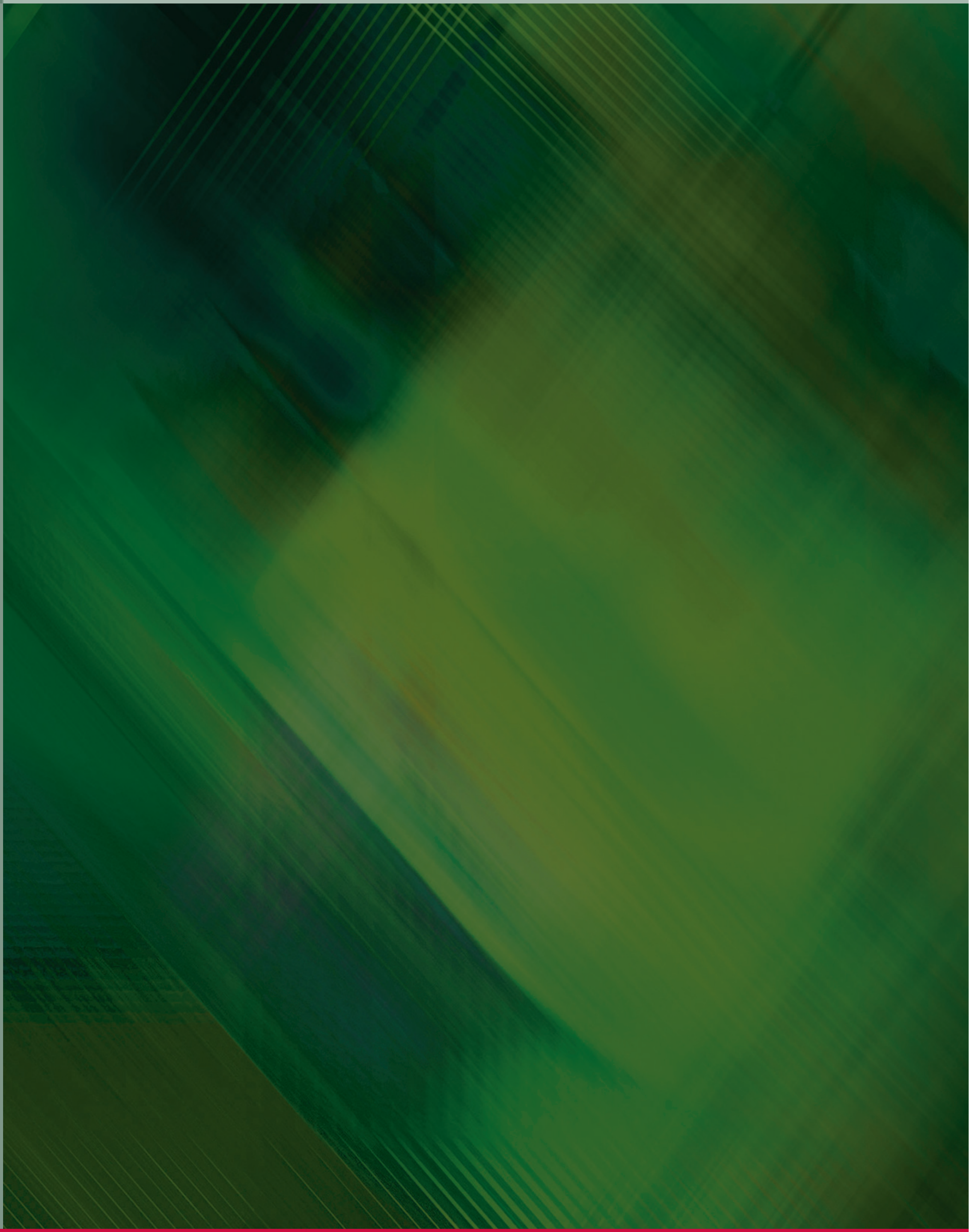
GAIT FOR BUSINESS AND IT RISK



The Institute of Internal Auditors

PROFESSIONAL GUIDANCE

Setting the Standard

GAIT for Business and IT Risk

(GAIT-R)

The Institute of Internal Auditors
March 2008

Table of Contents

1. INTRODUCTION

GAIT[1] *for Business and IT Risk* (GAIT-R)[2] is a methodology for identifying all the key controls that are critical to achieving business goals and objectives. GAIT-R identifies the critical aspects of IT that are essential to the management and mitigation of organizational risk, generically described in this document as *business risk*. These critical IT functionalities and their corresponding risks can then be considered when planning audit work.

GAIT-R was developed primarily for internal audit practitioners. It also can be used by IT governance and security managers or those who are charged with designing and managing IT risks within their organizations.

Because GAIT-R has been developed primarily for internal audit practitioners, it is focused on identifying the key controls that are in place to manage or mitigate risk. A discussion on risk management strategies is included in the conclusion.

[1] GAIT stands for Guide to the Assessment of IT Risk.

[2] GAIT-R is part of the family of IIA guidance products derived from *The GAIT Methodology*, which is a process for defining the IT general controls that should be included in an organization's assessment of internal control over financial reporting under Section 404 of the U.S. Sarbanes-Oxley Act of 2002.

2. EXECUTIVE SUMMARY

The GAIT-R Methodology is built around four principles. These are:

Principle 1: The failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business.

Principle 2: Key controls should be identified as the result of a top-down assessment of business risks, risk tolerance, and the controls — including automated controls and ITGCs — required to manage or mitigate business risk.

Principle 3: Business risks are mitigated by a combination of manual and automated key controls. To assess the system of internal control to manage or mitigate business risks, key automated controls need to be assessed.

Principle 4: ITGCs may be relied upon to provide assurance of the continued and proper operation of automated key controls.

The GAIT-R Methodology delivers a scope, based on the risks to each identified business objective, which includes:

- Manual key controls within the business process.
- Automated and hybrid key controls within the business process.
- Key controls within ITGC processes.
- Controls at the entity level, including activities in the control environment, information and communication, and other layers of the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) internal control model.

By using GAIT-R, the auditor or person performing the assessment can define the scope of work to be performed with a more complete understanding of the controls that provide reasonable assurance of the achievement of business objectives.

The end product of this methodology is a list of the key controls needed to provide reasonable assurance that selected business risks and related business objectives will be managed or mitigated adequately. The auditor can then plan an efficient and effective audit project, providing either assurance that adequate controls are in place or value-added consulting services to help management improve those controls.

The following illustrates the combination of controls that GAIT-R is likely to identify to ensure business risks are managed and objectives are achieved.

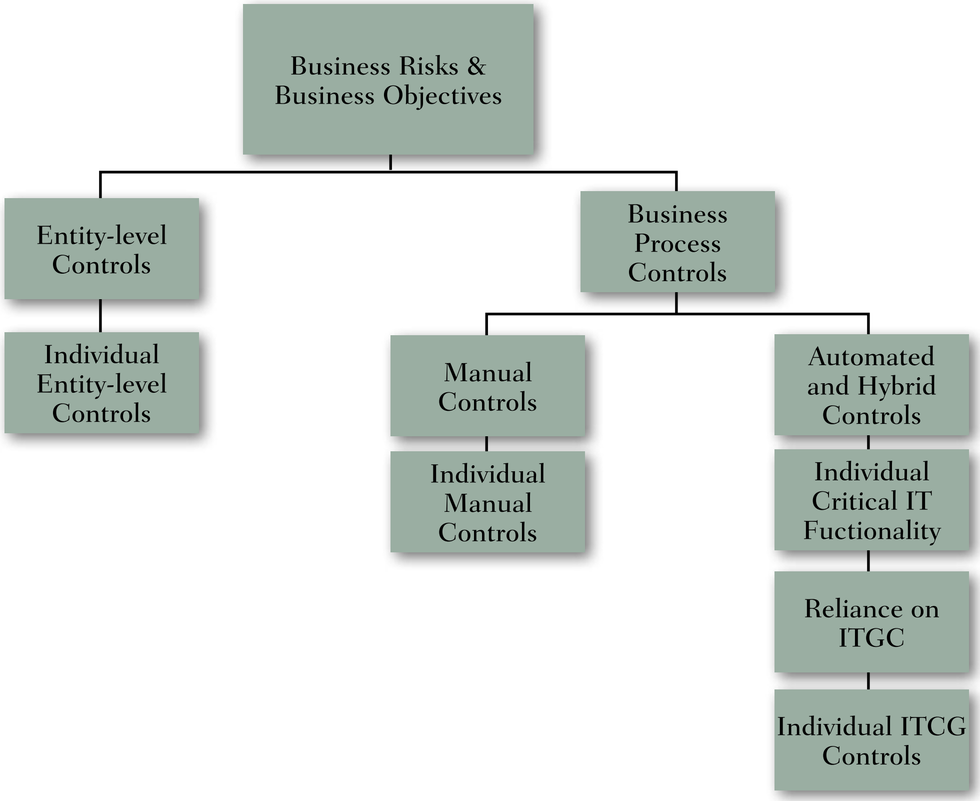

Business Risks & Business Objectives
Entity-level Controls
Business Process Controls
Individual Entity-level Controls
Manual Controls
Automated and Hybrid Controls
Individual Manual Controls
Individual Critical IT Fuctionality
Reliance on ITGC
Individual ITCG Controls

Figure 1. Identification of controls using the GAIT-R Methodology

3. WHY GAIT-R?

The need for GAIT-R is best described using two examples of real-life situations:

Company A operated a large convenience store business with approximately 4,000 stores and gasoline stations across the United States. Several years prior to the Sarbanes-Oxley Act, the external auditors' IT audit team decided it was critical to audit both application and general IT controls operating within the stores. Each store had its own server, supporting the cash register and gasoline pump operations. At least daily, often twice a day, the server would be pinged by the central computer system and upload operational and accounting data.

The external auditors' IT audit manager contacted the company's chief audit executive (CAE) and alerted him that they had identified significant control weaknesses. The CAE immediately organized a high-level meeting with the corporate controller, chief information officer, and the external auditors' overall engagement partner and senior manager.

At the meeting, the IT audit manager reported that there were security issues relating to the store servers (e.g., passwords were not regularly changed) and there were no controls to ensure the uploads were performed, complete, or accurate.

However, the external auditors' engagement senior manager immediately responded that his team had identified and tested controls in the central store accounting function that would detect any upload problem at the store level. These included the review of reports identifying missing store uploads and detailed analyses of store operations that included trends and variances from forecast by store and merchandise category. The meeting concluded with an agreement that the company's overall system of control was adequate as it related to financial reporting and that the external auditor would improve their internal coordination and risk assessment.

The lesson this example brings home is that identifying areas to audit based only on an understanding of technology risk can lead to inefficient audits. Only when all business controls are considered — both manual and automated — is it possible to identify technology risks that merit audit attention.

Some may argue that technology risks such as availability and data security are so pervasive and significant that a holistic view, as suggested in this guide, is not necessary. However, we believe that they need to be translated into business risk terms and viewed in the context of business risk before a determination can be made as to the value of auditing. Therefore, where there is value, an assessment of business rather than technology risk can serve to focus the scope of the audit more effectively. For example:

- *Availability* is clearly important to the success of an IT function. However, the business risk is not availability per se; it is the effect a failure to provide continuous IT services can have on critical business processes. For example, consider a typical manufacturing business where multiple IT services are relied on to run the business: the procurement, inventory, and manufacturing resource and planning (MRP) systems, as well as the sales ordering, billing, payroll, accounts payables, accounting, and e-mail systems, among others.

  The organization's business impact analysis[3] identifies the value of each of these services' continued availability and the cost of a loss of service for an extended period. If the business impact analysis identified the MRP and e-mail systems as the only ones where a loss of availability would be significant to the organization, then the audit should be focused on those business risks. In other words, the more effective audit would consist of a review of the controls and other measures that prevent or mitigate the business risk of a loss of the MRP and e-mail systems.

[3] A *business impact analysis* also is called a critical systems analysis, IT risk assessment, or similar.

The issue of data security is similar. Many types and forms of data are processed or stored on an organization's information network. However, the business risk of loss, inappropriate change, or unauthorized access is not consistent across all data. Audits of data security, therefore, should focus on protecting the information assets that are required to support critical business operations or where the damage to or loss of the data could represent an immediate liability (e.g., in the case of consumer credit card information or patient health records). These critical information assets are best identified by a top-down business risk assessment, rather than a risk assessment based purely on a technology perspective.

The second example shows how a business audit could fail to recognize reliance on technology and, consequently, fail to address all risks to the achievement of business objectives.

> **Company B's** internal auditors are performing an audit of the company's compliance with environmental regulations over emissions. The company operates a refinery on the West Coast of America and has to limit emissions to the air of certain gases produced during normal operations. It also has to provide weekly reports of emissions to the state regulator and take corrective actions should emissions exceed regulatory limits.
>
> The auditors' scope includes tests of, among others:
>
> - The completeness of reports submitted to the state regulator.
> - Whether all reports are reviewed and approved by the appropriate manager prior to their submission.
> - Whether the reports are filed on a timely basis.
> - Whether all instances of excessive emissions are reported promptly to management and corrective actions are taken.
> - Whether appropriate accruals are established in the event of excessive emissions where fines and other penalties are expected.
> - Whether the emissions monitoring equipment is maintained adequately.
>
> However, the scope has been designed purely from an operational and financial perspective. As a result, the auditors have not identified reliance on data and processing within the IT systems that support emissions compliance. (In this guide, automated controls and IT-dependent controls relied upon to achieve business objectives are collectively called *critical IT functionality*). Had the auditors taken a top-down approach, they should have identified significant reliance on critical IT functionality, such as:
>
> - The integrity of emissions monitoring results (i.e., data) stored in the system and used to produce the reports that monitor operations and file regulatory reports. This might have led to the in-scope inclusion of controls over access to the data.
> - The reliability of the software used to generate the key reports that monitor operations and are filed with the regulator.
> - The reliability of the emission equipment's operating system — failures in this system could lead to incorrect or incomplete monitoring results. The auditors might have gone further and assessed the controls over remote access by the equipment vendor, so that the vendor could apply patches and otherwise maintain the emission equipment's software.

The situations described in the two examples are not uncommon. This guide proposes a methodology for assessing reliance on critical IT functionality as part of a top-down assessment of business risk. In some cases, technology risks are suggested by third parties as worthy of an audit. This guide includes a process for assessing those risks and incorporating them into the top-down assessment (see Step 1 in the Methodology section).

4. THE GAIT-R PRINCIPLES

The GAIT-R Methodology is based on four principles.

Principle 1: The failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business.

Technology exists to further a business goal or objective. The failure of technology to perform as intended (i.e., technology risk) may result in or contribute to a business risk — the risk that business goals and objectives are not achieved effectively and efficiently.

Assessing technology in isolation — without identifying the related business risks and the extent to which those business risks may be insulated from the effect of technology failures — can result in inefficient audits. The approach of selecting audits based on a checklist of IT risks or control objectives from a publication, or because it appears to be important, is insufficient justification for an audit. Hence, it is necessary to understand the risks to business goals and objectives (e.g., the inability to process sales orders resulting in a loss of revenue or a failure to protect customer credit data resulting in a privacy failure).

> "There is no such thing as IT risk."
>
> – *Jay Taylor*
> *General Director, IT Audit,*
> *General Motors*

Similarly, assessing operational or financial risk without considering reliance on technology is likely to result in an inefficient or incomplete audit. Controls over critical IT functionality may not be included in scope, and manual controls may be evaluated when there are more reliable automated controls.

The second GAIT-R principle discusses the need for a top-down assessment, a holistic consideration of the business risks, the extent of manual controls, and the reliance on critical IT functionality.

Principle 2: Key controls should be identified as the result of a top-down assessment of business risks, risk tolerance, and the controls — including automated controls and ITGCs — required to manage or mitigate business risk.

In the United States, the scope of work for an assessment of internal control over financial reporting required by Section 404 is typically the result of a top-down risk assessment that starts with the business risk — the risk of material misstatement of the financial statements filed with the U.S. Securities and Exchange Commission (SEC). This approach has been influenced by guidance from the SEC, which regulates the actions of management, and the U.S. Public Company Accounting Oversight Board (PCAOB), which regulates the actions of external auditors. Both agencies have declared that the top-down assessment of risk is the key to defining an efficient scope of work.

In 2007, The Institute of Internal Auditors (IIA) published *The GAIT Methodology* to help management and auditors develop a scope for the audit of ITGCs as part of their annual assessment of internal control over financial reporting. It continues the top-down risk assessment that starts with the risk of material error in the financial statements (i.e., business risk in this case) into the assessment of risk (i.e., to that business risk) represented by ITGC.

Since its publication, the methodology has helped a growing number of companies and their auditors define a Section 404 scope for ITGC that is both effective and efficient. It has provided assurance that the right ITGC controls are evaluated. While the overall number of ITGC controls included in scope is typically reduced when the methodology is used, a number of companies have reported that their reduction is net: They have added controls in areas previously overlooked and taken out of scope controls that are not key (*key controls* are those required to prevent or detect a material misstatement of the financial statements).

It is clear from experience with Section 404 over the last few years that a top-down approach to scoping business controls is essential to an efficient scope. *The GAIT Methodology* has shown that the top-down approach also works for scoping ITGC.

Principle 3: Business risks are mitigated by a combination of manual and automated key controls. To assess the system of internal control to manage or mitigate business risks, key automated controls need to be assessed.

A system of internal control typically includes manual and automated controls. Both must be assessed to determine whether business risks are effectively managed. In particular, the assessment of controls should determine whether there is an appropriate combination of controls, including those related to technology, to mitigate business risks.

Guidance from U.S. regulators on the assessment of internal control over financial reporting (i.e., the annual assessment required by Section 404) suggests that the top-down assessment process should start with the identification of controls at the entity level. This is good advice, whether the assessment is of controls over financial reporting or related to other business objectives.

The identification of key controls should include the identification of controls at the entity level (e.g., the code of business conduct) or activity level (e.g., within the local sales function). It also should consider controls and activities within different layers of the COSO framework (e.g., the organization's recruiting process, the tone at the top, etc.). These controls and activities may be manual or automated.

Several controls usually exist around a business risk and some may address the same risk. For instance:

- Multiple approvals of a purchase order by different levels of management all ensure the purchase is authorized.
- An automated interface control may report exceptions in an upload of accounts payable transactions to the general ledger, while a manual reconciliation of the accounts payable and general ledger may also be sufficient to detect upload errors.

To assess whether there are adequate controls to manage or mitigate a defined business risk, key controls should be identified. Key controls are those relied on to ensure failures in achieving business objectives will be either prevented or detected on a timely basis.

The key controls that are identified include:

- Manual controls (e.g., the performance of a physical inventory).
- Fully automated controls (e.g., matching or updating accounts in the general ledger).
- Partly automated or hybrid controls where an otherwise manual control relies on application functionality.[4] If an error in that functionality is not detected, the entire control would be ineffective. For example, a key control to detect duplicate receipts might include the review of a system report. The manual part of the control would not be able to ensure that the report was complete. Therefore, the report would be in scope as a key report.

[4] ISACA's *IT Control Objectives for Sarbanes-Oxley* describes these as IT-dependent manual controls or hybrid controls.

The audit of a business risk should assess — by appropriate testing — all key controls, whether they are manual, fully automated, or hybrid controls.

> ***Note: If an audit of business risks includes only some but not all controls that mitigate risks (e.g., only those related to IT security or that are manual), such is a scope limitation that should be communicated clearly in the audit report.***

When there are key automated controls, including hybrid controls, consideration should be given to assessing and testing the ITGCs required to provide assurance that the automated controls perform consistently and appropriately.

Principle 4: ITGCs may be relied upon to provide assurance of the continued and proper operation of automated key controls.

Key automated controls, including hybrid controls and collectively considered *critical IT functionality,* need to operate effectively and consistently. Often, auditors will rely on ITGCs for that assurance. The top-down methodology presented below includes a process for assessing the risk to key automated controls due to failures in IT processes (e.g., in change management) and identifying the key controls within ITGCs.

If a failure in ITGCs results in a failure or lack of assurance in key automated controls relative to a business risk, an audit of controls around that business risk would be incomplete without a consideration of those key ITGCs.

The identification of the specific key ITGCs required to provide assurance over critical IT functionality is based on three sub-principles (similar to the principles in *The GAIT Methodology*):

Principle 4a: *The ITGC process risks that need to be identified are those that affect critical IT functionality in significant applications and related data.*

This relates to the concepts in the first three principles: the top-down assessment of risk to the business objectives identifies key business process controls and, from among them, critical IT functionality. Risks to that critical IT functionality from failures in ITGC — which exist in processes such as change control and security — should be identified and assessed as part of and as a continuation of the top-down approach.

Principle 4b: *The ITGC process risks that need to be identified exist in processes and at various IT layers: the application program code, databases, operating systems, and network.*

Just as there are business processes (e.g., accounts payable, budgeting, and hiring) with key business controls, there are ITGC processes (e.g., change management, computer operations, and security management) with key ITGCs.

Each ITGC process operates at the four layers[5] of each application's IT infrastructure — application, database (including related structures such as the schema), operating system, and network infrastructure. These layers are also known as the stack. Risks to the reliability of critical IT functionality can be assessed for each ITGC process at each layer of the IT infrastructure (e.g., by assessing risk in the change management process at the application code layer or in the security management process at the database level).

[5] GAIT-R uses a stack with four layers that can be customized for each organization. For example, a user of this methodology may identify a different set of four layers or use a model with a different number of layers in the stack. The number of layers and the choice of descriptions do not affect the operation of the GAIT-R Methodology.

Principle 4c: *Risks in ITGC processes are mitigated by the achievement of IT control objectives, not individual controls.*

Each ITGC process contains controls that help to achieve IT control objectives, such as:

- Systems are appropriately tested and validated prior to being placed into production.
- Data is protected from unauthorized change.
- Any problems or incidents in operations are properly responded to, recorded, investigated, and resolved.

Failure to achieve these objectives might imply that critical IT functionality fails to perform appropriately and consistently. GAIT-R helps identify the IT control objectives that are required for the significant applications.

Controls in ITGC processes do not always directly relate to the risk of failure of business objectives. Individual ITGCs assure that relevant IT control objectives are achieved. Those control objectives assure that critical IT functionality operates consistently and that critical IT functionality is required for key controls in the business processes to function consistently. The key controls in the business processes are required to provide assurance for the business objectives under review.

As a result, it is important to first identify relevant IT control objectives and only when they have been defined should the key controls in ITGC be identified. The key ITGC controls that should be included in scope are those that are required to satisfy the IT control objectives. While certain ITGCs might appear important, unless they are required to address an identified IT control objective, they do not need to be included in the review's scope.

5. GAIT-R's TOP-DOWN METHODOLOGY

Because assessing IT risk is only part of the holistic review and assessment of risks to the achievement of business goals, the steps discussed below cover the entire risk assessment and control identification process.

The GAIT-R Methodology consists of eight steps, starting with understanding the audit's review purpose or controls assessment and ending with a defined scope of work.[6]

1. Identify the business objectives for which the controls are to be assessed.
2. Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved.
3. Identify the critical IT functionality relied upon, from among the key business controls.
4. Identify the significant applications where ITGCs need to be tested.
5. Identify ITGC process risks and related control objectives.
6. Identify the ITGC to test that it meets the control objectives.
7. Perform a reasonable person holistic review of all key controls.
8. Determine the scope of the review and build an appropriate design and effectiveness testing program.

Step 1: Identify the business objectives for which the controls are to be assessed.

As noted in principle 1, IT exists to further a business goal or objective. The failure of technology to perform as intended (i.e., technology risk) may result in or contribute to a business risk — the risk that business goals and objectives are not achieved effectively and efficiently.

The auditor[7] should start the definition of scope by defining and understanding the business objectives for which assurance is required.

At times, the auditor will be presented with a concern for an identified technology risk. For example, a member of the board, the CIO, or other member of management may ask about network security or application change management risk. In those situations, the auditor should still identify the affected business risks and return to a top-down assessment. Only in this way can the underlying business risk and the relevant mitigating factors be identified, allowing the appropriate assessment of whether the concern raised for the technology risk is valid and, if so, to what extent.

[6] To enable readers to use the Methodology section of this document without the need to reference back to the principles, parts of the text used to explain the principles have been repeated.

[7] The GAIT-R Methodology also can be used by nonauditors to identify and assess risks, especially those related to IT. This methodology's reference to auditors from this point forward is intended to include other users of the methodology.

For instance, in the Company A example at the beginning of this guide, a prudent auditor would have stepped back before embarking on an audit of the application and ITGCs operating within the convenience stores.

The business risk the auditors were concerned about was that all activity within the stores was completely and accurately captured in the company's records. This would include the risks that sales are not recorded, inventory is misappropriated, and cash is not stolen.

The auditor should have obtained an understanding of all the mitigating factors, including the controls around store operations. This holistic view should have identified not only the central review of store activity, including an analysis of trends and variances, but also that there are other important controls (i.e., daily cash audits by the store manager, monthly inventory and cash audits by the area manager, and at least quarterly inventory and cash audits by the independent store auditors).

As a result, the prudent auditor would have concluded that any failure of technology within the store would have been detected within a reasonable period of time. (The assessment of whether the detective controls were sufficient should include discussions with operating management. Management would confirm that they are willing to take the risk of a delay in finding out that store employees have stolen merchandise or cash until the area manager or store auditor visits, because the cost of tighter controls is too high.)

Principle 2 asserts that technology risk only can be assessed if the related business risk is understood. The top-down approach identifies business risks and the controls in place to manage or mitigate those risks.

Step 2: Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved.

Step 2 is based on principle 3. The auditor should identify the key controls required to provide reasonable assurance that the business objectives identified in Step 1 will be achieved. Only those key controls need to be assessed, although the auditor can choose to include an assessment of nonkey controls (e.g., redundant or duplicative controls) if there is value to the business in providing such assurance.

A system of internal control typically includes manual and automated controls. Both must be assessed to determine whether business risks are effectively managed. In particular, the assessment of controls should include an assessment of whether there is an appropriate combination of controls, including those related to technology, to mitigate business risks.

Guidance from regulators in the United States related to the assessment of internal control over financial reporting (i.e., the annual assessment required by Section 404) suggests that the top-down assessment process should start with the identification of controls at the entity level. This is good advice, whether the assessment is of controls over financial reporting or related to other business objectives.

The identification of key controls should include the identification of controls at the entity level (e.g., the code of business conduct) or activity level (e.g., within the local sales function). It also should consider controls and activities within different layers of the COSO framework (e.g., the organization's recruiting process, the tone at the top, etc.). These controls and activities may be manual or automated.

There are usually several controls around a business risk. Some may address the same risk. For example:

- Multiple approvals of a purchase order by different levels of management all ensure the purchase is authorized.
- An automated interface control may report exceptions in an upload of accounts payable transactions to the general ledger, while a manual reconciliation of the accounts payable and general ledger also may be sufficient to detect upload errors.

To assess whether there are adequate controls to manage or mitigate a defined business risk, key controls should be identified. The key controls are the controls relied upon to ensure failures to achieve the business objective will either be prevented or detected on a timely basis.

The key controls that are identified will include:

- Manual controls (e.g., the performance of a physical inventory).
- Fully automated controls (e.g., matching or updating accounts in the general ledger).
- Partly automated or hybrid controls, where an otherwise manual control relies on application functionality.[8] If an error in that functionality is not be detected, the entire control would be ineffective. For example, a key control to detect duplicate receipts might include the review of a system report. The manual part of the control would not be able to ensure that the report was complete. Therefore, the report would be in scope as a key report.

The audit of a business risk should assess all key controls by appropriate testing, whether manual, fully automated, or hybrid controls.

Note: If an audit of business risks includes only some but not all controls that mitigate the risks (e.g., only those related to IT security or that are manual), such is a scope limitation that should be clearly communicated in the audit report.

[8] ISACA's *IT Control Objectives for Sarbanes-Oxley* describes these as IT-dependent manual controls or hybrid controls.

Step 3: Identify the critical IT functionality relied upon, from among the key business controls.

The critical IT functionality that is relied upon will include fully automated controls and hybrid controls (identified in Step 2) and other critical IT functionality.

Many applications perform calculations and other procedures[9] that the organization relies on. These procedures are technically not controls. However, if the functionality failed, errors might be introduced without detection from key manual or automated controls. If the errors could lead to the undetected failure to achieve the business objective they should be included as critical IT functionality.

Step 4: Identify the significant applications where ITGCs need to be tested.

Once the critical IT functionality has been confirmed, significant applications can be identified. Significant applications are those where there is a potential ITGC process risk because they contain critical IT functionality. To identify significant applications:

A. Sort the critical IT functionality by application. The resulting list of applications with critical functionality is a list of the significant applications for which risks in ITGC processes will be assessed, subject only to the next step.

B. For applications that are not considered significant based on the presence of critical IT functionality, there is one additional step: To assess whether an unauthorized change directly to the application's data could result in an undetected failure to achieve the business objective. If that is possible, the application should be assessed as a significant application.

   It should be noted that, on occasion, calculations and other functionality use data created in a prior application. Where a change to that data could result in an undetected error, the risk may lie not only within the application that uses the data, but in other applications (e.g., the application where the data was created and any other applications where the data was stored and therefore at risk). Each of these upstream applications may be significant if changes to the data in those applications is not detected there or elsewhere.

C. Continue only with significant applications.

Step 5: Identify ITGC process risks and related control objectives.

For each significant application, GAIT-R takes each IT process (e.g., change management, operations, and security) at each layer in the stack (e.g., application code, database, operating system, and infrastructure) and identifies the IT process risks and related control objectives. Table 1 is an example of a partially completed GAIT-R matrix. The matrix is an excellent way to capture the results of this step.

[9] Some IT auditors use the terms *programmed procedures* or *programmed accounting procedures* for these calculations, updating of ledger accounts, etc.

Table 1. Partially completed GAIT-R matrix

Layer	Change Management	Operations	Security
Application	*Yes* The application contains numerous key automated controls and other critical functionality, including key reports, calculations, and the updating of the general ledger, whose consistent functionality is at least reasonably likely to be adversely affected if there are failures in change management processes at the application code level. Control objectives to be addressed include: • All program changes are approved prior to implementation by IT and user management. • Program changes are appropriately tested and the results of testing approved prior to implementation.	*Yes* The application contains a number of interface batch jobs that rely on controls in this process. Control objectives include: • Batch jobs are monitored to ensure normal completion; all processing incidents are reported and appropriate corrective actions taken. • Batch jobs are included in an automated schedule that assures they are executed as required.	*Yes* User access controls are relevant since the application includes automated controls that are relative to restricting authorization of transactions to certain individuals and functions. Relevant control objectives include: • Access is limited based on defined job roles appropriate to each user's responsibilities. • Access granted to employees and contractors is removed promptly on termination of employment. • Periodic reviews are performed to ensure only authorized individuals have privileged access.
Database	Assessment not completed.		
Operating System	*No* Changes including emergency patches to the operating system are not considered likely to affect critical IT functionality to the extent that they fail. In particular, inappropriate changes or changes made without sufficient testing are immediately apparent as the entire application would fail.		
Network Infrastructure	Assessment not completed.		

When assessing risk, consider:

- The **likelihood** of an IT process failure occurring and its **potential impact.**
  - What is the likelihood that the IT process could fail in such a way that it causes critical IT functionality to fail?
  - Is it at least reasonably likely that the critical functionality could fail without prompt detection and result in the failure to achieve the business objective?

1. For each significant application, identify specific ITGC process risks and related control objectives for each layer in the IT infrastructure. In short, go through each cell in the GAIT-R matrix and answer the appropriate questions, which are shown in Table 2.
2. Use supplementary products as necessary, such as the IT Governance Institute's Control Objectives for Information and related Technology (COBIT), to ensure a complete assessment.

Table 2. Questions to ask for each cell in the GAIT-R matrix

Layer	Change Management	Operations	Security
Application	Is a failure in **change management** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **operations** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **security** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? Alternatively, is it at least reasonably likely that a failure in security could result in an unauthorized change to data in an application, such as a look-up table? If so, identify the risks and related control objectives.
Database	Is a failure in **change management** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **operations** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **security** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? Alternatively, is it at least reasonably likely that a failure in security could result in an unauthorized change to the data or other elements, such as schemas? If so, identify the risks and related control objectives.

Layer	Change Management	Operations	Security
Operating System	Is a failure in **change management** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **operations** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **security** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.
Network Infrastructure	Is a failure in **change management** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **operations** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.	Is a failure in **security** at least reasonably likely to affect critical functionality so that one or more of the identified critical functionality becomes ineffective? If so, identify the risks and related control objectives.

Step 6: Identify the ITGC to test that it meets the control objectives.

After all the risks and relevant IT control objectives are identified, the specific key controls in ITGC to address them can be determined. Frameworks such as COBIT can help significantly.

Every ITGC key control should be specifically linked to the IT control objectives identified through GAIT-R and, thus, to the proper operation of the critical IT functionality at risk.

Step 7: Perform a reasonable person holistic review of all key controls identified.

As noted above, the system of internal controls required to manage or mitigate business risks and provide reasonable assurance that business objectives will be achieved includes a number of key controls, including an appropriate combination of:

- Entity-level controls.
- Manual controls.
- Automated control, both fully automated and hybrid controls.
- ITGCs.

In this step, the auditor should step back and review the controls identified and ensure they will provide the level of assurance required. The auditor also should examine whether there are duplicative or redundant controls in which the efficiency of the review can be improved by eliminating controls where failures would be detected or compensated by other key controls.

Step 8: Determine the scope of the review and build an appropriate design and effectiveness testing program.

GAIT-R helps the auditor identify the key controls required to provide reasonable assurance that business objectives will be achieved. The auditor then can decide what type of audit or review to perform:

- A complete business audit — some might consider this an integrated audit — of all the risks.
    - The auditor should decide whether to perform the assessment in a single project or split the assessment into multiple projects that may be performed at different times.
    - If the assessment is split into multiple projects, the auditor should determine how the combined assessment will be made and reported as well as how the results of individual projects will be assessed and reported.
- An audit that is limited in scope to only selected key controls.
    - The limited scope should be clearly identified and communicated prior to starting work and also in the audit report.
    - Keep in mind that the assessment of any control deficiencies may be more difficult without understanding the effectiveness of all related controls and whether the impact of any deficiencies may be mitigated by other key controls that were not assessed.
- A consulting project, rather than an assurance project, designed to add value by improving the effectiveness of the internal control system.

6. CONCLUDING COMMENTS ON RISK MANAGEMENT

As noted in the introduction, the GAIT-R Methodology has been developed primarily for internal audit practitioners. However, a discussion of risk is not complete without considering the fact that controls are only part of the process for managing risk.

The COSO[10] Enterprise Risk Management (ERM) framework has eight interrelated components, illustrated below.

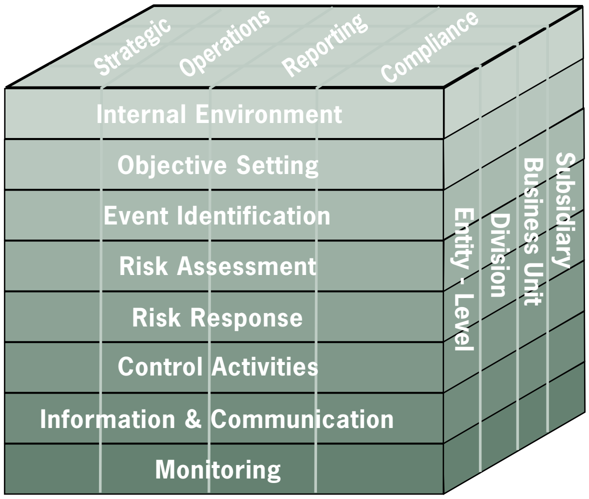


Figure 2. COSO's ERM framework

GAIT-R provides a framework for linking IT-related control activities to organizational objectives as a result of activities in two of the components:

- **Event identification,** which includes identifying those incidents that could affect strategy and achievement of objectives.
- **Risk assessment,** which includes understanding the extent to which potential events might impact objectives.

The **risk response** component includes identifying and evaluating possible responses to risk. Those responses can include risk avoidance, reduction, sharing, and acceptance. Risk response is a management responsibility outside the scope of GAIT-R, which is more focused on identifying, during an audit, key control activities (i.e., the policies and procedures that help ensure risk responses are properly executed).

[10] Go to www.coso.org for information about the COSO ERM framework.

The COSO ERM framework states:

> "With widespread reliance on information systems, controls are needed over significant systems. Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation. The second is application controls, which include computerized steps within application software to control the technology application. Combined with other manual process controls where necessary, these controls ensure completeness accuracy, and validity of information."

The value of GAIT-R for risk management professionals is that it enables the identification of specific aspects of IT that are essential to the management and mitigation of organizational risk and the achievement of objectives by using a top-down approach rather than a broad approach that, as discussed above, may not be accurate or complete.