

# Making Use of the ICAT Scores

Guidance for Departments

April 2016



**THE TREASURY**  
Kaitohutohu Kaupapa Rawa

New Zealand Government

© Crown Copyright

The “Making use of ICAT scores – Guidance for Departments” is based on *International Good Practice Guidance: Evaluating and Improving Internal Control in Organizations* of the Professional Accountants in Business Committee (PAIBC), published by the International Federation of Accountants (IFAC) in June 2012 and is used with permission of IFAC.

*International Good Practice Guidance: Evaluating and Improving Internal Control in Organizations*  
© 2012 by the International Federation of Accountants (IFAC). All rights reserved. Used with permission of IFAC.

ISBN: 978-0-908337-70-5 (Online)

The Treasury URL at 14 April 2016 for this document is  
<http://www.treasury.govt.nz/publications/guidance/mgmt/internalcontrol/icatscores>  
The PURL for this document is <http://purl.oclc.org/nzt/g-icats>

# Contents

- Introduction..... 2
- 1 Do internal controls support the department’s objectives? ..... 3
- 2 Do internal controls reflect roles and responsibilities? ..... 5
- 3 Do internal controls link to Individual performance? ..... 6
- 4 Do internal controls get applied with sufficient competency?..... 7
- 5 Are internal controls supported by a suitable “tone at the top”?..... 8
- 6 Do internal controls respond to risk? ..... 9
- 7 Do internal controls get communicated regularly?..... 11
- 8 Do internal controls get monitored and evaluated? ..... 12
- 9 Do internal controls provide for transparency and accountability? ..... 14
- Summary ..... 15

# Introduction

The process for providing supplementary assurance on internal controls in Government focuses on nine principles that represent good practice for evaluating and improving internal control systems. These principles are not formulated to design and implement an internal control system, but rather to facilitate the evaluation and improvement of existing internal control systems by highlighting a number of areas where the practical application of such guidelines often fails in many organisations.

The assessments will be whether internal controls in Government:

- 1 Support the department’s objectives
- 2 Reflect roles and responsibilities
- 3 Link to individual performance
- 4 Get applied with sufficient competency
- 5 Are supported by a suitable “tone at the top”
- 6 Respond to risk
- 7 Get communicated regularly
- 8 Get monitored and evaluated
- 9 Provide for transparency and accountability.

The assessments will be along a scale from “hardly” to “strongly” or on a scale from 0-to-4, with intervals at 0.5 points as shown below.

Hardly			Somewhat		Mostly		Strongly	
0	0.5	1	1.5	2	2.5	3	3.5	4

This guidance discusses each of these assessments, why it is important, and what to do if a “hardly” or “somewhat” score represents a result that is not aligned with the department’s risk appetite.

This guidance is based on *Evaluating and Improving Internal Control in Organisations* International Good Practice Guidance of the Professional Accountants in Business (PAIB) Committee, published by the International Federation of Accountants (IFAC) on Jun 28, 2012 and is used with permission of IFAC.

If leaders in an entity are concerned about the feedback from ICAT (Internal Control Assessment Tool) on any of the principles, the guidance suggests avenues that might be used to respond, and improve that area. These suggested responses are summarised for quick reference at the end of this paper.

# 1 Do internal controls support the department's objectives?

Internal control should be used to support the department in achieving its objectives by managing its risks, while complying with rules, regulations, and organisational policies. The department should therefore make internal control part of risk management and integrate both in its overall governance system.

Departments always face uncertainty in achieving their strategic, operational, and other objectives. However, they can decide the level of risk they wish to be exposed to in the pursuit of those objectives. Proper risk assessment and internal control assist organisations in making informed decisions about the level of risk that they want to take, and implementing the necessary controls, in pursuit of the organisations' objectives. However, risks should not be taken without an explicit understanding of their potential consequences for achieving an organisation's objectives. Therefore, decision makers require relevant and reliable information, produced through the internal control system, to effectively implement and execute their strategic and operational plans.

In recent years, focus has shifted from internal control as a separate concept to internal control as an integrated part of risk management and governance. For example, corporate governance codes worldwide now generally put greater emphasis on effective risk management than just on internal control. Internal control can be most effective when it is integrated with risk management and both are embedded in all the governance processes of a department. Risk management and internal control can therefore be viewed as two sides of the same coin, in that risk management focuses on the identification of threats and opportunities, while controls are designed to effectively counter threats and take advantage of opportunities.

Sustainable success depends on how well a department can integrate risk management and internal control into a wider governance system as an integral part of its overall activities and decision-making processes. A strong, integrated governance system is an integral part of managing a disciplined and controlled department. Effective integration can result in an enterprise-wide governance, risk management, and internal control system that:

- supports management in moving an organisation forward in a cohesive, integrated, and aligned manner to improve performance, while operating effectively, efficiently, ethically, and legally within established limits for risk-taking, and
- integrates and aligns activities and processes related to objective setting, planning, policies and procedures, culture, competence, implementation, performance measurement, monitoring, continuous improvement, and reporting.

Conversely, an excessive and exclusive focus on financial internal controls can distract management from ensuring that its operations or strategy are functioning as intended. Analyses of major failures frequently identify insufficiently controlled risks at the operational level that caused significant problems before any accountability documents could even be prepared. The challenge is to recognise that key financial controls might be able to pass a validation test, while underlying ineffective controls still expose the department to unacceptable levels of risk. For example, ensuring the effectiveness of financial reporting controls on property plant and equipment does not necessarily lead to reduction of risks such as underutilised surplus capacity, inappropriate gold plating, private misuse or theft.

Departments should, therefore, take an approach that manages all types of risk in line with the guidance under the principle, *Responding to Risk*.

### **Suggested Response**

If the leadership is concerned about the survey assessment of this principle, leaders within the department can challenge for improvements within the department include asking and following up on the following questions:

- Do the various divisions that are dealing with a particular risk or are responsible for associated controls actually work together?
- Does the department have an accurate and comprehensive understanding of its current risks?
- Does the department understand how various risks might have common causes or mutually reinforcing consequences?
- Are the department's risks within the limits for risk taking as determined by its risk appetite and tolerance levels in articulated risk management strategy and policies on internal control?
- Are risks only treated on an individual basis or does the department understand the overall effect of uncertainty on its objectives?
- Does the department sufficiently know the effectiveness of its controls and how they could be further improved?
- How can the department be certain it knows the correct answers to the preceding questions? What are its processes for monitoring and evaluation and are they effective?

## 2 Do internal controls reflect roles and responsibilities?

Departments should determine the various roles and responsibilities with respect to internal control, including the management at all levels, employees, and internal and external assurance providers, as well as coordinating participants.

Responsibilities for internal control are usually distributed among numerous groups:

- Senior Management should assume overall responsibility for the department's internal control strategy, policies, and system, and act accordingly. This group should define the risk management strategy, approve the criteria for internal control, and ensure that management has effectively undertaken its internal control responsibilities (ie, the oversight function).
- Finance staff, should design, implement, maintain, monitor, evaluate, and report on the organisation's internal control system in accordance with risk strategy and policies on internal control as approved by the governing body.
- Budget holders should be held accountable for proper understanding and execution of risk management and internal control within their span of authority.
- Internal auditors play an important role in monitoring and evaluating the effectiveness of the internal control system and conveying—independent of management—reassurance to the governing body. However, they should not assume responsibility for managing specific risks or for the effectiveness of controls.

A medium to large department should have an audit or risk management subcommittee, to which some of the primary oversight tasks with respect to internal control may be entrusted. However, the chief executive and senior management should retain overall responsibility for overseeing risk management and internal control.

In some departments, separate risk management functions exist. This function should enable broad risk management and internal control awareness across the organisation, rather than be an enforcer of compliance. Risk management staff can strengthen the risk management and control competence of governing bodies, management, and employees, but should not take over risk management and internal control responsibilities from line managers.

### Suggested Response

If the leadership is concerned about the survey assessment of this principle, leaders within the department should work to clarify how risks are “owned” within the department. Note that **controls** should be owned by someone who is responsible for their operation. The control owner or operator would normally be the person who executes the control on a day-to-day basis and can be someone other than the **risk** owner. The department should explicitly designate and communicate the various risk and control owners.

Qualified finance staff with their specific training and mindset, are in a good position to support management in determining, as well as implementing and monitoring, the various roles and responsibilities with respect to internal control.

### 3 Do internal controls link to Individual performance?

The department should link achievement of the organisation's internal control objectives to individual performance objectives. Each person within the organisation should be held accountable for the achievement of assigned internal control objectives.

It is important that the department ensures that those who are responsible for each risk are maintaining those risks within established limits for risk taking, as they may be inclined to choose their own risk limits over those of the department. Because achieving the department's objectives and maintaining effective controls are linked, this should be recognised in the department's process of performance assessment. Managers should also be held accountable for being in control, for example, by issuing in control statements or letters of representation.

#### **Suggested Response**

If the leadership is concerned about the survey assessment of this principle, then attention needs to be directed at the department's performance management system. This system needs to recognise the crucial importance of internal control to sustainable departmental success. Achieving the department's objectives and maintaining effective controls are inextricably linked. Sustainable success is based on people who create opportunities and properly control their operations.

## 4 Do internal controls get applied with sufficient competency?

Department staff should be sufficiently competent to fulfil the internal control responsibilities associated with their roles.

Competence in this respect means:

- having sufficient understanding of how changes in the department's objectives, external and internal environment, strategy, activities, processes, and systems affect its exposure to risk
- knowing how risks can be treated with appropriate controls, in line with the department's risk management strategy and policies on internal control
- knowing the principles of the segregation of duties to ensure that incompatible duties are properly segregated, so that no individual has total control over a transaction
- being able to implement and apply controls, monitor their effectiveness, and deal with any insufficiently covered risks, as well as with possible control weaknesses or failures
- having sufficient capabilities available to evaluate and improve individual controls, and
- being able to execute or review the evaluation and improvement of the organisation's internal control system.

### Suggested Response

Leadership that is concerned about the survey assessment of this principle are likely to look to their internal assurance staff for assistance. While professional internal audit staff can support the department as coaches and provide on-the-job training on risk management and internal control, they need senior-level management sponsorship and financial support to serve in these roles. With this sponsorship, departments can make the necessary make, lease or buy decisions to enhance the level of internal control competence to desired levels within the department.

## 5 Are internal controls supported by a suitable “tone at the top”?

The chief executive, the senior management group and management generally should foster an organisational culture that motivates members of the department to act in line with risk management strategy and policies on internal control set to achieve the department’s objectives. The tone and action at the top are critical in this respect.

The “tone at the top,” the culture, and the ethical framework of the department are essential to an effective internal control system. The chief executive and the senior management group alike need to lead by example with respect to good governance, risk management, and internal control. For example, if senior management appears unconcerned with risk management and internal control, then employees down the line will be more inclined to feel that appropriate management of risk through effective controls is not a priority.

While a code of conduct can support and enable the desired types of employee behaviour, the principles in such codes need to be continuously reinforced principles in word and deed, with training programs, model behaviour, and by taking actions in response to violations.

### **Suggested Response**

Leadership that is concerned about the survey assessment of this principle need to look to ways they can instil a broader culture of responsibility within an organisation. Governance, risk management, and internal control topics will need to be accorded high priority at regular governing body, management, and employee meetings. Other steps may include more positive recognition of a “hands-on” approach in the operation of controls, effective whistle-blowing procedures, and appropriate and diligent follow-up on control weaknesses or failures.

## 6 Do internal controls respond to risk?

Controls should always be designed, implemented, and applied as a response to specific risks and their causes and consequences.

Controls are a means to an end—the effective management of risks, enabling the department to achieve its objectives. Before designing, implementing, applying, or assessing a control, the first question should be what risk or combination of risks the control is supposed to modify.

Departments should mandate that all strategic and operational decision making is supported by risk management and the subsequent implementation of appropriate controls. All important deviations from the intended outcome need to be assessed.

Departments should be aware that various risks can create an aggregated effect of uncertainty on the achievement of their objectives. Therefore, risks should be assessed and controls designed taking common causes and synergies into account, including escalation and domino consequences.

Appropriate controls should be put in place to modify risk so that the level becomes acceptable. Important considerations for adequate selection, implementation, and operation of controls include:

- the characteristics (causes, consequences, and their likelihoods) of the corresponding risks
- the department's limits for risk taking
- the various types of controls, for example, managerial or transactional controls, preventive or detective controls, and manual or automated controls
- the suitability of the mix of controls, taking into account the department's size, structure, and culture
- the costs compared with the benefits of more or different controls, and
- the continuous changes that can make existing controls ineffective or obsolete and drive the need for periodic assessment of controls.

Departments should also consider the need to remain agile, avoid over-control, and not become overly bureaucratic. Internal control should enable, not hinder, the achievement of organisational objectives.

Depending on the type and level of risk and based on, among other things, the internal control considerations mentioned above, organisations can decide:

- to avoid a certain risk by not starting or terminating the activity that gives rise to the risk
- to take on additional risk in pursuit of higher reward by engaging in riskier activities or lowering the level of internal control
- to control a risk by removing the source, changing the likelihood, or changing the nature, magnitude, or duration of the consequences
- to share a risk by insuring against the risk, which is also considered a control, or
- to accept a risk by doing nothing apart from monitoring the changes in risk.

These decisions should be made explicitly and consciously.

Controls should be cost-effective in a broad sense—the overall benefits, taking into account economic, environmental, and social considerations, regulation, and the department's limits for risk taking, should be larger than the costs, and the greater the difference, the more cost-effective the control. The consequence of this principle is that internal control can, therefore, only provide reasonable assurance that an organisation meets its control objectives. It should be recognised, though, that some risks, albeit relatively small from a monetary perspective, can nevertheless have very significant consequences if they materialise, warranting a greater degree of control than a purely quantitative approach might suggest. For example, the payment of even a small bribe can cause very serious reputational damage to any department.

The balance between risks and related controls is continually changing in a dynamic environment and controls should be continually re-evaluated and re-optimised. Risk reassessment and adjustment of internal controls should be carried out on a continuous cycle. For each business cycle, when management revisits strategy the related risk and control policies also need to be reassessed. Changes in risk-taking strategy lead to changes in the amount of risk taken on or the level of controls applied. Additionally, external developments may affect risk, which, in turn, may necessitate changes in internal controls.

The effort to design, plan, execute, and monitor internal control must be properly balanced with the effort to plan, execute, and monitor the organisational business plan. With too little attention on internal control, business objectives will not be achieved. On the other hand, overly stringent control requirements can paralyse the organisation: internal control becomes a goal in itself.

### Suggested Response

Leadership that is concerned about the survey assessment of this principle have a number of avenues they can explore:

- **What is the context the department is working in?** Can we clarify the objectives? the stakeholders? their level of importance? What is the department's risk appetite? Is this consistent across the entire department or does it vary within and between projects or programmes?
- **How does the department identify the risks it faces?** What is the 'risk' in this context? What is the risk identification method? Are any 'known unknowns' or 'unknown unknowns' overlooked?
- **How does the department assess its risks?** What criteria have been employed to reach this conclusion?
- **Which risks need the most attention?** What are the chosen methods of risk management (eg, accept, minimise, mitigate or share)?
- **How does the department manage its risks?** How are specific risk management approaches implemented? What does the plan include?
- **How does the department know its risk management process is working?** Can this be used to feed back into the risk management framework and improve it?
- **How does the department keep the key people informed about the risks and their management?** Has this been legitimised including others, ie, stakeholders? Has the department planned carefully and listened to stakeholder concerns?

## 7 Do internal controls get communicated regularly?

Management should ensure that regular communication regarding the internal control system, as well as the outcomes, takes place at all levels within the department to make sure that the internal control principles are fully understood and correctly applied by all.

Internal controls can only work effectively when they, together with the risks they are supposed to modify, are clearly understood by those involved. Therefore, controls should not be documented and communicated in isolation but integrated through formal and informal channels into the elements of the management system in which they are intended to operate, including the related objectives, activities, processes, systems, risks, and responsibilities.

Proper documentation and communication are vital for effective internal control. Attention should be paid to the usability and understandability of the various policies, procedures, etc. when documenting and communicating controls. The use of plain language supports effective internal control. This language should meet professional and technical standards but also be understandable for non-professionals in this area, such as budget holders.

Documentation is only the beginning; risk management and internal control should also be embedded into the way people work. Therefore, management should ensure, through active communication and discussion, that what is written in a policy document or handbook is understood widely across the organisation and applied in practice by employees. A natural way of internalising risk management and internal control is to actively engage people, through training and team meetings, in the treatment of the risks they “own” and the development, implementation, operation, and evaluation of the related controls. This is especially important when people change roles—the risk profile, the relevant limits for risk taking, the controls in place, and the residual risk should be fully passed on to incoming staff.

Changes in the internal control system should be reflected in updated documentation and additional communications. This requires identifying, documenting, and communicating who makes the decisions; assigning responsibility for various processes; and determining how changes in the internal control system are to be approved, implemented, and monitored. It is crucial to test the design of newly implemented and documented controls, followed by monitoring their operating effectiveness.

The common use of online systems both facilitates and challenges the effective documentation, communication, and monitoring of internal control. This reality must be considered in ensuring effective dissemination and use of the organisation’s internal control policies and procedures, including updates.

### Suggested Response

Leadership that is concerned about the survey assessment of this principle may seek to engage their internal auditors in the improvement of documentation and communication of internal control systems. In addition, these staff, with risk owners and control owners, can support the organisation, for example, by organising internal control training sessions and establishing an understandable, common internal control language that meets professional and technical standards.

## 8 Do internal controls get monitored and evaluated?

Monitoring and evaluation of the internal control system is often confused with the monitoring and evaluation of the individual controls themselves. At first glance, an individual control might seem to be effective, but it should also be evaluated in the context of how the overall internal control system is intended to work. Conversely, an effective internal control system should be able to detect and remediate, in a timely manner, individual controls that have become deficient or redundant. Therefore, both the individual controls and the overall internal control system should be regularly monitored and evaluated in conjunction with each other.

Individual controls that have previously been proven to be effective can weaken over time, fail, or become redundant. Required controls could also be non-existent.

Even after remediation of deficient controls, the residual risk can still be outside the organisation's limits for risk taking, which might necessitate the implementation of additional or different controls. For example, hacking of corporate and government computer systems has become much more sophisticated, and, therefore, what was good internal control practice only a year or two ago may be inadequate today.

Poorly designed or implemented controls are a major source of risk and the design of controls themselves, as well as their implementation, should be subjected to risk assessment. In particular where the controls are in the form of written instructions or a procedure, then a suitable form of risk assessment should be used to test and optimise the controls and the process whereby they are implemented through training and communications.

The regularity of such evaluations depends on factors such as: volatility of the environment, the importance of the control, the nature of the control (eg, routine or non-routine controls), the stability of the control, the history of failures of the control, the existence of compensating controls, and cost-benefit considerations. Monitoring should include the investigation of events and other incidents to determine how controls have performed and how they could be improved. Existing controls are also to be evaluated as part of every risk assessment and reassessment.

Good quality monitoring and evaluation of individual controls occurs at a number of levels:

- Those directly involved in the execution of the control activity check the effective operation of the control as part of their control routine (ie, self-control).
- Managers who “own” the underlying risk and are responsible for the continued suitability and effective operation of the related controls may undertake ongoing monitoring, for example via their supervision of those involved in the execution of the control activity.
- Independent monitoring and evaluation, for example, via internal and external audit, can provide additional, and more objective, assurance on maintaining the effectiveness of individual controls, for example as part of monitoring and evaluation of the internal control system.

Even where internal control systems were previously effective, over time they can deteriorate and lose their effectiveness to the point where significant weaknesses or failures can start occurring. Therefore, departments need a structured process to ensure that the internal control system is being thoroughly evaluated on a timely basis.

### Suggested Response

Leadership that is concerned about the survey assessment of this principle therefore need to consider whether their concern is associated over individual risks and controls or the monitoring of the overall risk management and internal control system.

If the concern is over the monitoring and evaluating of individual controls, a first step is to recognise the value of direct evidence of effectiveness, such as error rates, customer complaints, and numbers and amounts of unmatched cash items. In fact, these are among the best sources of information on control failure.

Actions arising from individual control evaluations that leaders could then stress include:

- determining whether the control is working the way it is intended to work
- correcting failures or mistakes, understanding why the failure happened or the mistake was made, and ensuring that it will not happen again, all of which should be part of the continuous-improvement cycle
- decommissioning outdated controls—while making sure that they are truly obsolete—to keep the internal control system effective
- properly documenting the corrections of the controls and communicating them to all those involved, and
- summarising the various individual control failures as input for the evaluation of the internal control system, as many failures of individual controls may indicate weaknesses in the overall internal control system.

If the concern is over the monitoring and evaluating of the internal control system, then leaders need to consider a structured review to ensure that the internal control system is being thoroughly evaluated on a timely basis. The timing of such reviews will depend on the pace of internal and external change. For example, monitoring can take place periodically in tandem with the yearly business planning and evaluation cycle, or when there are indications of reduced effectiveness, such as several failures of individual controls.

The internal control system should be monitored and evaluated against the risk management strategy and policies on internal control, taking into account strategic, financial, and operational performance and the risks associated with achieving objectives for these areas. Elements should include re-examining the underlying choices, principles, and assessments made in arriving at the current system; review of reported incidences of control failures since the last evaluation; review of external and internal developments that, taken together, could suggest that overall choices may need to be re-considered.

Actions arising from the evaluation of the internal control system should include combining the results of the previous “Plan-Do-Check-Act Cycle” with new input, so that the organisation can quickly and effectively react to departures from its plan and adapt to environmental changes that impact its ability to achieve its objectives within its limits for risk taking.

## 9 Do internal controls provide for transparency and accountability?

The department should periodically report to stakeholders the organisation's risk profile as well as the structure and factual performance of the organisation's internal control system.

Departments should transparently report on the structure and performance of their governance, risk management, and internal control system in their various reports to internal and external stakeholders, such as through their periodic accountability reports.

In NZ these requirements are placed in statute, and there are separate scrutiny processes to ensure these statutory requirements are complied with.

### **Suggested Response**

Leadership that is concerned about the survey assessment of this principle, may need to look at the scrutiny processes that support the statements of responsibility. They may also wish to consider reporting not only on the existence of their system, but also about major risks the department faces; what controls it has established; how internal control is monitored and evaluated; how the system works; and what has been done to remediate any control failures or weaknesses. A better understanding as to how a department manages its risks creates trust and the necessary reassurance to its stakeholders.

# Summary

Principle of Concern	Leadership Response
Do internal controls support the department's objectives?	<p>Challenge for improvements within the department by asking and following up on the following questions:</p> <p>Are the various divisions that are dealing with a particular risk or are responsible for associated controls actually working together?</p> <p>Does the department have an accurate and comprehensive understanding of its current risks?</p> <p>Does the department understand how various risks might have common causes or mutually reinforcing consequences?</p> <p>Are the department's risks within the limits for risk taking as determined by its risk appetite and tolerance levels in articulated risk management strategy and policies on internal control?</p> <p>Are risks only treated on an individual basis or does the department understand the overall effect of uncertainty on its objectives?</p> <p>Does the department sufficiently know the effectiveness of its controls and how they could be further improved?</p> <p>How can the department be certain it knows the correct answers to the preceding questions? What are its processes for monitoring and evaluation and are they effective?</p>
Do internal controls reflect roles and responsibilities?	Clarify how risks are "owned" within the department. The department should explicitly designate and communicate the various risk and control owners.
Do internal controls link to individual performance?	Improve the department's performance management system so that it recognises the crucial importance of internal control to sustainable departmental success, based on people who create opportunities and properly control their operations.
Do internal controls get applied with sufficient competency?	Look to internal assurance staff to support the department as coaches and provide on-the-job training on risk management and internal control. Provide them with senior-level management sponsorship and financial support to serve in these roles.
Are internal controls supported by a suitable "tone at the top"?	Look to ways to instil a broader culture of responsibility within an organisation. Accord high priority to governance, risk management, and internal control topics at regular governing body, management, and employee meetings. Other steps may include more positive recognition of a "hands-on" approach in the operation of controls, effective whistle-blowing procedures, and appropriate and diligent follow-up on control weaknesses or failures.
Do internal controls respond to risk?	<p>A number of avenues may need to be explored:</p> <p>What is the context the department is working in?</p> <p>How does the department identify the risks it faces?</p> <p>How does the department assess its risks?</p> <p>Which risks need the most attention?</p> <p>How does the department manage its risks?</p> <p>How does the department know its risk management process is working?</p> <p>How does the department keep the key people informed about the risks and their management?</p>

<b>Principle of Concern</b>	<b>Leadership Response</b>
Do internal controls get communicated regularly?	Engage internal auditors in the improvement of documentation and communication of internal control systems. Support the organisation, for example, by organising internal control training sessions and establishing an understandable, common internal control language that meets professional and technical standards.
Do internal controls get monitored and evaluated?	<p>If the concern is over the monitoring and evaluating of individual controls, recognise the value of direct evidence of effectiveness, such as error rates, customer complaints, and numbers and amounts of unmatched cash items, and ensure action is taken on this evidence.</p> <p>If the concern is over the monitoring and evaluating of the internal control system, then undertake structured review to ensure that the internal control system is being thoroughly evaluated on a timely basis.</p>
Do internal controls provide for transparency and accountability?	Update the scrutiny processes that support the statements of responsibility. Consider the value to be obtained from the trust and the reassurance to its stakeholders of a better understanding as to how a department manages its risks.