avoid manual error:** Relying on manual processes and antiquated technology rather than analytics and reporting tools, to properly mitigate risk and perform key control activities. This leads to a higher risk of manual workaround solutions and control breakdowns that often scale across accounting processes.
5. **Ineffective Segregation of Duties (SOD):** Increased system complexity, difficulty in talent retention, and hybrid workforces can cause proper and timely checks and balances over key roles and potential conflicts to be easily overlooked. The lack of thorough and consistent SOD analysis without effective mitigating controls can lead to accountability issues, an increased opportunity for fraud and a significantly weakened internal control environment.

Overall, corporations face a range of pressures when it comes to remediating significant deficiencies and material weaknesses. Just like there are often several factors that contribute to a material weakness, there are several factors to consider when choosing the right path to remediation.

Misconceptions about remediating material control weaknesses

The following are common misconceptions that we have witnessed over years of helping companies remediate significant or material control deficiencies. Organizations struggle to meet their goals and sustain strong controls due to these issues.

Implementing a new system will always fix the problem

- System implementations may be completed without proper training, change management, and ongoing monitoring of system performance.
- If not handled properly, a new ERP system could lead to bigger issues early (i.e. delayed billing, slower close, poor data entry and utilization) that can linger without the proper outline for increasing personnel efficacy.

Designing new controls on ineffective processes

- We have noticed challenges when organizations embark on a new control design and implementation effort without also addressing process ineffectiveness head-on.
- In these cases, processes can continue to be broken or distressed, which may prove to be the root cause of a MW. Even if a MW can be remediated today through brute force, the risks of issues occurring again in the future may remain high until accounting processes are designed efficiently and with scale.

Only addressing current control issues singularly

- In some cases, addressing only the control issues that have been found in the most recent audit, without addressing the root causes that may be deeper to the accounting organization can lead to masking larger challenges.
- Many factors including staff turnover, changes in the business (i.e. acquisitions), lack of technical acumen, disintegrated processes, tone at the top, and cultural factors could play a deeper role in the problem.

Impacts of pervasive control issues on the business

We have observed that the challenges with a material weakness are vast and go beyond non-compliance.

1. SIGNIFICANTLY INCREASED AUDIT COST

- Material weaknesses are a proven driver for audit, consulting, and human capital cost increases
- Extremely difficult to control until accounting operations are structured
- Risk of external auditor withdrawal

2. INABILITY TO RETAIN ACCOUNTING TALENT

- Ineffective processes and controls add significant pressure on head-count
- New hires joining have less long-term retention in a messier, inconsistent environment

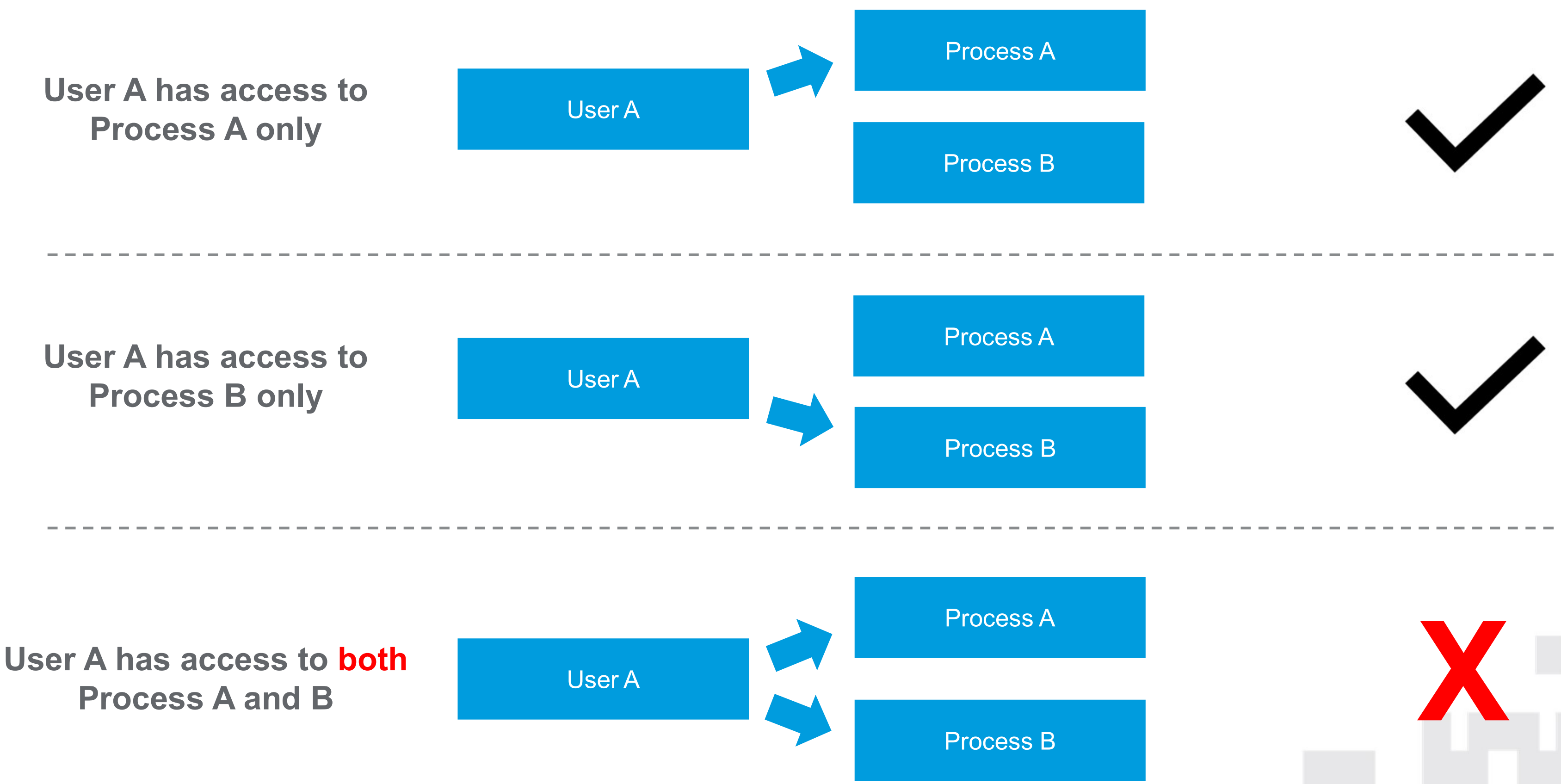
3. CHALLENGES WITH BUSINESS SCALABILITY AND GROWTH

- Lack of consistent processes and operational effectiveness impacts integration success and desired synergies
- Investor confidence in accounting accuracy erodes

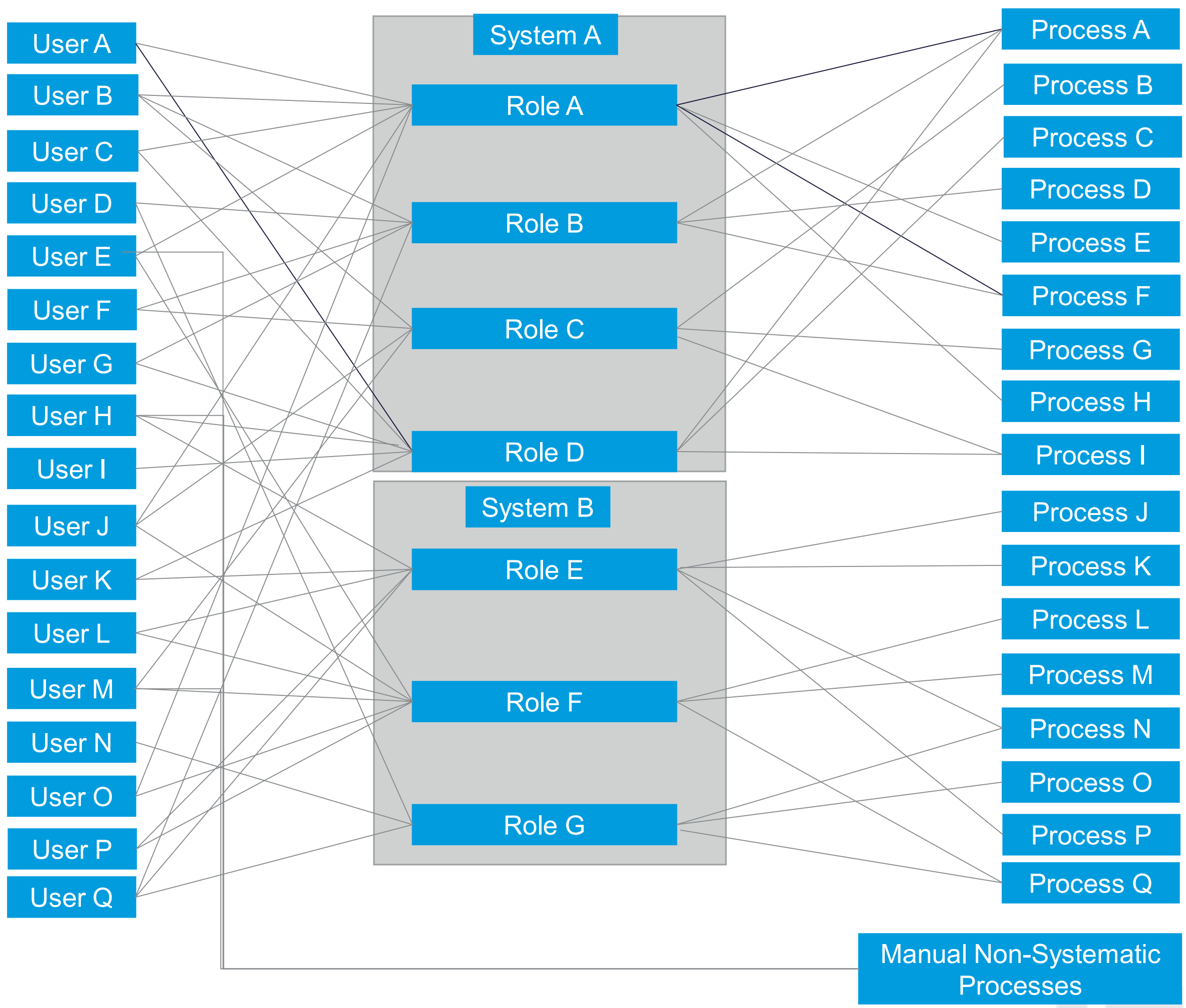
Benchmarks impacted

	1. Significantly increased audit cost	2. Inability to retain accounting talent	3. Challenges with business scalability and growth
Current state	• Audit fees consistently increasing post material weakness by material amounts (upwards of 40%) • Cost of hiring consulting support increases	• Various accounting teams with disintegrated processes and significant pressure to improve	• Business changes are not properly implemented • Increased remediation costs slow business growth
Target state	• MW remediation within one year • Year two consulting and audit fees down to pre-MW levels	• Accounting process and ERP integration • Processes are consistent and replicable period-over-period • Employees are empowered by improved state	• Global accounting centers of excellence with competent global accounting leadership • Faster, more accurate accounting close and financial reporting cycles

Case study – Segregation of Duties (SOD) risk



Case study – Segregation of Duties (SOD) risk



Addressing SOD risk is **complex**

No **specific** guidance provided by Regulators

SEC guidance

- General guidance provided to Management
- Recommends taking a risk-based approach
- Recommends mitigating risk where SOD is not realistic

PCAOB Guidance

- Audit Standard No.12 appendix B
- Provides general guidance which is **interpreted** by your **external auditor** and used to evaluate SOD Risk

Case study – Segregation of Duties (SOD) risk

Scenario

- Implemented a new ERP system prior to becoming a public company.
- Segregation of Duties (SOD) risk was not a consideration when designing and implementing their ERP security model as part of the implementation.
- User provisioning and deprovisioning was very manual in nature.
- Technology was not being leveraged to prevent or detect SOD risk at the Company.
- Business Process Owners (BPOs) had been identified by the Company but had not been trained on SOD Risk.
- As part of their Sarbanes Oxley implementation, other key controls were identified, designed and implemented.

Audit results

- Due to the lack of formal SOD controls, the Company's internal and external auditors independently evaluated SOD as part of their SOX compliance procedures.
- Both internal and external auditors identified a Material Weakness around Management's lack of controls around their SOD risk.

Case study – Segregation of Duties (SOD) risk

1st pass at remediation

- SOD Risk was treated as purely an IT issue rather than an IT and business issue
- IT implemented an SOD tool to monitor for SOD risk
- The vendor provided “out of the box” SOD ruleset was used to identify SOD risk
    - >100 unique conflicts to monitor not customized for the business
- Using the identified SOD risk, IT proceeded to remediate risk by removing security roles from users and/or removing access from the existing security roles

Impact of remediation efforts on the business

- Many users lost access that was needed to perform their day-to-day job responsibilities
- Much of the access that was removed was later reassigned
- Newly provisioned access and updates to the current security design created new conflicts
- The business was not aligned with IT in terms of SOD risk, causing tension between IT and the business

Audit results – Remediation testing

- The SOD Material Weakness was determined to be unremediated at year end

Case study – Segregation of Duties (SOD) risk

2nd pass at remediation

Key success factors

- SOD Risk was treated as both an **IT and business issue,** clearly defining **roles and responsibilities.**
- As part of step I, the business **defined SOX relevant SOD conflicts** defining SOX vs. lower risk SOD issues & aligned SOX risk with both **internal and external audit partners**.
- As part of step II, IT and the business worked together to refine the SOD ruleset to **eliminate false positives** & aligned with both **internal and external audit partners.**
- As part of step III, user level SOD violations were segmented between **risks that would be mitigated vs risks that need to be removed.**
- As part of step IV, security roles were redesigned and implemented to be **free of SOD risk** (no inherent conflicts).
- **New processes and controls** were implemented to properly manage SOD risk (stay clean).

Solutions for remediating pervasive control issues

I. First 30 days
Analyze root cause, determine technical needs to remediate, obtain buy-in and sponsorship

- Solidify root cause – properly determining the root cause issue supports a more targeted investment in remediating the issue
- Build team – Determine technical capabilities needed and identify program management support to drive execution efficiently – consult subject-matter experts where needed
- Produce cost-analysis and project plan including internal and external needs to support investment
- Coordinate with external auditors in first 30 days to obtain their feedback on plan
- Obtain Audit Committee buy-in
- Tone at the top – communicate critical remediation program to key stakeholders

II. Remediation period
Coordinate plan with auditors, program manage, execute

- Program management oversight is often critical – manages budget, external support expectations, key stakeholder buy-in, timelines
- Documentation throughout remediation is key – examples include requirements/design documentation for new systems, process flows with changes captured, review steps performed in control performance, etc.
- Coordinate throughout with external auditors on progress and set expectations for remediation testing
- Training is key

III. Testing and monitoring
Proactive test, report, and disclose

- Develop collaborative testing plan with internal or external support that includes minimum viable product (MVP) timeline for completion
- Coordinate with external auditors on potential reliance strategy for controls testing
- Provide regular updates on testing status to external auditors
- Report progress to Audit Committee and key stakeholders to promote responsibility and accountability

Overall goals and targets

- Remediation with velocity and precision – limit multi-year efforts
- Stakeholder buy-in and proper investment to be successful
- Sustainment of controls – remediation without sustainment can create repeat or new challenges
- Retention of talent and cost of compliance reductions in year 2 and beyond

Common areas of technical needs for remediation

How RSM can help

Technology transformation	• Business requirements and design for ERPs / CRMs • Internal controls automation • Segregation of duties and role-based security design
Business process restructuring	• Alignment of business processes with technology • Process design – Level 1, 2, 3 • Control design on restructured processes
Accounting organization change management	• Accounting and finance operating model development
Technical accounting	• Revenue recognition across industries • Complex accounting arrangements • Valuation analysis
Program management and governance	• Training development and delivery • Remediation program oversight and project plan execution

Thank you

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING