Enhancing the Audit Follow-up Process Using COBIT 5

COBIT® 5 for Assurance builds on the COBIT® 5 framework by providing detailed and practical guidance for assurance professionals on how to use COBIT 5 to support a variety of IT assurance activities.

One of the key IT assurance activities is ensuring that risk has been mitigated. *COBIT 5 for Assurance* requires that, where appropriate, recommendations should include provisions for timely monitoring and follow-up.[1]

Implementing an audit follow-up process using the COBIT 5 enablers and ISACA's Information Technology Assurance Framework (ITAF)[2] provide value to the enterprise.

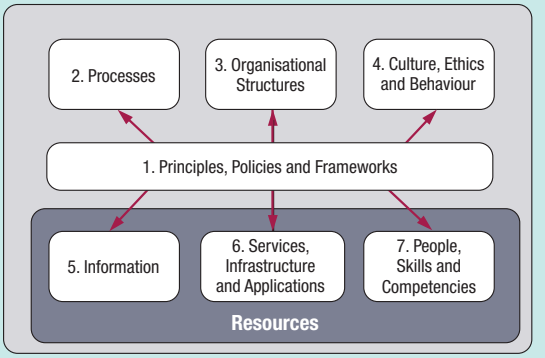
COBIT 5 Enablers and the Audit Follow-up Process

Enablers are factors that, individually and collectively, influence whether something will work. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve.[3] The COBIT 5 framework describes seven categories of enablers (**figure 1**). *COBIT 5 for Assurance* reviews each of these enablers, highlighting the assurance perspective. This article follows a similar methodology focusing on the audit follow-up process.

Principles, Policies and Frameworks
Principles, policies and frameworks are the vehicles to translate the desired behavior into practical guidance for day-to-day management.[4]

Practical guidance for audit follow-up activities are included in ITAF. Specifically, standard 2402, Follow-up Activities,[5] requires IS audit and assurance professionals to monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

Figure 1—COBIT 5 Enterprise Enablers



Source: ISACA, COBIT® 5, USA, 2012

Processes
Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.[6]

Processes require good practices. These are provided by the ITAF guideline 2402,[7] which documents guidelines on confirming the actions taken in response to audit recommendations. Processes should also have a life cycle. This is documented in the 2402 guideline as:

- 2.1 Follow-up process
- 2.2 Management's proposed actions
- 2.3 Assuming the risk of not taking corrective action
- 2.4 Follow-up procedures

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Ian Cooke, CISA, CGEIT, CRISC, COBIT Foundation, CFE, CPTS, DipFM, ITIL Foundation, Six Sigma Green Belt
Is an IT audit manager based in Dublin, Ireland, with more than 25 years of experience in all aspects of information systems. A member of ISACA's Communities Working Group, he is also the topic leader for the Oracle Databases, SQL Server Databases and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke welcomes comments or suggestions at *Ian_J_Cooke@hotmail.com* or on the Audit Tools and Techniques topic in the ISACA Knowledge Center.

- 2.5 Timing and scheduling of follow-up activities
- 2.6 Nature and extent of follow-up activities
- 2.7 Deferring follow-up activities
- 2.8 Form of follow-up responses
- 2.9 Follow-up by professionals on external audit recommendations
- 2.10 Reporting of follow-up activities

The steps suggest that audit recommendation items have different statuses as they flow through the life cycle. **Figure 2** summarizes the statuses that an action may have through its life cycle.

Organizational Structures

Organizational structures are the key decision-making entities in an enterprise.[8] Good practices here include defining the operating principles, the span of control, the level of authority, the delegation of authority and the escalation procedures for audit recommendation items. The best way to do this is using a responsible, accountable, consulted and informed (RACI) chart. A suggested RACI chart for the audit follow-up process can be seen in **figure 3**.

Culture, Ethics and Behavior

Culture, ethics and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.[9] For the audit follow-up process, the focus is on confirming the implementation of audit items. Good practices are discussed in **figure 4**.

Figure 3—Audit Follow-up RACI Chart

Responsible	Auditee—Issue manager
Accountable	Auditee's manager—Issue owner
Consulted	Risk management, compliance, legal, etc.
Informed	Board, audit committee, external audit

Source: Ian Cooke. Reprinted with permission.

Information

Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and properly governed.[10]

Information about the audit follow-up items should be captured in an assurance findings register. This is a register of issues/findings raised during assurance activities. It is maintained and followed up on to

Figure 2—Audit Recommendation Statuses

Status	Description	Related Date
Draft	The action has yet to be agreed upon with management.	Date raised
Outstanding	The action has been agreed upon with management, but has not yet been implemented.	
Partially implemented	The action is a work in progress; some elements have been implemented.	
Fully implemented	Management has indicated that all elements of the agreed-upon action have been completed.	Fully implemented date
Confirmed	Internal audit has confirmed, via follow-up procedures, that the agreed-upon action has been completed.	Date closed
Deferred	The action has been deferred until a later date (e.g., it may be dependent on another action, activity or upgrade).	Date closed
Disagreed	Management has decided against implementing the agreed-upon action.	Date closed

Source: Ian Cooke. Reprinted with permission.

ensure that significant issues/findings have been acted on as agreed upon in assurance reports.[11] **Figure 5** shows the data items that should be captured at a minimum.

Figure 4—Culture, Ethics and Behavior Good Practices

Communication	The purpose of the audit follow-up process should be documented and communicated to all employees, but especially those identified in **figure 3**.
Champions	Employees who are willing and/or able to champion the follow-up process should be identified.
Enforcement	There may be a need for enforcement. For example, there may be a need for a human resources (HR) policy stating that any misrepresentation by auditees will result in disciplinary action.
Incentives and rewards	Completion of audit recommendations items could form part of the auditee's incentives schemes.

Source: Ian Cooke. Reprinted with permission.

Figure 5—Assurance Findings Register Minimum Data Items

A unique reference number
The report reference
A description of the item/risk
Significance—denotes the level of perceived risk
A description of the proposed solution/mitigation
The proposed implementation date

Source: Ian Cooke. Reprinted with permission.

However, it is advantageous to add additional data items. *COBIT® 5: Enabling Information* describes information attributes. Specifically, semantics refers to the meaning of information.[12] One can add to the meaning of information by adding data items (**figure 6**).

Other items may be applied that add meaning to the enterprise.

Figure 6—Assurance Findings Register Suggested Additional Data Items

Recommendation theme
Company, division
Country
Related framework/regulation

Source: Ian Cooke. Reprinted with permission.

Services, Infrastructure and Applications

Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.[13]

From an audit follow-up perspective, what is really required is a facility to store the assurance findings register and produce reports based upon the same. This may be an application (e.g., audit management software) or Microsoft Excel/Access. Workflow-type applications may also be helpful for requesting and following up on the recommendations.

People, Skills and Competencies

People, skills and competencies are required for the successful completion of all activities and for making correct decisions and taking corrective actions.[14]

The auditor must be competent and have the necessary skills to confirm the implementation of the audit item. The auditor should know or have an idea in advance of what would be acceptable to confirm implementation. This may vary depending on the significance of the item. A Certified Information Systems Auditor® (CISA®) qualification and familiarity with ITAF would also be of benefit.

Bringing It All Together—The Audit Follow-up Process in Action

Management's Proposed Actions

The follow-up process begins with the creation of the audit report, specifically, at the time recommendations are made and management's proposed actions[15] are documented. **Figure 7** documents what should be captured at this stage.

Enjoying this article?

- Read ***Information Systems Auditing: Tools and Techniques—IS Audit Reporting.*** *www.isaca.org/tools-and-techniques*
- **Learn more about, discuss and collaborate on using COBIT® 5 in the Knowledge Center.** *www.isaca.org/cobit-5-use-it-effectively*

Figure 7—Sample Audit Recommendation Item

Data Item	Reference	Example
A unique reference number	**Figure 5**	3434
The report reference	**Figure 5**	2016/05
A description of the item/risk	**Figure 5**	There was no service level agreement (SLA) defined….
Significance—denotes the level of perceived risk	**Figure 5**	3 (1 is highest)
A description of the proposed solution/mitigation	**Figure 5**	An SLA will be defined….
The proposed implementation date	**Figure 5**	09/30/2016
Auditee—issue manager	**Figure 3**	IT manager 4
Auditee's manager—issue owner	**Figure 3**	Executive 2
Status	**Figure 2**	Outstanding
Date raised	**Figure 2**	06/30/2016
Fully implemented date	**Figure 2**	
Closed date	**Figure 2**	
Recommendation theme	**Figure 6**	SLAs
Company, division or location	**Figure 6**	Dublin
Country	**Figure 6**	Ireland
Related framework/regulation	**Figure 6**	COBIT 5 APO09

Source: Ian Cooke. Reprinted with permission.

Follow-up Procedures

Once the proposed actions are agreed upon, procedures for follow-up activities should be established.[16] This should include:

- An evaluation of management's response
- A verification of the response, if appropriate
- Follow-up work, if appropriate

Upon completion of the follow-up activities, the status of the audit recommendation item should change. For example, the recommendation status may change from "outstanding" to "partially implemented," "fully implemented" or, if verified, "closed."

The significance can also change. This could occur where application systems have changed, compensating controls have been implemented, or business objectives or priorities have changed in such a way as to effectively remove or significantly reduce the original risk.

Assuming the Risk of Not Taking Corrective Action

Management may decide to accept the risk of not correcting the reported condition because of cost, complexity of the corrective action or other considerations.[17] In such circumstances, the recommendation may be disagreed with or deferred until a later date.

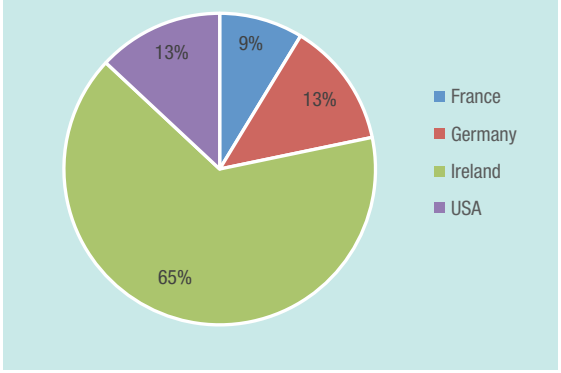
Reporting of Follow-up Activities

ISACA's documentation recommends that a report on the status of agreed-upon corrective actions arising from audit engagement reports, including agreed-upon recommendations not implemented,

should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).[18]

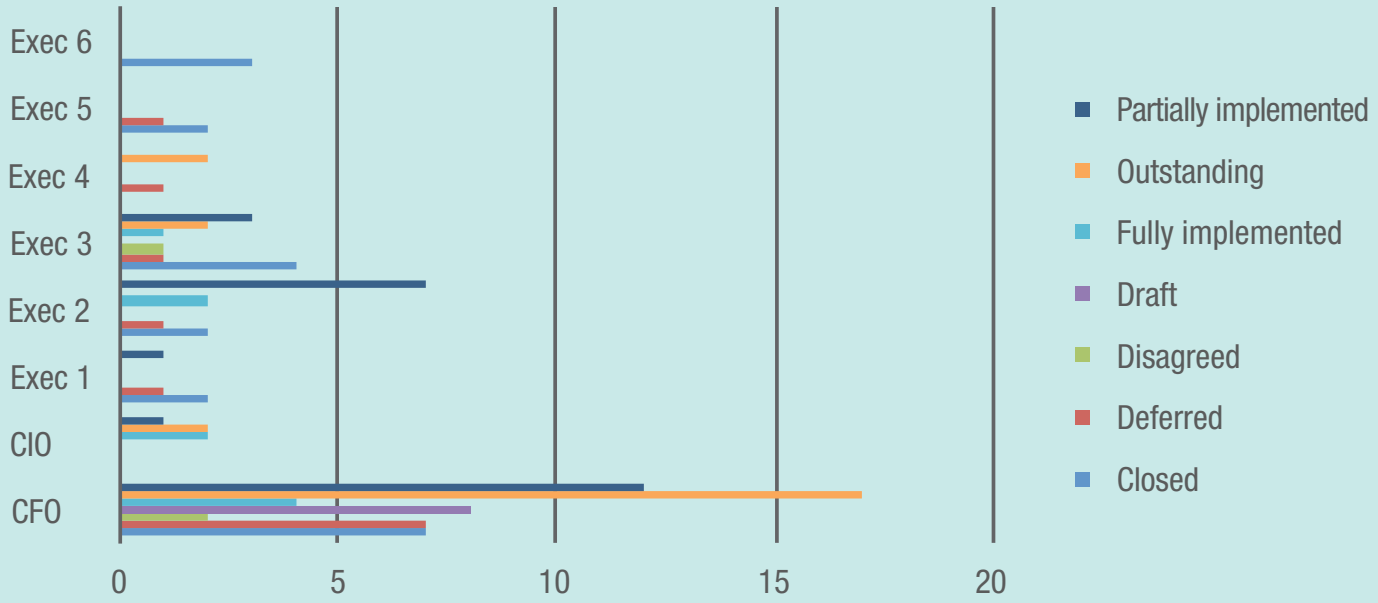
Reporting on the status of individual items is good practice. However, by collecting the information suggested earlier, together with the tracked statuses and related dates, more can be done. First, by using Excel pivot tables (or a similar tool) the data can be aggregated. This can then be used to show how entire sections, divisions, countries or owners are performing (**figures 8** and **9**).

Figure 8—Sample Summary—Outstanding by Country



Source: Ian Cooke. Reprinted with permission.

Figure 9—Sample Summary—Status by Owner



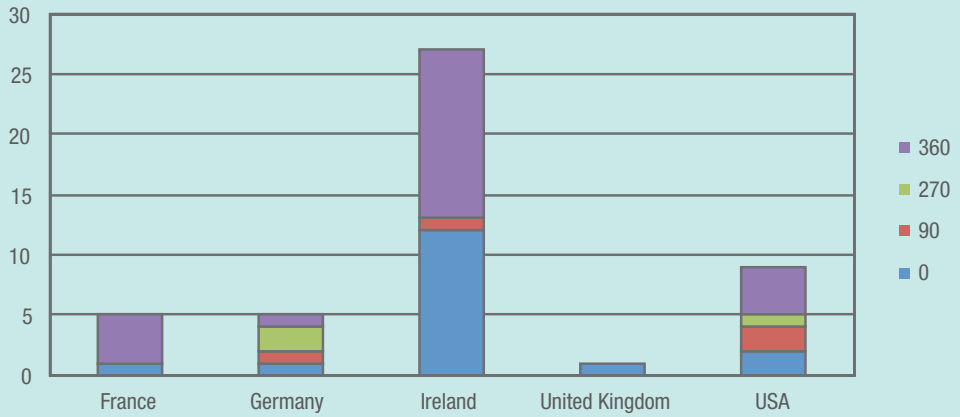
Source: Ian Cooke. Reprinted with permission.

Excel pivot tables can also be used to summarize the audit recommendations statuses into formats with which management will be familiar (**figure 10**).

Or, they can be used to demonstrate compliance to the enterprise's standards (**figures 11** and **12**).

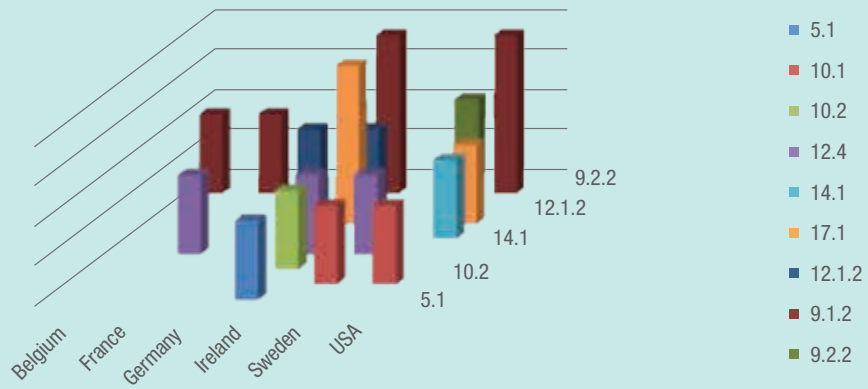
These examples indicate pain points and are very much lag indicators. However, a careful review of the allocated themes reveal that they can also be considered lead indicators. For example, if a new application is going to be implemented in Ireland, there are likely to be issues with authentication and authorization (**figure 13**).

Figure 10—Sample Summary Overdue Items by Number of Days



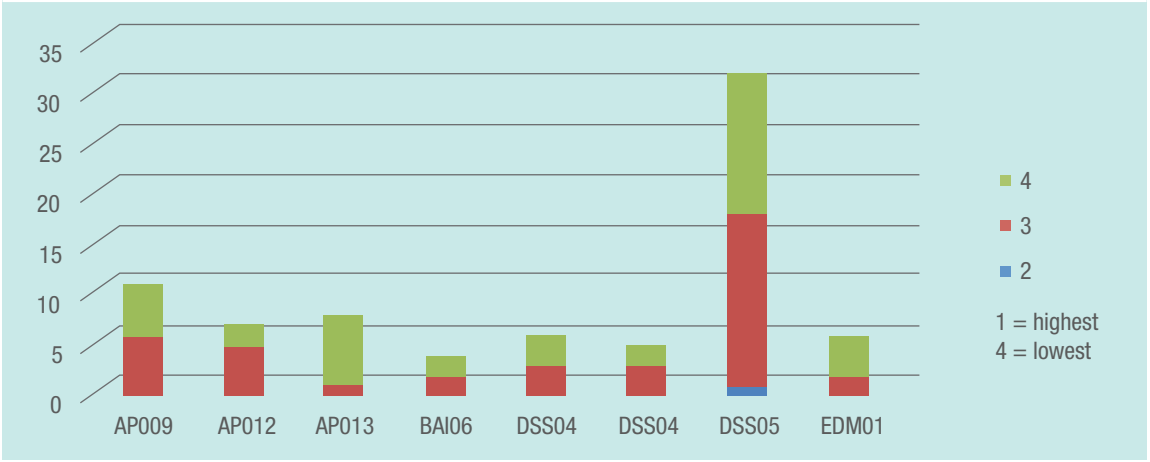
Source: Ian Cooke. Reprinted with permission.

Figure 11—Sample Summary Closed Items by International Organization for Standardization (ISO) Clause



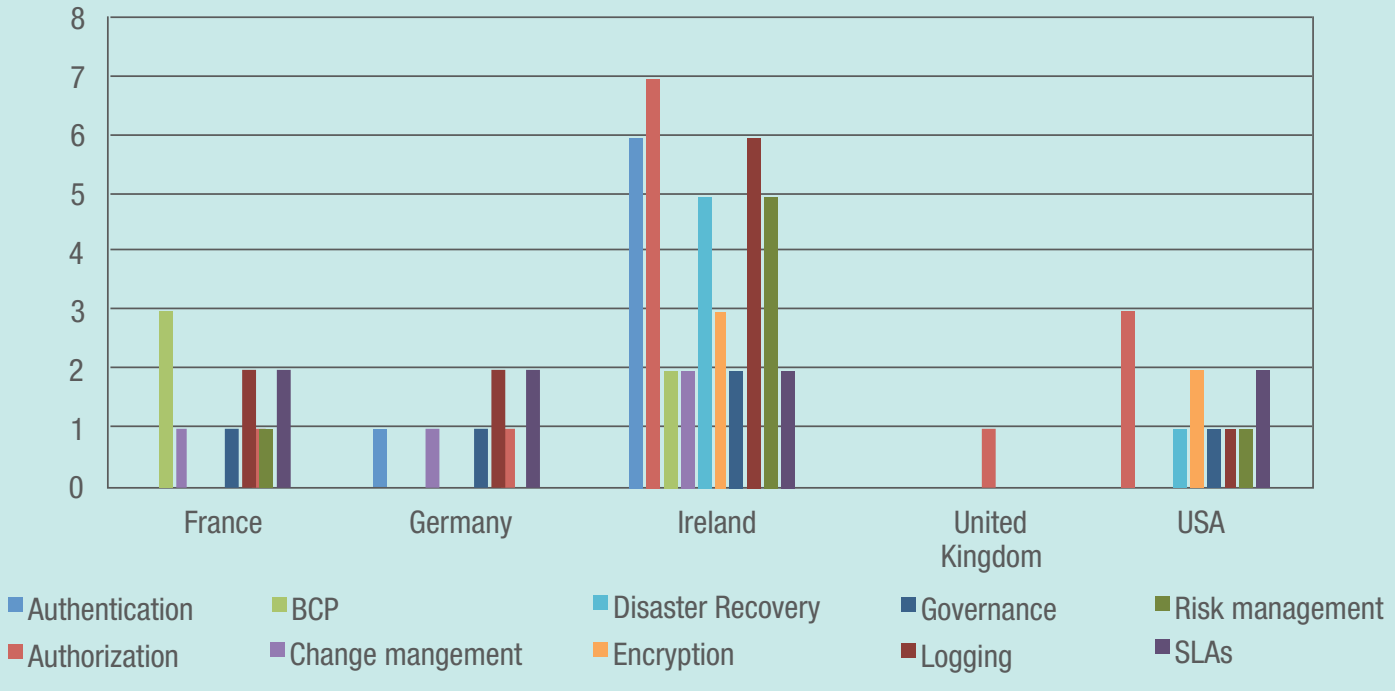
Source: Ian Cooke. Reprinted with permission.

Figure 12—Sample Summary—Significance by COBIT 5 Reference



Source: Ian Cooke. Reprinted with permission.

Figure 13—Sample Summary—Open Items by Theme



Source: Ian Cooke. Reprinted with permission.

Benefits of the Enhanced Audit Follow-up Process

Capturing the audit recommendation statuses in an assurance findings register means that, as per good practice, a report on the status of agreed-upon corrective actions can be presented to senior management and the audit committee. However, by capturing the suggested additional information, one can:

- Present summarized information by country/department/region/owner
- Present the information in a format with which executives are familiar
- Clearly show compliance to standards and regulation
- Use the information as a lead indicator for new initiatives

This gives a better perspective of the risk affecting different areas of the enterprise.

Endnotes

1 ISACA®, *COBIT® 5 for Assurance*, USA, 2013, p. 17, *www.isaca.org/COBIT/Pages/Assurance-product-page.aspx*
2 ISACA, *ITAF™: A Professional Practices Framework for IS Audit/ Assurance, 3rd Edition*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITAF-3rd-Edition.aspx*
3 ISACA, COBIT® 5, USA, 2012, p. 27, *www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx*
4 *Op cit*, COBIT 5, p. 27
5 *Op cit*, ITAF, p. 39
6 *Op cit*, COBIT 5, p. 27
7 *Op cit*, ITAF, p. 141
8 *Op cit*, COBIT 5, p. 27
9 *Ibid*.
10 *Ibid*.
11 *Op cit*, *COBIT® 5 for Assurance*, p. 45
12 ISACA, *COBIT® 5: Enabling Information*, USA, 2013, p. 37, figure 28, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*
13 *Op cit*, COBIT 5, p. 27
14 *Ibid*.
15 *Op cit*, ITAF, p. 142
16 *Ibid*.
17 *Ibid*.
18 *Ibid*.