Kick Start Guide

TickIT*plus*

Software and IT Quality Management and Certification

ISO 9001
ISO/IEC 20000
ISO/IEC 27001
ISO/IEC 25030
ISO/IEC 15504
ISO/IEC 12207
ISO/IEC 15288

BSi

Kick Start Guide

TickIT*plus*

Dave Wynn

Reviewed by JTISC

First published in the UK in 2011
by
BSI
389 Chiswick High Road
London W4 4AL

Typeset in Calibri by Helius

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN 978-0-580-74632-1

Contents

Overview

This guide aims to provide sufficient information for IT suppliers to implement a certified management system compliant with the new TickIT*plus* scheme. It is divided into the following sections:

- a general introduction providing a brief background to the scheme and the basic concepts
- information about identifying and selecting the certification scope and developing in-house resources
- guidance on identifying organizational processes, mapping them to TickIT*plus* processes and establishing the Assessment Strategy
- advice on preparing for, participating in and following up an assessment.

While this guide covers the involvement of an organization in formal certification assessments, and in particular the preparation aspects, it does not detail or discuss activities undertaken by certification bodies in conducting such assessments. Further, as an introductory guide, it concentrates specifically on achieving the Foundation level of the scheme, either through initial entry or transition from the existing TickIT scheme.

Further detailed guidance and additional information on certification can be obtained from the scheme documentation and certification bodies.

General introduction and scheme concepts

TickIT*plus* is a new scheme that was launched in early 2011 by the JTISC (Joint TickIT Industry Steering Committee). The principal aims of the scheme are to capitalize on the strengths of TickIT, while recognizing the changes in today's world of software development. Some of the key goals are to:

- adopt a full process-driven approach to business systems management
- introduce capability assessment concepts
- accommodate multiple requirement standards, e.g. ISO 9001, ISO/IEC 20000-1 (*IT service management*) and ISO/IEC 27001 (*IT information security management*)
- strengthen the commitment to improvements
- enable collaborative assessments to be undertaken more formally.

The TickIT scheme has existed since the early 1990s and, although it has been at the forefront of encouraging good IT engineering, auditing and certification practices,[1] it is now becoming outdated. In the early 1990s, TickIT was introduced primarily to address issues within the classic software development areas. Over the years, IT provision has significantly diversified and there is now much less bespoke development being undertaken. There is greater emphasis on, for example, package adaptation, system integration and configuration, internet applications, etc. There is also an increasing trend towards the provision of IT-related services, with the associated availability and security concerns.

From its launch, TickIT only ever provided guidance on the interpretation of ISO 9001 and, although the use of processes was encouraged, because it was tied to ISO 9001, it was still predominantly requirements-driven. The 2000 edition of ISO 9001 significantly strengthened the process-based approach, but in essence it still remained requirements-driven, even though the *TickIT Guide Issue 5* incorporated the process definitions of ISO/IEC 12207 to provide guidance on the use of good software lifecycle processes. By comparison, newer requirements standards, such as ISO/IEC 20000-1 and ISO/IEC 27001, were emerging and were more clearly process-based.

Another consequence of being tied to ISO 9001 was that TickIT audits could only result in a pass or a fail and this is now seen as a serious limitation. Customers are starting to need, and even demand, clearer indications of supplier performance in key business processes, such as risk management, to provide better criteria for supplier selection. One very strong indication of process performance can be established through capability assessments conforming to ISO/IEC 15504-2.

Many organizations have created integrated management systems and have requirements for combined assessments. This is particularly relevant when organizations are adopting closely related standards such as ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001. The benefits are clearly seen through easier deployment of processes, greater cost-effective maintenance and more efficient third-party assessments.

[1] Primarily through the TickIT Guide, TickIT Auditor Training Courses, Accredited Certification and the introduction of a 3-year Certification Cycle

TickIT*plus* addresses all these aspects through:

- defining a core set of well-defined processes that provide complete coverage for a range of organizational activities
- adopting graded levels of process capability assessment and a maturity approach based on ISO/IEC 15504-2
- providing mappings between the core processes and combinations of requirement and reference standards
- introducing the concept of having formally trained practitioners within an organization to support ongoing improvements, promote higher levels of process capability and benefit from closer involvement in assessments.

Forty processes have been defined. Collectively, they cover business, engineering, functional and support activities, and are contained within a database maintained by JTISC, called the BPL (Base Process Library). Processes are grouped into one of six defined categories, as described later in Figure 3.

TickIT*plus* defines five levels of maturity of an organization, consistent with the requirements stated within ISO/IEC 15504-2. These levels are, in ascending order, Foundation, Bronze, Silver, Gold and Platinum. Levels from Bronze to Platinum are progressed by determining whether an organization has complied with certain process attributes by means of capability assessments. Compliance at the Foundation level is determined by making sure that an organization has identified processes correctly and is operating those processes. It is recognized that existing TickIT organizations will want to progress through the graded levels at their own pace and as improvements allow. Consequently, the Foundation level exists to allow organizations to progress to TickIT*plus* with minimal effort and then start their process maturity journey.

The scheme has been designed to allow combinations of IT-related requirement and reference standards to be mapped into the BPL, which will initially include ISO 9001. As the scheme develops, further requirements and reference standards will be added according to demand, such as:

- ISO/IEC 20000-1, *Information technology — Service management — Specification*
- ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

- ISO/IEC 25030, *Software engineering — Software product quality requirements and evaluation (SQuaRE)*
- IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- BS 25999, *Business continuity management*.

These would then be mapped across to the existing or enhanced BPL processes. Past experience shows that far more internal auditing staff took part in TickIT training than registered auditors, and, apart from the certificates awarded at the end of the courses, they received no formal recognition. JTISC recognized the benefits to be gained by organizations having qualified practitioners and their importance in facilitating the uptake of the scheme and so it has formally defined the role of TickIT*plus* practitioner and aligned it with the training and development route for assessors. Thus, the practitioner is seen as providing an important contribution to organizational improvements and system assessments, and can, where appropriate, participate during formal assessments.

Identifying the certification scope and preparing resources

Once top management commitment and support has been obtained to progress towards TickIT*plus*, the first major activity involves identifying and defining the coverage, or scope, of TickIT*plus* and developing or securing the necessary resources to proceed.

There are three important scopes to be considered; firstly the organizational scope, secondly the certification scope and thirdly the TickIT*plus* scope. It is worth noting that many organizations will already have certified management systems, covered either generally under ISO 9001 or specifically under TickIT, and, as such, the need for determining scope will have already been considered.

The organizational scope represents the full range of organizational activities undertaken at all locations. The certification scope is determined by considering the products or services to be covered by certification, the activities undertaken and the locations to be included, as for existing certification schemes. By way of an example, take an organization that develops and manufactures peripherals for PCs, such as printers, scanners and plotters, and manufactures hard disks under licence. While many different organizational scopes are possible, a typical one might be as shown in Figure 1.

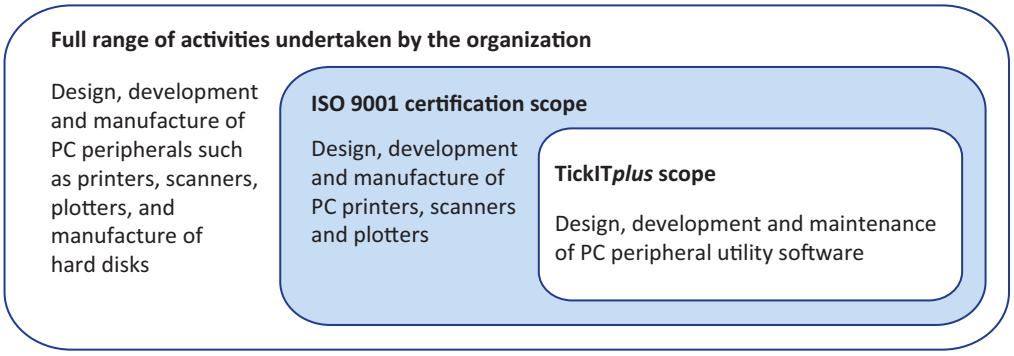

Figure 1: Hierarchy of scopes

In the example in Figure 1 the largest box represents the organizational scope, i.e. all the activities that the organization undertakes. The middle (shaded) box represents those parts of the business which are to be covered under an ISO 9001 certificate, and this is referred to as the certification scope. Finally the innermost box represents that part of the business which is to be covered under TickIT*plus* certification, the TickIT*plus* scope.

Next, it is necessary to consider which standards are to be referenced, the desired capability level and the selection of what is known as a Scope Profile that is applicable to the TickIT*plus* scope. In this introductory guide, only ISO 9001 at the TickIT*plus* Foundation level is being considered.

TickIT*plus* defines eight Scope Profiles that have been designed to cover a wide range of IT-related organizational activities, such as developing and maintaining systems and software, providing an IT-related service, or ensuring security in IT systems. Scope Profiles are pre-defined templates that simply define a group of interrelated processes in the BPL that are relevant to the TickIT*plus* scope chosen by the organization. The eight pre-determined Scope Profiles cover:

- Information Management and Security
- Service Management
- Systems and Software Development and Support
- Project and Programme Management
- Corporate Strategy Planning and Management
- Legal and Compliance
- Product Validation, Quality and Measurement
- IT Systems Engineering and Infrastructure.

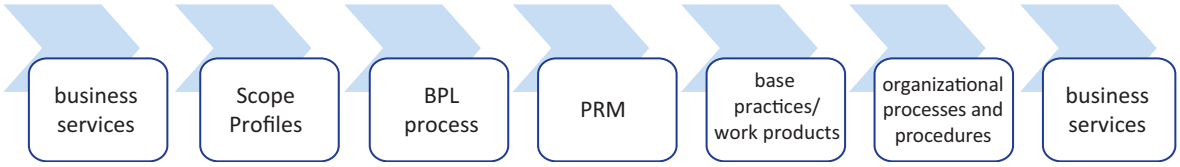

Figure 2: Flow from Scope Profile to business service

Figure 2 shows how Scope Profiles are selected on the basis of business services and how the relationships already described cascade through the organization back to the business services to be included in the scope of TickIT*plus*.

These eight Scope Profiles address all but the most specialized services undertaken by IT organizations.

For the organization shown in Figure 1, the Systems and Software Development and Support Scope Profile would probably be the most appropriate for the TickIT*plus* scope. However, it is possible to select more than one Scope Profile to cover, for instance, multiple business activities and/or standards. For example, if operating a support desk was also included in the example shown in Figure 1, or the organization was required to show compliance to ISO/IEC 20000-1, then the Service Management Scope Profile would also be included. However, describing this level of complexity is outside the scope of this guide, where the selection of only one Scope Profile is discussed.

By selecting a Scope Profile (or multiple Scope Profiles), the organization will then know which of the forty TickIT*plus*-defined processes need to be implemented to provide the desired process platform for business improvements. Figure 3 lists the forty processes and shows how they are assigned to the different process types and allocated to different categories.

The Type A mandatory processes are necessary for compliance with ISO 9001 and are required for all certified TickIT*plus* assessments.

Type B/C processes are referred to as scope dependent processes. Whether or not they are required depends on the selected Scope Profiles, the requirements and reference standards, and the certification scope. If required, they are designated Type B processes and are treated in the same way as Type A processes. If not required, they are designated Type C processes and are treated as supporting processes and included as necessary.

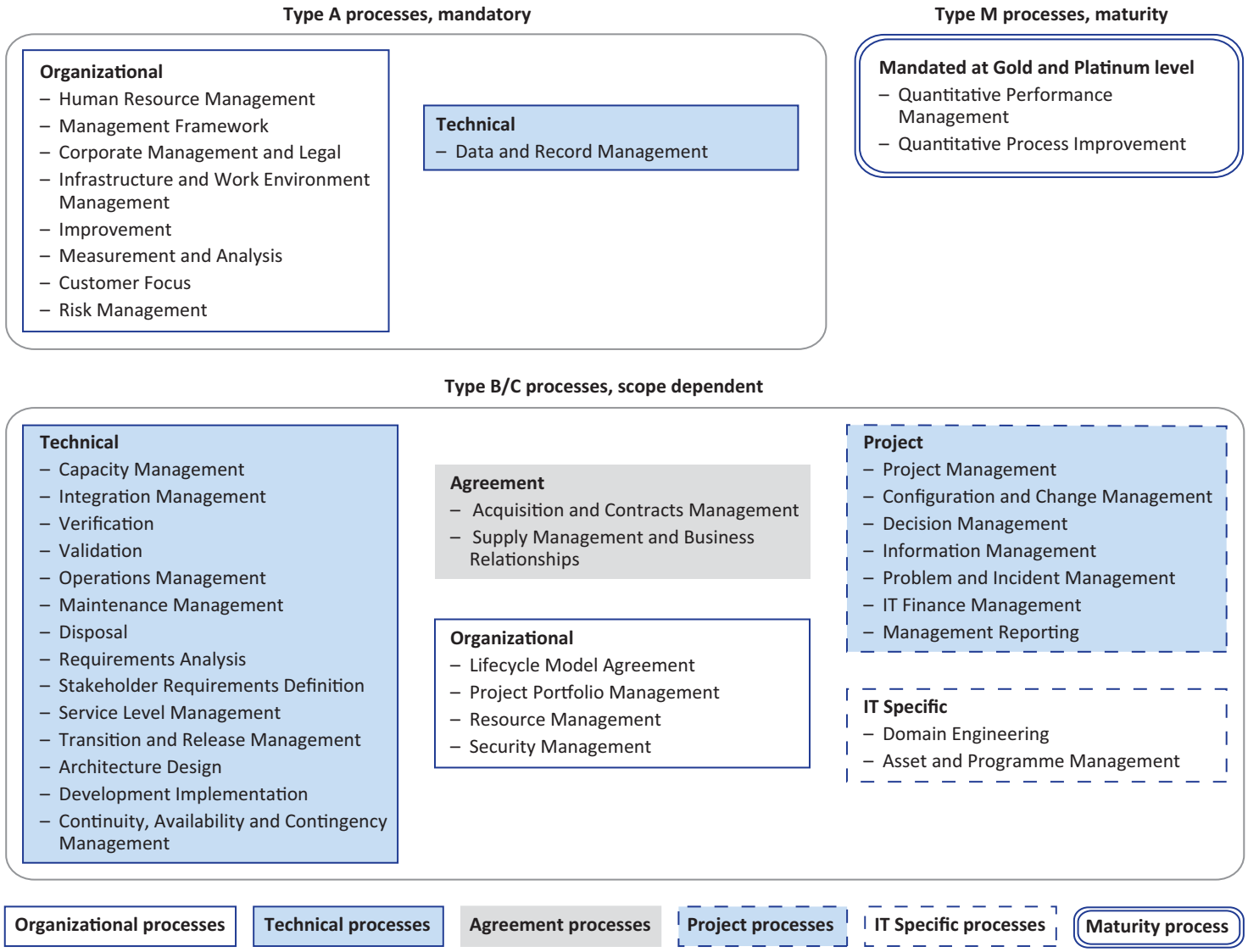

Figure 3: BPL processes

The Type M maturity processes are required only at the Gold and Platinum levels.

While there are a few other formalities that need to be addressed, such as crafting the exact wording for scope statements, which will typically be done jointly with the certification body, the initial work on scoping is now complete.

At this point, the organization should also consider which human resources and skills will be required to support the implementation of a TickIT*plus*-based certificated BMS (Business Management System). Having appropriately skilled resources has been identified as an important aspect within TickIT*plus*, hence the need to define TickIT*plus* practitioners. While an organization must actively involve a practitioner, they do not necessarily need to be a member of staff. Practitioners are required to have undergone similar training to TickIT*plus* assessors and they will be formally registered in the same way. Their role involves providing detailed support to an organization in implementing, internally assessing and preparing for formal external assessments. Under TickIT*plus* a practitioner can also be a member of the external assessment team, given some defined constraints and prerequisites.

Developing the Process Reference Model

The second major activity necessary for an organization to undertake in addressing the requirements of TickIT*plus*, is the development of a PRM (Process Reference Model). In effect, this is a data repository which allows the organization to relate the generic processes defined in the BPL, and which have been selected by means of the Scope Profile(s), to existing (or new) processes in the organization, i.e. those processes actually undertaken. In order to understand how this should be achieved, it is necessary to understand how the processes are constructed in the BPL.

Each BPL process is defined in terms of four elements. These are:

- the purpose
- one or more outcomes
- a set of tasks, called base practices, which must be performed if the process is to be fulfilled satisfactorily – they are also cross-referenced to relevant standards
- input and output work products.

Process ID: PRJ.1

Process name: Project Management

Process purpose: To ensure that the projects meet their objectives

Process outcome: The organization achieves project objectives in a controlled manner and delivery is on time, within budget and of the required quality

Process Base Practice		Input Work Products	Output Work Products	ISO 9001
PRJ.1.BP.1	**Establish Project Management Policies and Procedures**	Business Plan	Project Management Policies Project Management Procedures	4.2.1 d) 4.2.3
PRJ.1.BP.2	**Scope the Project**	Stakeholder Requirements	Scope Statement	7.2.1 7.2.2
PRJ.1.BP.3	**Plan the Project**	Scope Statement	Management Plan Project Schedule	7.3.1
PRJ.1.BP.4	**Initiate the Project**	Management Plan Project Schedule	Project Approval Record	
PRJ.1.BP.5	**Monitor and Control the Project**	Management Plan Project Schedule	Project Reports	7.3.4 7.5.1
PRJ.1.BP.6	**Manage Risks and Issues**	Risks Issues	Risks Issues	8.5.2 8.5.3
PRJ.1.BP.7	**Manage Changes to Project**		Change Request	7.2.2 b) 7.3.7
PRJ.1.BP.8	**Close the Project**	Management Plan Project Schedule	Closure Report Lessons Learnt Report Improvement Requests	8.4 8.5.1

Figure 4: Simplified example of a process in the BPL

In Figure 4, for example, the Project Management process has a defined purpose, a single process outcome, eight base practices and a number of associated work products. In most cases, there will be only one process outcome that usually addresses an ISO 9001 requirement, although some processes will have additional outcomes that either support further ISO 9001 requirements or cover other standards such as ISO/IEC 20000-1.

The process purpose statement provides a simple narrative of the intention of the process, i.e. what it is aiming to achieve.

The process outcome statement aims to provide a clear indication, expressed in observable terms, where appropriate, of what would be expected, desired or evident if the process was working fully and effectively. In many cases, the process outcome statement is defined as an end state, or ultimate goal but, in practice, this may not be demanded. However, the organization must have evidence to show that it is moving towards these goals, typically through audit results but more effectively through measurements.

For each process outcome, there are a set of pre-defined base practices. A base practice consists of a brief title referencing the intent of the practice along with some supporting mandatory requirements (for simplicity, the reference titles only are shown in Figure 4).

Supporting each base practice, where relevant, will be a number of work products that are defined in generic terms.

Finally, for each base practice, although again not in all cases, there will be one or more references to requirement standards, such as ISO 9001, and reference standards such as BS 25999.

Given that the BPL processes have to be written using generic terminology and language so as to be applicable to the many different organizations that might use them, a mapping or translation must be done to relate the generic processes to the organizational terminology and language, and this is achieved through the PRM. What is necessary, therefore, is to understand the processes that have been selected from the BPL by choosing the applicable Scope Profile and identifying, or if necessary creating, organizational processes, procedures and work products to match. Ideally there will be a one-to-one mapping, but this is not mandated and if needed, a one-to-many mapping can be adopted.

The PRM mapping between the BPL and the organization's BMS, quite frequently called the QMS (Quality Management System), is done at the base practice and work product level.

As an example of one-to-one mapping, the Management Framework process (ORG.2 in the BPL), has a base practice that requires audits to be scheduled and that the schedule is a defined output work product. The organization could simply reference its audit procedure, provided it included resources and controls, and audit plan or schedule against the BPL process requirements.

If, on the other hand, the Risk Management process (ORG.8 in the BPL) is considered and the organization identifies that it has two different risk processes, say one for project risk,

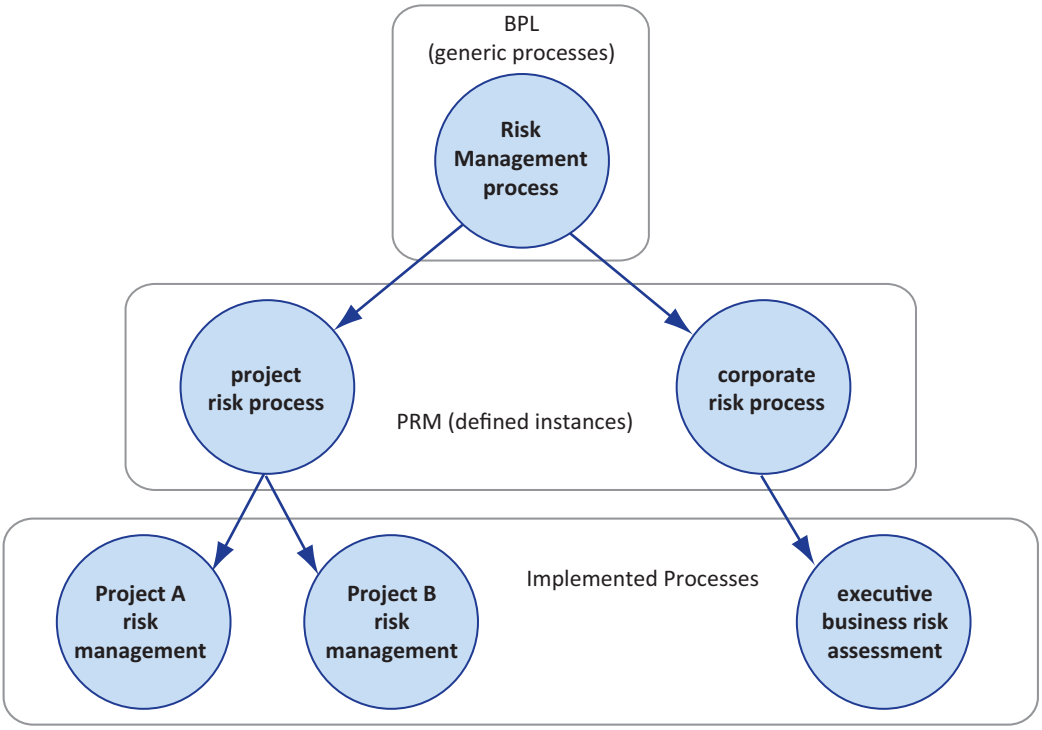

Figure 5: BPL to PRM mapping

and the other for business risk, the mapping would identify two procedures and possibly two identified output work products, hence the PRM would identify two defined process instances (see Figure 5). Having said this however, the organization could decide that having two separate procedures is not desirable, and rationalize the two procedures into one, giving a simpler system which is easier to deploy and maintain.

To conclude this part of the guide, the organization needs to identify a mapping between each of the base practices and work products for each in-scope outcome of each selected process, identified by selecting the Scope Profile against its actual processes, procedures and work products.

Preparing for, participating in and following up an assessment

The final part of this guide covers TickIT*plus* assessments and, in particular, what an organization must do to prepare for an assessment, how it may then be involved and what it

should do following an assessment. Although there are a number of different ways in which organizations may take up TickIT*plus*, for simplicity, this guide only considers those most likely to be adopted by organizations either starting or moving towards the scheme. Also, as mentioned earlier, this guide only addresses the initial Foundation level of TickIT*plus* and not the higher levels which involve capability assessments. It does, however, consider the two options that are available at the Foundation level, that of the transition assessment and the initial assessment. Transition assessments are only applicable to existing TickIT registered organizations that are within their three year certification period, i.e. the next visit is not a certificate renewal or reassessment visit.

While the main differences between these two options are in the way the assessment is actually conducted, as described later, there are a few differences that an organization needs to consider in preparing for an assessment and these will now be highlighted.

One of the first necessary activities is to select a certification body that is able to provide TickIT*plus* certification services. Once the certification body has been selected, and this should be done as soon as possible after deciding to progress with TickIT*plus* certification, there are a number of activities and events that need to be undertaken or completed and these are discussed in the remainder of this section. A general overview of these is shown in Figure 6.

The first activity that should be undertaken in preparing for an assessment is to create the Assessment Strategy, which will be updated and maintained for subsequent visits, e.g. surveillances or certificate renewals. TickIT*plus* identifies the need for an Assessment Strategy in order to provide a clear description of:

- the organization in terms of sites, products, activities, functions, size, etc.
- the hierarchy of scopes including exceptions and deviations
- the selected Scope Profile and capability level being sought
- the approach to implementing and monitoring improvements; an improvenment plan must be evident
- assumptions, constraints and other important information that affects or influences the assessment
- use of Type C supporting processes
- other organizational information that assists in planning the assessment.

After the creation of the Assessment Strategy for an initial assessment, only general maintenance should then be necessary.

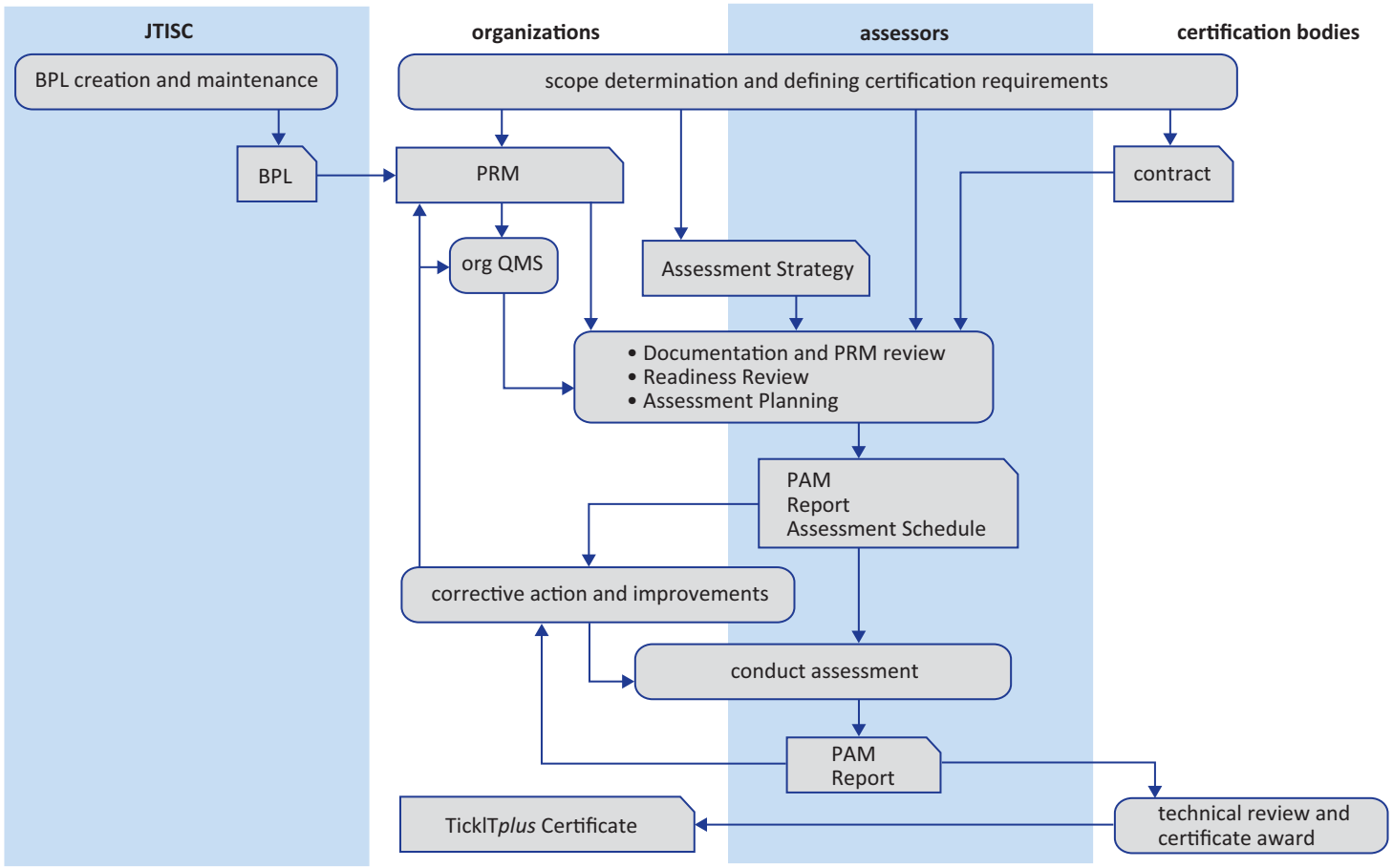

Figure 6: Assessment flow

The TickIT*plus* scheme documentation provides a sample template for the content of the Assessment Strategy, although any format can be used. The organization should complete the Assessment Strategy prior to the Documentation and PRM Review visit by the assessor from the certification body.

The Documentation and PRM Review is one of three events that have to be completed by the assessor prior to the formal assessment; the others being the Readiness Review and Assessment Planning. The duration, physical location and scheduling of these is not specified in the scheme, as they will depend entirely on specific organizational situations such as size, locations, complexity, standards and capability level being sought. In practice, examples could range from all three being completed in a one day remote review (in rare situations), through combinations of on- and off-site reviews over a number of days, to each one being covered over multiple on-site days.

The timing of these events will be dependent on the progress being made by the organization in preparing for the assessment but, in general, they will be undertaken sequentially in the following order: Documentation and PRM Review, Readiness Review and Assessment Planning. Clearly, there can be multiples of each of these, in which case the only stipulation over the total elapsed time is that the assessment must be started within six months of the Documentation and PRM Review and not more than three months after a successful Readiness Review.

The Documentation and PRM Review, best undertaken on site, might be the first contact between the organization and the assigned lead assessor from the certification body, unless, of course, the organization already has a TickIT certificate and a transition assessment is being undertaken. Much of this review will be similar to the existing documentation reviews conducted prior to a conventional audit but will also include additional activities, such as evaluating the PRM, the Assessment Strategy and improvement plans. For transition assessments, the review would normally only concentrate on the additional activities.

The Readiness Review is to ensure that the organization is ready to undergo an assessment. Specifically, it checks and evaluates that the organization has conducted internal assessments, has held management reviews, is implementing the improvement plans, is undertaking appropriate corrective actions, has implementation records controlled and available, and is complying with the arrangements as specified. The Readiness Review may be combined with the Documentation and PRM Review and, once again, it is highly recommended that it is conducted on-site. The Readiness Review for initial assessment at the Foundation level and for transitional assessments are the same.

Assessment Planning, as the name suggests, not only aims to produce a plan for achieving an effective assessment but also considers the surveillance schedule over the FCC (Full Certification Cycle), which normally lasts for three years. In essence, it is not too dissimilar to the audit planning that is undertaken as part of any certification audit, although there are specific sampling rules that have to be considered. This activity is undertaken primarily by the assessor, but with input from the organization. The assessor will make extensive use of the organizational Assessment Strategy to prepare the plan for the assessment.

The main factors driving the sampling rules are processes and process categories, and hence the Scope Profile, sites and staff, the locations where processes can be evidenced, i.e. the Implemented Process samples, and the method of assessment. The other main factor being considered by the lead assessor will be the skill requirements of the assessment team. This will accommodate skills around the Scope Profile, additional processes, requirement standards being used such as ISO 9001 or ISO/IEC 20000-1, any reference standards such as ISO/IEC 25030 and any specific or specialized activities of the organization, e.g. safety critical development.

There are rules on the minimum size of the assessment team for capability assessments, i.e. for Bronze level and above, but for Foundation level and transitional assessments, only a single external lead assessor is required.

Although not compulsory for Foundation level assessments, the organization may opt to use the services of a TickIT*plus* practitioner; either a full- or part-time employee or a contractor. The practitioner, with agreement from the lead assessor, can participate in the assessment team. However, there are a few limitations on the activities they can undertake. For example, they cannot raise nonconformities.

Other than for transitional assessments, there are two types of assessment methods used at Bronze level and above, the CMA (Confirmation Mode Assessment) and the EMA (Exploration Mode Assessment). Without going into too much detail, the differences between these two modes are around the amount of evidence that can be collected beforehand and the amount that needs to be sought out by the assessment team.

The organization needs to prepare for the assessment and the way in which the assessment will be conducted, ensuring that both are in accordance with the assessment plan, with or without practitioner involvement in the team. Much of the existing reporting will continue to be generated under the scheme, although there are new requirements for reporting on

the results of the capability assessments above Foundation level. The main tool used by the assessment team is the PAM (Process Assessment Model), but, as the organization has minimal involvement in its preparation, it is not discussed further in this guide. However, in essence, the PAM simply records the Implemented Process sampled, confirmation that the base practices and work products were checked and the ratings awarded to the process outcomes. It will also link any nonconformities raised and provide the basis for calculating the capability level of processes and the organizational maturity level.

Once the assessment has been completed, there may be a number of corrective actions or improvements that the organization will need to address. While the scheme does not specify the mechanics for undertaking this, it does require the use of an improvement plan to address these aspects.

So, what benefits can the organization expect from achieving Foundation level certification? Organizations that have already gone through transition assessment have been able to verify that they have all the processes and base practices that are required to conform to the relevant Scope Profiles in place. In many cases, important omissions have been identified and the necessary remedial actions then taken. The achievement of Foundation level also facilitates moving on to Bronze and higher levels of capability and hence opening up a path to continuing improvement and resultant benefits.

Apart from the information being freely available at www.tickitplus.org, further detailed guidance and additional information on certification can be obtained from the scheme documentation and certification bodies.

Abbreviated terms

BMS	Business Management System
BPL	Base Process Library
CMA	Confirmation Mode Assessment
EMA	Exploration Mode Assessment
FCC	Full Certification Cycle
JTISC	Joint TickIT Industry Steering Committee
PAM	Process Assessment Model
PRM	Process Reference Model
QMS	Quality Management System

Bibliography

BS 25999-1, *Business continuity management — Code of practice*

BS 25999-2, *Business continuity management — Specification*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

ISO 9001, *Quality management systems — Requirements*

ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*

ISO/IEC 15504 (all parts), *Software engineering — Process assessment*

ISO/IEC 15504–2, *Software engineering — Process assessment — Performing an assessment*

ISO/IEC 20000–1, *Information technology — Service management — Specification*

ISO/IEC 25030, *Software engineering — Software product quality requirements and evaluation (SQuaRE) — Quality requirements*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*