MorganFranklin® CONSULTING

Using a Risk-Based Approach to Assess IT Controls

Organizations rely heavily on automated systems to record business activity. The audit trail for business transactions from source journal to financial statement may only exist in an electronic format. In today's environment, it may not be possible—or efficient—to "audit around" systems.

A crucial component in understanding and ensuring compliance of organizations' business transactions is recognizing which IT controls support processes that ultimately feed each line item within the financial statements. This analysis is a key element in achieving financial compliance, fulfilling reporting objectives, and ensuring audit readiness. Most organizations have tight budgets for IT and, therefore, IT spending is reviewed rigorously. A well-structured risk management methodology can help management identify where to allocate resources and provide the critical IT capabilities needed for organizations to meet mission, financial, and compliance objectives despite budget constraints.

Organizations should consider performing periodic risk assessments over IT controls when preparing their systems for either internal or external operational or financial statement audits. The objectives of an internal control structure to include IT are to provide reasonable assurance with regard to the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. A risk assessment for IT controls should be part of every organization's overall risk management framework. It is imperative that organizations conduct risk assessments to fully understand those IT controls that have the greatest impact on achieving a clean financial audit opinion. After performing risk assessments, organizations will be able to identify which IT controls are considered high, medium, and low risk. It is the organization's responsibility to understand which IT controls pose the greatest risks to mission, the control environment, and financial reporting objectives. By applying a risk-based approach, organizations can better structure resources to:

- More efficiently allocate appropriate funds and personnel
- Gain a better understanding of the IT control environment
- Perform less substantive testing for operational and financial sampling

Risk management is the process of identifying, assessing, and taking steps to reduce risk to an acceptable level.[1] The three key steps for an organization to consider when conducting a risk assessment over its IT controls are:

1. Likelihood Determination
2. Impact Analysis
3. Risk Determination

Likelihood Ratings

1	**Remote**	Highly unlikely, but the control deficiency may occur in exceptional circumstances. It could happen, but probably never will.
2	**Unlikely**	Not expected, but there is a slight possibility the control may fail at some time.
3	**Possible**	The control deficiency may occur at some time, as there is a history of casual occurrence.
4	**Likely**	There is a strong possibility that the control will fail, as there is a history of frequent occurrence.

Impact Ratings

1	**Minor**	The control deficiency causes low impact to the financial statements due to the loss of integrity, availability, or confidentiality of data.
2	**Moderate**	The control deficiency causes minor impact to the financial statements due to the loss of integrity, availability, or confidentiality of data.
3	**Significant**	The control deficiency causes major impact to the financial statements due to the loss of integrity, availability, or confidentiality of data.
4	**Severe**	The control deficiency causes critical impact to the financial statements due to the loss of integrity, availability, or confidentiality of data.

[1] *NIST Guide for Conducting Risks Assessments, September 2012*

The likelihood determination phase involves considering the probability that an IT control will fail. Next, the impact analysis phase takes into account the effect that an IT control deficiency would have on an entity's ability to produce accurate financial statements. The final phase is risk determination. The determination of risk for a particular likelihood/impact pair can be expressed as a function of the magnitude of the impact in the event that an IT control fails. The outcome of this phase is the control risk rating. This ranking (high, medium, or low) is based on likelihood of occurrence and impact to the financial statements.

As a practical example of using the risk assessment model, consider the following application-level access control from the Federal Information System Controls Audit Manual (FISCAM): "Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner."

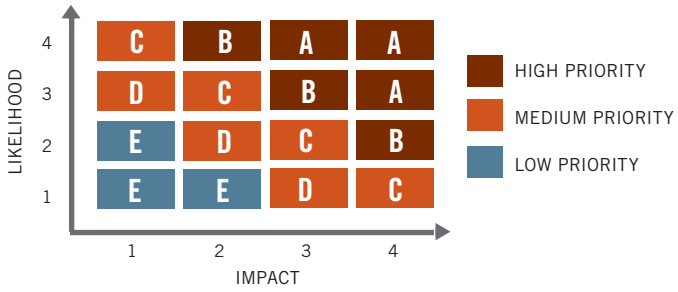
The first step in the model is for the organization to determine the likelihood of the control failing. In this example, inactive accounts and accounts for terminated individuals will not be disabled or removed in a timely manner. Based on prior experience with this control, the organization assesses that there is a history of inactive accounts, as well as accounts for terminated individuals not being deactivated. Therefore, the likelihood of the control failing is "Possible."

The next step in the risk-based approach is to determine the impact that the control deficiency will have on operations and financial statements due to the loss of integrity, availability, or confidentiality of data. Because there is a risk of users that no longer require access to the system but still have the ability to process transactions, the integrity of the data from that system is compromised. There is a direct impact on the integrity of transactions that could lead to misstatements on financial reports. The impact rating is determined to be "Significant," depending on the severity of inactive or terminated users that still have system access. The organization would need to use historical data, past audit findings, and knowledge of compensating controls to determine the level of significance of potential inactive or terminated users having continued access.

With a likelihood rating of "Possible" and an impact rating of "Significant," using the risk matrix, the control is deemed "High Priority" since there is a serious threat to financial statements if the control is operating ineffectively. This analysis is based on the high or possible likelihood that a deficiency in the control could threaten the accuracy, completeness, or validity of information. The organization should take action soon to reduce the risk. This action could include strengthening procedures around inactive or terminated user accounts, or a more frequent review of the accounts.

A risk-based approach to assessing IT controls can aid organizations in preparing systems for audit. Knowing which IT controls have the greatest impact on operations and financial reporting is a critical step in the overall risk management process. Not all IT controls affect operations or financial reporting equally. Organizations should first focus resources on remediating IT controls with high to moderate risk of adversely impacting financial statements. Then organizations should consider addressing low-risk IT controls to further strengthen the systems control environment.

Risk Matrix Based on Likelihood & Impact



Risk Rating Definitions

A	- Immediate threat to financial statements - High likelihood that risk could threaten the accuracy, completeness, or validity of information - Significant or severe impact - Immediate action should be taken to reduce risk
B	- Serious threat to financial statements - High or possible likelihood that risk could threaten the accuracy, completeness, or validity of information - Significant or severe impact - Action should be taken soon to reduce risk
C	- Moderate risk to financial statements - Moderate or significant likelihood that risk could threaten the accuracy, completeness, or validity of information - Significant or severe impact - Action should be taken in the near future
D	- Low risk to financial statements - Unlikely or possible probability that risk could threaten the accuracy, completeness, or validity of information - Moderate or significant impact - Corrective action should be taken
E	- Very low risk to financial statements - Remote or unlikely probability that risk could threaten the accuracy, completeness, or validity of information - Minor or moderate impact - Action should be taken if cost is not a significant factor

MKTG-15-CORP-TL-3815

| 7900 Tysons One Place, Suite 300, McLean, VA 22102 | 703.564.7525