

A close-up, high-angle shot of a hand holding a silver pen, poised to write on a document. The background is blurred, suggesting an office setting.

Internal Control over Financial Reporting:

Best practices and useful strategies for creating
an effective system of internal control



March 2021

A solid green triangle located in the bottom right corner of the page.

Internal Control over Financial Reporting:

Best practices and useful strategies for creating an effective system of internal control

March 2021

Keeping in synch with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework

For non-public banks with assets at or approaching \$1 billion and public banks at the accelerated filer mark, it is crucially important to have rigorous internal controls in place, to test those controls, and to document all controls thoroughly. Based on the COSO framework, there are five interrelated components to consider when analyzing your institution's control environment:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

Because the framework is not highly prescriptive about specific internal controls, we've put together some practical considerations and actions to help you focus on areas that can be overlooked. These areas include spreadsheet controls, sample sizes, exception monitoring, testing, and commonly missed controls. In this paper, we provide you with tips and recommendations on creating a more effective control environment.

How do your existing (and, of course, well-documented) controls match to the 17 principles underlying the 5 components of the COSO framework?

When looking at and aligning to the COSO framework as part of Internal Control over Financial Reporting (ICFR), use the backbone of the framework to guide your work (see page 3 for the 17 principles).

Are your risk assessment, oversight activities, and planned or in-place controls covering, in aggregate, the principles for each of the five areas? Take the time to match the components of your internal control with the COSO principles so you can identify gaps in coverage. Are you thoroughly documenting all your controls? It's equally important to have controls in place, manage them effectively, and take credit for the work already taking place before reinventing the wheel for a more complete system.



Control environment

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority, and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability



Risk assessment

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant changes



Control activities

10. Selects and develops control activities that contribute to risk mitigation
11. Selects and develops general controls over technology
12. Deploys thorough policies and procedures



Information and communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally



Monitoring activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies



Audits of banking spreadsheets found that:

94% contained errors and

91% contained at least a

5% error in a bottom-line value.¹

Where to focus for impact

As you map out your specific controls, here are five areas to focus on when analyzing your bank's control environment.

1. Spreadsheet controls

Spreadsheet controls should be one of the first controls to examine. Spreadsheet errors occur through human error, including data entry mistakes, cut and paste errors, and inaccurate formulas, as well as intentional fraud. These errors can have major ramifications for financial institutions and can be very difficult to identify. For this reason, implementing specific spreadsheet controls is critical for reducing errors, especially for significant audit areas, such as Allowance for Loan and Lease Loss (ALLL) calculations and the ICFR matrix.

ALLL calculations

With the increased complexity linked to CECL implementation, it will be more important than ever to scrutinize the accuracy of your ALLL calculation spreadsheet. In addition to reporting current losses, banks must forecast future credit losses and use a "life of loan" expected credit loss estimate.

As ALLL spreadsheets are typically complex, using multiple formulas and linked cells, the margin for error is great. It is important to identify and fix all errors as an error in the calculation can result in a change in the ALLL amount and could amount to a material weakness, depending on the extent of the error.

Recommendation:

Conduct and thoroughly document a secondary independent review of the ALLL calculation spreadsheet. It should include:

- Review of key data points to system reports
- Review of formulas and checks put in place
- Consistency between the calculation and written memo

For an in-depth look at CECL requirements, download our ebook [here](#).

ICFR matrix

Now that your mapping of internal controls to the COSO principles is complete, the ICFR matrix summarizes the key controls in place under COSO, including testing and sample sizes. It is important this spreadsheet includes all key controls, is accurate, and free of errors as it is a key document for auditing.

Recommendations:

- The CFO should conduct a secondary review of the matrix after control testing is accumulated and documented
- Once established, your management team can conduct a quarterly review to verify that the controls documented are still key controls, and to review processes and procedures in place for new key controls
- The reviews should include a check of formulas and references, including accumulation of sample sizes and test counts
- If you require an integrated audit, external and internal auditors should review the matrix well before testing is set to begin, in order to allow time to address issues
- Management needs to maintain and verify consistency between the matrix, internal audit reports, and work papers, especially in reference to processes, key controls, sample sizes, and results

2. Sample sizes

Sample sizes represent another critical area that can be a control risk for testing. An appropriate sample size minimizes the risk of sampling error, and the risk of providing an inaccurate assessment.

The sample size will depend on a number of factors, including the frequency of the control and the assessed risk associated with the control area.

Recommendations:

Increase sample size when deviations are found

Once you determine a sample size, if you find a deviation, increase the sample size to reduce possible deviations in the larger sample.

For example, 40 is a good sample size for a daily control needing high effectiveness (this number may vary depending upon your auditor's requirements). If you identify a single deviation during testing, increase the sample size by approximately 50% (60 in this example). If you identify more than one deviation, consider this an exception and document and track it appropriately. See the section on Control Exception Tracking for more information.

Maintain consistent sample sizes across all controls

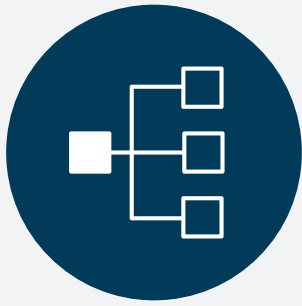
Once you determine sample sizes based upon frequency and risk assessment, apply them to all of your controls. For example, all daily high-risk controls would have the same sample size. If there are exceptions to this, document the reason for the difference and make it easily accessible to those conducting an audit.



Typical sample sizes for infrequent controls

Your sample sizes may vary depending on your auditor's requirements, but here are minimum sample sizes we typically recommend for infrequent controls:

Frequency	Sample size
Weekly	5–9
Semi-monthly	3–8
Monthly	2–4
Quarterly	2



Assess each control exception

At the end of the testing window (i.e. the quarter being reviewed) thoroughly assess each control exception, and implement a remediation plan to correct the issue prior to year-end.

Categorize exceptions as:

- Isolated incidents
- Control deficiency
- Significant deficiency
- Material weakness

Present this spreadsheet to the audit committee or board on a quarterly basis.

3. Control exception tracker and monitoring process

Once you establish and test controls, it is important to track any control exceptions where deviations occur. Establish a process to track and address control exceptions performed by all parties, including management, internal auditors, and external auditors.

Recommendations:

One point of contact for tracking exceptions

The person in charge of monitoring all internal testing should be the one to maintain and present the control exception tracking spreadsheet. Ideally, this person is independent from the controls themselves and reports directly to the board or audit committee. An internal audit manager or risk officer is ideal for this role.

Track all details of exceptions in one place

Track details of each exception, as well as an assessment of the cause of the exception. Below is an example of fields we recommend you use in your spreadsheet.

General Information about the Identified Issue

- | | |
|--------------------|----------------|
| ▪ Date or period | ▪ Description |
| ▪ Control | ▪ Auditable |
| ▪ Reference source | ▪ Evidence |
| department control | ▪ Issue detail |

Assessment of identified issue

- | | |
|---------------|--------------|
| ▪ Isolated | ▪ Deficiency |
| ▪ Incident | ▪ Material |
| ▪ Control | ▪ Weakness |
| ▪ Deficiency | ▪ Assessment |
| ▪ Significant | ▪ Rationale |

Track all identified controls on one spreadsheet, which enables easier identification of repeat control exceptions throughout the year.

4. Testing approach

Bank management is responsible for monitoring key identified controls. You can test these controls in a variety of ways, as long as there is assurance that the controls are effective.

Who should conduct the testing?

How the auditor performs the integrated audit is influenced by whether the internal testing was conducted independently or non-independently. Some things to consider:

- **Management – Non-independent**

If management is directly conducting the testing, this is not considered independent since they may be involved in the actual day-to-day functions of the key controls

- **Internal Audit Department – Independent**

If testing is performed by an internal audit department that reports directly to the audit committee or board, and is not involved in the day-to-day functions of key controls, this is considered independent

- **Independent Internal Audit Firm – Independent**

If an external firm is hired to conduct an internal audit, this is independent

If you conduct the internal testing independently, the external auditor can place more reliance on that testing, with limited reperformance to understand how the testing was performed, especially in less significant areas. The external auditor may need to perform more testing if the internal testing is not independent or involves a significant area.

Recommendations:

Independent testing creates efficiencies in the audit process

As indicated above, if those independent from the key controls perform the initial testing, the external audit firm conducting the integrated audit is more likely to rely on the testing, which increases efficiencies and decreases the amount of overlap in testing.

The bank is responsible for due diligence to ensure the auditors chosen are knowledgeable and experienced with integrated audits. Be sure to ascertain:

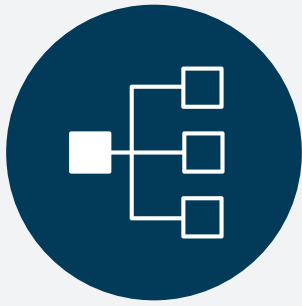
- What is their experience and knowledge with ICFR?
- What is their experience and knowledge with reporting under FDICIA ICFR/SOX 404?

Conduct testing quarterly

We recommend quarterly testing of all key controls. This allows time to identify, document, and remediate any exceptions. If you only conduct testing at year-end, it is harder to fix a potential issue and it could affect the audit opinion.



Testing needs to cover the full year under audit for an integrated audit to show the control has been operating effectively.



Assess each control exception

At the end of the testing window (i.e. the quarter being reviewed) thoroughly assess each control exception, and implement a remediation plan to correct the issue prior to year-end.

Categorize exceptions as:

- Isolated incidents
- Control deficiency
- Significant deficiency
- Material weakness

Present this spreadsheet to the audit committee or board on a quarterly basis.

5. Commonly missed documentation

There are several areas where we observe key controls over financial reporting in place, but not included in the overall control matrix. It's important to take credit for the work the bank is doing and to include all the control information in one central location. The following areas are where we commonly see banks not documenting the full control environment. As with all other controls, document and test them thoroughly.

Entity-level controls

Entity-level controls are internal controls that pertain to how the company as an entity is run, rather than being specific to a certain area of the organization. It's important to document these controls.

Corporate governance

- Review all significant policies and procedures related to corporate governance such as the Code of Ethics
- Document employees and board members acknowledging these policies and procedures

Tone at the top

This refers to the organization's general ethical climate, as established by its board of directors, audit committee, and senior management. This can be expressed in the Code of Ethics and other company communications. Having a strong "tone at the top" can have a very positive impact on preventing fraud and other unethical practices.

Overall risk assessment over financial reporting

Complete a risk assessment over financial reporting, including an assessment of fraud risk.

Regulation O

Regulation O pertains to loans to insiders, such as executive officers, directors, and principal shareholders. Include controls over transactions with these related parties in the overall control matrix.

Board of directors or audit committee self-assessment/evaluation

Have a process in place for the board of directors or audit committee to conduct a self-assessment of their performance.

Hiring and retention practices

Document all job descriptions and annual reviews/evaluations for all employees.

Controls over financial reporting

Be sure to include the following in your control matrix. As with the items above, many of these are controls that are routinely completed but not documented appropriately. As the saying goes, "If it hasn't been documented, it hasn't been done."

- Review of financial statements and footnotes
- Review of new accounting pronouncements, disclosure checklists (provided by external auditors)
- Review of estimates for Accounting for Loan Loss Allowance
- Review of assumptions and actuary report for pension and post-retirement liabilities
- Budget-to-actual reviews, including scope used
- Yield and cost-of-fund reviews, including scope used

Controls over ALLL

Normally there are controls in place regarding the review of the allowance for loan loss calculation, memo, and supporting reports. Be sure you document these items, include them in the control matrix, and test the internal controls, including controls over loan risk rating changes.

Take credit for the controls in place: Document, document, document

The key lesson here is to not only have your controls in place, but to document and test them thoroughly. Remember, if you didn't document it, you didn't do it. By having all of your key controls over financial reporting in your control matrix, you save time in the integrated audit and you can feel more confident that your bank will get credit for the full scope of your control environment.

Examples from integrated audits performed:

- A bank had documented loan processes and procedures, and had identified controls to test. The internal audit department tested them and created a separate internal audit report. However, the bank did not include these controls as part of the key controls identified in the control matrix and therefore the testing results were not included.
- Another bank was thoroughly testing employee accounts as a response to fraud risk, but, again, they did not include these controls as part of the key controls identified in the control matrix and therefore the testing results were not included.

In order to structure a control environment that meets the COSO framework, it's important to consider spreadsheet controls, to analyze your testing approach, ensure appropriate sample sizes, monitor any exceptions, and pay attention to commonly missed controls. Any bank looking at the ICFR requirement should start the process a year before the actual effective date. This allows time to set up your processes, conduct testing, and work out any challenges you find in your controls and documentation.



Review appropriate use of internal checklists, such as month-end close and year-end close. Verify that you have made all entries, performed all reconciliations, and recorded all accruals.

BerryDunn contacts

If you want advice from people with years of internal control and financial institution experience, look to BerryDunn. For more information contact:



Kaylyn Landry, CPA

Senior Manager | Financial Services

klandry@berrydunn.com

Resources

COSO Internal Control – Integrated Framework Executive Summary

<https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf>

“COSO 2013 and the Auditor” from Corporate Compliance Seminars

https://www.slideshare.net/Accountware/coso-2013-and-the-auditor-ppt-jcb-2015-april03?qid=9369fd55-dc44-445c-a4e5-8ae45435f741&v=&b=&from_search=5



Maine | New Hampshire | Massachusetts | Connecticut | West Virginia | Arizona

berrydunn.com