A Framework for Improving IT Service Continuity Management

Teduh Dirgahayu
Department of Informatics
Universitas Islam Indonesia, Yogyakarta, Indonesia
Tel: (+62) 274-895287, Email: teduh.dirgahayu@uii.ac.id

Ulya Anisatur Rosyidah
Department of Informatics
Universitas Muhammadiyah Jember, Jember, Indonesia
Tel: (+62) 331-336728, Email: ulyaanisatur@gmail.com

Abstract. IT service continuity management (ITSCM) is a process to ensure the availability and connectivity of information technology (IT) in an enterprise during interruptions. Available frameworks and literatures have recognised that ITSCM improvement is important, but they do not address ITSCM improvement in sufficient details. This paper proposes a framework that defines a set of activities to systematically formulate recommendations for improving ITSCM. The activities are taken from proven practices, i.e. (i) evaluation of process execution, (ii) root-cause analysis, (iii) risk assessment, and (iv) recommendation formulation. Also, the framework includes several tables for organising inputs, facilitating analysis, and defining outputs of those activities. The tables are concerned at execution findings, causes, risks, and recommendations. Risks and recommendations are defined from the technical and management perspectives. Risks and recommendations from the technical perspective, respectively, indicates potential harms that might happen to the enterprise IT and actions to mitigate those risks. Risks and recommendations from the management perspective are necessary to call for commitment and support from senior management. This paper includes an application of the framework in a case study in which a COBIT Quickstart process is used for ITSCM.

Keywords: IT service continuity management, business continuity management, risk management, improvement framework

1. INTRODUCTION

Enterprises nowadays depend greatly on information technology (IT) services. Their business hence becomes very risky to IT interruptions that can be caused by malicious attacks, human errors, utility disruptions, or natural disasters. In order to avoid or mitigate risks that are caused by such IT interruptions, enterprises have to develop their *business continuity plans* (BCPs) (Cerullo and Cerullo, 2004). A BCP is included in a management process called *business continuity management* (BCM) that identifies threats to the enterprise and their impacts to business operations and provides effective responses to those threats (Woodman, 2007).

While it concerns mainly on IT services, BCM is a business issue (Hecht, 2002). BCM is a process to ensure IT availability and connectivity during interruptions. It focuses on avoiding or minimizing the impacts of IT failures. Nevertheless, most BCM also addresses recoverability. As a process, BCM must anticipate changes and adapt with the organization (Hecht, 2002).

As it adresses IT service continuity, BCM can also be called *IT services continuity management* (ITSCM) (Ministr et.al, 2009). Frameworks and literatures on ITSCM have been provided (Botha and vol Solms, 2004; ISACA, 2012; ISO, 2012; Karakasidis, 1997; Lam, 2002; Quirchmayr, 2004; TSO, 2011). They list requirements, considerations, and guidelines for enterprises to conduct ITSCM. Those frameworks and literatures, however, do not address ITSCM improvement in sufficient details.

The objective of this paper is to propose a framework for improving ITSCM. The framework identifies *concepts* related to ITSCM improvement and defines *activities* that are necessary to do the improvement. It also provides a set of tables as a *tool* to facilitate a systematic analysis and to formulate recommendations for improving ITSCM.

This paper is further organized as follows. Section 2 presents related work on ITSCM. Section 3 proposes our improvement framework for ITSCM. Section 4 discusses the application of the framework on a case study. Finally, section 5 concludes this paper and identifies future work.

2. IT SERVICE CONTINUITY MANAGEMENT

Enterprises should conduct ITSCM to ensure their business continuity. ITSCM is a process that must anticipate and adapt to enterprise changes. Enterprises should also educate and make aware their employees of ITSCM (Hecht, 2002).

Several frameworks related to ITSCM have been proposed, e.g. COBIT (ISACA, 2012), ITIL (TSO, 2011a) and ISO 22301 (ISO, 2012). Some frameworks address a wider scope, e.g. IT governance or IT service management, in which IT service continuity management is a part of that scope.

COBIT is an IT governance framework (ISACA, 2012). In version 5, COBIT has 37 governance and management processes that are grouped into five domains, i.e.

1. evaluate, direct and manage (EDM),
2. align, plan and organize (APO),
3. build, acquire and implement (BAI),
4. deliver, service and support (DSS), and
5. monitor, evaluate and assess (MEA).

ITSCM is mainly addressed in process DSS04 (manage continuity). This process is focused on ensuring the continuity of critical business operations at an acceptable level when incidents and disruptions happen to IT service. Process DSS04 consists of eigth practices; each of which consists of several activities. The practices are

1. define a business continuity policy, objectives and scope,
2. maintain a continuity strategy,
3. develop and implement a business continuity response,
4. exercise, test and review the BCP,
5. review, maintain and improve the continuity plan,
6. conduct continuity plan training,
7. manage backup arrangement, and
8. conduct post-resumption review.

Each practice may require inputs from other process or organisational units, e.g. service level agreements (from APO09), risk assessment (from APO12) and a list of personnels that require trainings (from Human Resources Department). Its outputs can be used by other processes, e.g. business continuity policy (to APO01), incident response actions (to DSS02), and training requirements (APO07).

COBIT's practice for ITSCM improvement is defined in DSS04.5 (review, maintain and improve the continuity plan). Its activities are

1. review the continuity plan and capability,
2. consider whether a revised business impact assessment may be required,
3. recommend and communicate changes, and
4. review the continuity plan on a regular basis to consider the impact of new or major changes.

IT Infrastructure Library (ITIL) is a collection of best practices on IT service management (TSO, 2011a). It deals with five aspects of service lifecycle, i.e.

1. service strategy,
2. service design,
3. service transition,
4. service operation, and
5. service improvement.

ITIL addresses IT service continuity management thoroughly in service design. Its operation is then defined in service operation. The process of IT continuity management is focused on disastrous events, while less significant events are dealt with the process of IT incident management. Service improvement is a generic process to improve other processes in different aspects in the service lifecycle. It consists of seven steps (TSO, 2011b), i.e.

1. identify the strategy for improvement,
2. define target process to measure,
3. gather the data,
4. process the data,
5. analyse the information and data,
6. present and use the information, and
7. implement improvement.

ISO 22301 is a standard on BCM that specifies requirements to ensure that business recovers after IT interruptions (ISO, 2012). The requirements are of the organisational context, leadership, planning, support, and operations. This standard focuses on incident responses to ensure that the responses are conducted effectively. The standard also includes a improvement phase that consists of corrective actions and continual improvement. A corrective action is to address nonconformity by

1. identifying nonconformity,
2. reacting to nonconformity,
3. evaluate actions to eliminate the causes of nonconformity,
4. implementing necessary actions,
5. reviewing the actions' effectiveness, and
6. changing BCM, if necessary.

Continual improvement is to address suitability, adequacy, and effectiveness of BCM. No specific steps are defined.

Among the aforementioned frameworks, only ISO 22301 addresses ITSCM improvement. COBIT does not concern on the improvement at all. ITIL outlines practices for service improvement in general (TSO, 2011b), but does not specifically address ITSCM improvement.

Literatures on business continuity planning (Botha and von Solms, 2004; Karakasidis, 1997; Lam, 2002; Quirchmayr, 2004) have proposed approaches to ITSCM that are essentially similar to each other. None however puts attention on improving existing ITSCM. Botha and von Solms (2004) emphasises that ITSCM shall be reviewed regularly and updated to ensure that it stays effective. Karakasidis (1997) and Quirchmayr (2004) considered audit as a way to improve ITSCM. However, none gives further explanation on how the review and audit shall be conducted.

3. ITSCM IMPROVEMENT FRAMEWORK

Figure 1 depicts a set of concepts and their relationships in our improvement framework.

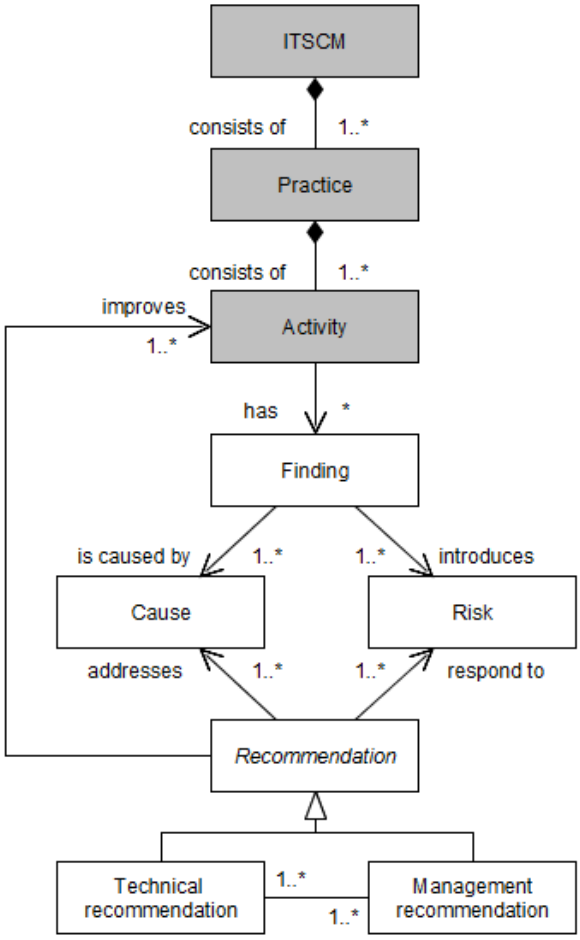

Figure 1: Concepts in our ITSCM improvement framework.

Our framework follows COBIT (ISACA, 2012) in three ways, i.e. (i) ITSCM is an IT management process, (ii) ITSCM consists of one or more practices, and (iii) a practice consists of one or more activities. In Figure 1, gray boxes represent ITSCM-related concepts.

Evaluation of ITSCM execution may result in one or more findings on the practices or activities. A finding can be conformity or nonconformity, i.e. ITSCM performance conform or does not conform, respectively, to the enterprise standards. Such standards can be internally established by the enterprise or be adopted from external standards (e.g. national and international standards). Our framework is focused on nonconformity findings as they are indicating that ITSCM is not conducted effectively.

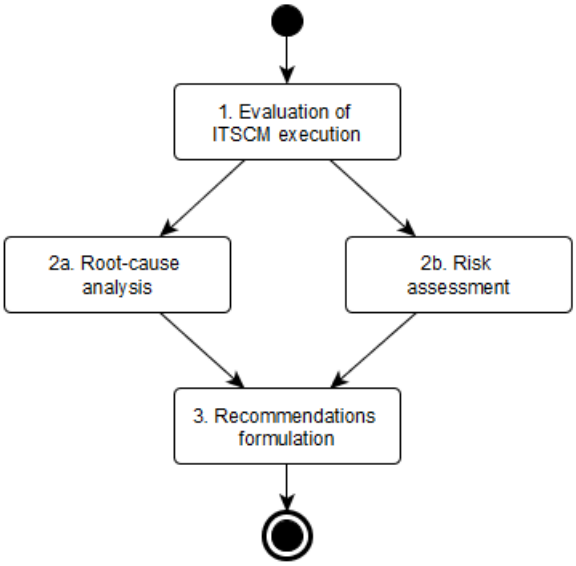

Figure 2: Activities in our ITSCM improvement framework.

A finding is caused by one or more causes that are found during ITSCM execution. A finding may introduce risks to the enterprise. Hence the enterprise should formulate recommendations to address those causes and to respond to those risks. Those recommendations should guide the enterprise to improve its ITSCM. A recommendation can be a technical or management recommendation. A management recommendation is associated with one or more technical recommendations; and vice versa.

In our framework, recommendations are formulated in detail at the level of ITSCM activities. By improving the activities, the related practices and the enteprise ITSCM, in general, will also improve.

Figure 2 depicts the activities in our framework. It starts with an evaluation of the execution of ITSCM practices and activities. When nonconformity findings are identified, a root-cause analysis are conducted to identify causes of the findings. Also, a risk assessment are conducted to assess potential risks that might be introduced to the enterprise by the findings. Their results are then considered to formulate the recommendations to improve the ITSCM execution. The recommendations should be formulated from both technical and management perspectives.

In addition, our framework provides a set of tables as a tool to facilitate systematic analysis and to formulate the recommendations. These tables are described below.

Table 1 is to document ITSCM practices and activities. It is also to record findings, both conformity and nonconformity, that we found on those practices and activities. In this way, we make sure that all practices and activities have been evaluated. A practice consists of one or more activities; each of which has associations with findings.

Table 1: Practices, activities, and findings.

Practices	Activities	Findings

Table 2 is to document the results of the root-cause analysis and risk assessment when nonconformity findings are found. A finding is associated with one or more causes and risks. Different findings can be caused by the same cause. The same cause however may introduce different risks depending on the practices and activities. Risk should be identified from both the technical and management perspectives.

Putting the results in one table by referring to the related findings would facilitate us in analysing the relation between causes and risks. When determining a recommendation as a risk response, we can know which causes have to be addressed.

Table 2: Causes and risks.

Findings	Causes	Risks

Table 3 is to list technical recommendations as risk responses to nonconformity findings. Different findings may have the same recommendation as they can be caused by the same cause. A finding is associated with one or more recommendations. The recommendations shall improve the ITSCM activities.

Table 3: Technical recommendations.

Findings	Technical recommendations

Table 4 is to formulate management recommendations from technical recommendations listed in Table 3. This is done by abstracting a number of similar technical recommendations and considering their business context. The management recommendations are necessary to call commitment and support from the top management for the ITSCM improvement.

Table 4: Management recommendations.

Technical recommendation	Management recommendations

4. CASE STUDY

As a case study, we applied our framework on ITSCM in a higher-education institution in Indonesia. We focused on IT service for academic administration. Data was collected by interviewing with key persons, i.e. policy maker (vice rector for academic affairs), business process owner (head of academic administration office), and IT executive (chief of IT operation). The application of the framework is described in the following.

4.1 Activity 1: Evaluation of ITSCM execution

The institution in our case study has implemented process DS4 of COBIT Quickstart (ITGI, 2007a) as its ITSCM. We evaluated the execution of that process.

COBIT Quickstart structures its ITSCM process into a number of control objectives; each of which consists of a number of activities. Several control objectives are grouped into management practices. Therefore we had to map this structure into our concepts first.

As depicted in Figure 3, the ITSCM conducted by the institution of the case study is process DS4 of COBIT Quickstart. The practices are the control objectives within process DS4. The activities are the activities of those control objectives.

Process DS4 consists of 10 control objectives that are grouped into three management practices. These management practices are not mapped to any concepts in our framework as they do not define any ITSCM activities. The management practices and the control objectives (ITGI, 2007a) are listed in Table 5.

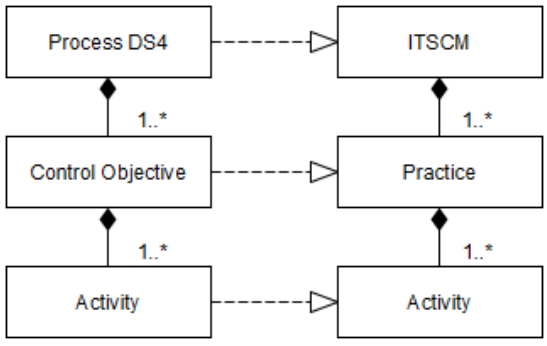

Figure 3: Mapping ITSCM process in COBIT Quickstart to the concepts of our framework.

Table 5: Control objectives are grouped into management practices.

No	Management practices	Control objectives
1	Identify critical business functions and informations […]	DS2.1, DS4.1, DS4.3
2	Establish basic principles of safeguarding and reconstructing IT services […]	DS4.2, DS4.8
3	[…], define what needs to be backed up and stored offsite to support recovery of the business […]	DS4.5, DS4.9, DS11.3, DS11.4, DS11.5

Due to space limitation, this paper describes the evaluation of and recommendations for several control objectives only. Our intention is to show the use of our framework, instead of a complete list of findings, causes, risks, and recommendations from the case study.

COBIT Quickstart refer to COBIT 4.1 (ITGI, 2007b) for the definitions of the control objectives. A COBIT 4.1 control objective does not list explicitly its activities. Instead, it gives a descriptive statement of the control objectives. For example, control objective DS4.9 (Offsite Backup Storage) is described as "*Store offsite all critical backup media, documentation and other IT resources* […]. *Determine the content of backup storage* […]. *IT management should ensure that offsite arrangements are periodically assessed* […]. *Ensure compatibility* […] *and periodically test and refresh archived data*" (ITGI, 2007b).

From that statement, we identified three activities in control objective DS4.9, i.e.

1. store offsite all backup media;
2. determine the content of backup storage; and
3. assess periodically the offsite backup.

During the evaluation of ITSCM execution, the activities and their results were confirmed. The practices, activities, findings are listed in Table 6. Note that the table contains selected practices and activities only due to space limitation. Discussion on the next subsections refer to the nonconformity findings listed in this table (these findings are printed bold).

4.2 Activity 2a: Root-cause analysis

We conducted a root-cause analysis to identify the causes of the findings. The causes should be specific and controllable by management (Rooney and vanden Heuvel, 2004). In this way, they allow us to formulate recommendations. A finding may have several causes. Table 7 lists the causes of the findings.

Table 6: Findings in ITSCM execution in the case study.

Practices	Activities	Findings
DS4.2 IT continuity plan	Define roles and responsibility for IT continuity	**Defined partially**
	Develop alternative processing capability	Exists
DS4.8 IT service recovery and resumption	Develop business continuity plan	Embedded in business owner' documents
	Define recovery time objectives	**Not available**
DS4.9 Offsite backup storage	Store offsite all backup media	Exists
	Determine content of backup storage	Available on a dedicated database server
	Assess periodically offsite backup	**Never**

Table 7: Causes and risks in the case study.

Findings	Causes	Risks
Roles and responsibility for IT continuity are partially defined	Limited knowledge on roles and responsibility in IT continuity management	Some IT interruptions will not be handled or recovered completely
		Business may involve invalid data
		Business operation may be unable to predict
Recovery time objectives are not available	Limited knowledge on time objectives in IT continuity management	Business will not be back into operation in predicted time
Offsite backup is never assessed periodically	No standard procedure is available	Data lost or corruption might be undetected
		Backup might be unable to restore
		Business can fail as necessary data is not available

4.3 Activity 2b: Risk assessment

We conducted a risk assessment to identify and estimate risks that may be introduced by the findings (NIST, 2010). A finding may introduces a number of risks. The risks are also listed in Table 7.

The risks should not only identified from the technical perspective, but more importantly also from the management perspective. This will make business executives aware of the risks and their impacts to business. For example, the unavailability of standard procedures for assessing offsite backup storage periodically will lead to business failure when necessary data are not available after IT interruptions.

4.4 Activity 3: Recommendations formulation

We took the identified causes and risks in Table 7 into consideration when we formulated technical recommendations to improve process execution. For each finding, we proposed one or more recommendations as listed in Table 8. These recommendations indicate detailed corrective actions to improve ITSCM execution. These technical recommendations are coded with prefix TR.

These detailed actions requires commitment and support from the top management to be executable. Therefore the actions need to be formulated in such a way, so they are understandable from the management perspective. This was done by making abstractions from the technical recommendations.

Table 8: Technical recommendations in the case study.

Findings	Technical recommendations
Roles and responsibility for IT continuity are partially defined	TR1. Educate personnels who are responsible for developing IT continuity plan
	TR2. Define roles and responsibility completely in a collaboration with business process owners
	TR3. Educate all personnels about the roles and responsibility
Recovery time objectives are not available	TR4. Educate personnels who are responsible for developing IT continuity plan
	TR5. Define recovery time objective in IT continuity plan
Offsite backup is never assessed periodically	TR6. Define a standard procedure for periodic backup assessment
	TR7. Assign responsibility to at least two personnels for backup assessment
	TR8. Educate dan train all personnels

Table 9: Management recommendations in the case study.

Technical recommendations	Management recommendations
TR5. Define recovery time objectives in IT continuity plan	MR1. Development of IT service continuity plan (procedures and objectives)
TR6. Define a standard procedure for periodic backup assessment	
TR2. Define roles and responsibility completely in a collaboration with business process owners	MR2. Definition and assignment of roles and responsibility in IT service continuity
TR7. Assign responsibility to at least two personnels for periodic assessment	
TR1, TR4. Educate personnels who are responsible for developing IT continuity plan	MR3. Personnels education on IT service continuity
TR3. Educate all personnels about the roles and responsibility	
TR8. Educate dan train the personnels	

For example, TR1, TR3, TR4, and TR8 are all about personnel education on IT service continuity. They are abstracted into a management recommendation MR3. Table 8 list the management recommendations (coded with prefix MR).

4.5 Remarks

The complete results of the application of our framework inform us that many nonconformity findings were found in the ITSCM of the institution of our case study. Therefore the ITSCM still has to be much improved to ensure the continuity of the IT service. While the institution claimed that they have already implemented ITSCM, the findings indicates that some ITSCM fundamentals, e.g. definition of recovery time objectives, periodic assessment of offsite backup, and responsibility assignment, are not yet implemented.

IT service interruptions cannot be avoided in entirety since it is inherent risks. These risks however can be accepted within the enterprise risk tolerance (NIST, 2010). Recovery time objectives define enteprise risk tolerance. They are hence must be defined as part of the IT continuity plan. This plan shall include a procedure for periodic backup assessment to ensure that the backup can be restored in time after IT interruptions. Also, it shall include the assignment of roles and responsibility to the persons that will be in charge during IT

interruptions. The enterprise is responsible to educate them so that they have sufficient knowledge on ITSCM.

We formulated technical and management recommendations as listed in Table 8 and 9. These recommendations are necessary to be implemented as responses to mitigate the identified risks. We can thus expect that the enterprise ITSCM will also improve.

5. DISCUSSION

The importance of ITSCM improvement are mentioned in COBIT 5, ITIL, and ISO 22301. We define detailed steps of activities that can be used in those frameworks or standard. Table 10 is a mapping from the activities of our framework to those frameworks and standards. It indicates which activities are mentioned in those frameworks and standard. Again, no detailed step is defined in those frameworks and standard.

Table 10: Mapping activities of our framework to COBIT, ITIL and ISO 22301

Activities of our framework	COBIT 5	ITIL	ISO 22301
Evaluation of ITSCM execution	+	+	+
Root-cause analysis	-	+	+
Risk assessment	+	-	-
Recommendation formulation	+	+	+

\+ : mentioned
\- : not mentioned

Some activities, steps or actions in those frameworks and standard, however, are not accomodated in our framework. Those activities are concerned on communication (COBIT); improvement strategy and implementation (ITIL); and implementation (ISO 22301). Our framework is focused on formulating recommendations, instead of their implementation.

Risk analysis or business impact analysis is an integral part in ITSCM (Botha and von Solms, 2004; Cerullo and Cerullo, 2004; Lam, 2002). In this analysis, risks are identified and analysed so that their impacts to business become clear. Enterprise can then decide the appropriate responses to the risks based on the analysis results.

6. CONCLUSIONS

In this paper, we have defined an improvement framework for IT service continuity management. We have applied the framework in a case study. The result have shown us that the framework can be used to effectively formulate technical and management recommendations to improve the ITSCM in the case study.

Although our improvement framework adopts the structure of a COBIT 5 process, it can be used to improve other ITSCM. In this paper, we have shown the use of our framework for improving ITSCM that implements COBIT Quickstart process.

We have learned that our improvement framework is generic enough to be implemented in other areas of IT management. Our future work will validate this claim and incorporate approaches from ITIL's service improvement.

ACKNOWLEDGMENTS

This work was supported by Universitas Muhammadiyah Jember. The authors thank to Universitas Islam Indonesia for supporting the publication of the work.

REFERENCES

Botha, J., and von Solms, R. (2004) A cyclic approach to business continuity planning. *Information Management & Computer Security*, **12**(4), 328-337.

Cerullo, V. and Cerullo, M.J. (2004) Business continuiting planning: a comprehensive approach. *Information Systems Management*, **21** (3), 70-78.

Hecht, J.A. (2002) Business continuity management, *Communication of the Association of Information Systems*, **8**, 444-450.

ISACA (2012) *COBIT 5: A business framework for governance and management of enterprise IT*. ISACA.

ISO (2012) *ISO 22301. Societal security – business continuity management systems – requirements*. ISO.

ITGI (2007a) *COBIT Quickstart 2nd edition*. IT Governance Institute.

ITGI (2007b) *COBIT 4.1*. IT Governance Institure.

Karakasidis, K. (1997) A project planning process for business continuity. *Information Management & Computer Security*, **5**(2), 72-78.

Lam, W. (2002) Ensuring business continuity. *IT Pro*, May/June, 19-25.

Ministr, J., Števko, M., and Fiala, J. (2009) The IT service continuity management principle implementation by method A2. *Proceedings of the Interdiciplinary Information and Management Talks*, 131-140.

NIST (2010) *Guide for applying the risk management framework to federal information systems: a security life cycle approach*. NIST Special Publication 800-37 revision 1, NIST.

Quirchmayr, G. (2004) Survivability and business continuity management. *Proceedings of the 2nd Workshop on*

Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation, 3-6.
Rooney, J.J., and vanden Heuvel, L.N. (2004) Root cause analysis for beginners. *Quality Progress*, 45-53.
TSO (2011a) *ITIL service operation*. Crown.
TSO (2011b) *ITIL continual service improvement*. Crown.
Woodman, P. (2007) *Business continuity management*. Chartered Management Institute.