Assessment and continuous improvement of information security based on TQM and business excellence principles.

Andrei Ioan Hohan, Marieta Olaru, Ionela Carmen Pirnea

University of Economic Studies, Bld. Dacia no.41, Bucharest, 010404, Romania
University of Economic Studies, Bld. Dacia no.41, Bucharest, 010404, Romania
Constantin Brâncoveanu University, Calea lui Traian Street, no.39, Rm. Vâlcea, Romania

Abstract

This paper highlights a part of the results of a doctoral research regarding information security management systems in the context of business excellence conducted by authors in the Research Centre of Business Administration of The Bucharest University of Economic Studies, Romania. It focuses on an approach for self-assessment and continuous improvement of information security based on the fundamental concepts and criteria of the European Foundation for Quality Management (EFQM) Business Excellence Model. The first objective of this paper is to highlight the state of the art regarding the approaches used for the assessment and continuous improvement of information security. A second objective is to propose a methodology for assessment and continuous improvement of information security integrating the criteria of the EFQM Model and its RADAR (Results, Approaches, Deploy, Assess and Refine) logic. The methodology presented can be used by organisations wishing to go beyond compliance with the requirements for Information Security Management System defined in standards such as ISO 27001 or NIST standards, to identify opportunities for improvement and to coordinate efforts towards sustainable information security performance.

Keywords: information security; total quality management; business excellence; self-assessment; continuous improvement; EFQM Model

* Corresponding author. Tel.: +4-021-3121347; fax: +4-021-3122106
E-mail address: andreihohan@gmail.com.
1. Introduction

In a changing environment, the success of an organization has become closely related to its ability to manage risks. As companies become more and more dependent on information for their competitive advantage and information gains even greater proportion in the value added embedded in companies’ products and service, the ability to protect valued and sensitive information has become a strategic ability to ensure enterprise sustainability, profitability and overall value of an enterprise. The increasing variety of threats and ferocity attacks make the protection of information assets a complex challenge. (Knapp, et al., 2010)

Ensuring information security becomes a necessary condition for the sustainable progress of the organisation at least for the following reasons (Buszta, 2010):

- Maintaining competitive advantage
- Protect reputation
- Ensure compliance with applicable laws and regulations

Yet a study conducted by Ponemon Institute among IT security professionals reveal that, as a rule, senior leadership does not view information security as a strategic priority, and, although resources, policies, procedures and technologies are in place as a result of compliance projects, they are not complemented by a shared culture of security aimed at engaging staff and resources in protecting information as a means to support the achievement of the organisation’s strategic goals. (Ponemon Institute LLC, 2012)

The first stone at the foundation of an effective security culture is defining a shared vision for security and clear goals, aligned with the organisation’s overall strategy (ISACA, 2011). This can be achieved through the use of the proposed methodology, based on the European Foundation for Quality Management (EFQM) model for business excellence, aimed at reconciling business and security objectives, to coordinate efforts towards sustainable security performance and to enable knowledge and best practice sharing. Integrating information security activities with organisational objectives and obtaining the commitment of top management for information security is a necessary (although not sufficient) condition to ensure the necessary resources and the effectiveness of information security activities. (Knapp et al., 2010).

Taking into account the above, the authors of the research have pursued the following objectives:

- to identify the state of the art regarding the approaches used for the assessment and continuous improvement of information security;
- to develop a methodology for assessment and continuous improvement of information security integrating the best practices of information security and the principles of total quality management.

To achieve the first objective, the authors have reviewed the existing literature, ranging from Plan-Do-Check-Act (PDCA)-based, audit approaches to process maturity / capability models and to continual improvement approaches based on total quality management principles.

To achieve the second objective, the research has built on the research conducted by Martin, Clemens and Bulkan (2011) to extend the total quality management and business excellence philosophies in order to create a new security excellence approach. The proposed methodology associates business excellence criteria, used to drive and measure the progress of the organisation towards sustainable performance, with the necessary security controls needed to safeguard information, assets and operations.

2. Research, methodology and results

The research has started with the analysis of existing literature on the use of self-assessment for continual improvement of information security management. Three main directions were investigated: auditing techniques and methodologies, as a driver for continual improvement inside the Plan-Do-Check-Act cycle for continuous improvement; process maturity/capability models as a driver for achieving compliance with requirements; total quality management approaches, aimed at driving performance in line with organisational
strategy and objectives. The research has focused on the strong points of all studied approaches, in order to identify the elements of a blended approach, based on information security and management systems best practices and on total quality management principles.

To achieve the second objective, the authors have correlated the Enabler criteria in the EFQM model for business excellence with information security best practices from widely-used references such as ISO and NIST (U.S. National Institute for Standards and Technologies) standards, at the same time using the RADAR (Results, Approaches, Deploy, Assess and Refine) logic built in the EFQM model to structure the self-assessment approach and the underlying continuous improvement process.

The resulting methodology was tested in the context of an information security management system implemented in an agency of the Romanian public administration.

3. Research results regarding the approaches for the assessment and continuous improvement of information security

Several approaches are proposed for the assessment and continuous improvement of information security. The reference standard for information security – ISO/IEC 27001:2013 (ISO, 2013), uses the established Plan-Do-Check-Act approach to drive continuous improvement. In this approach, auditing is the managerial tool which provides stakeholders with reasonable confidence in the achievement of organizational goals (ISACA, 2010). The modern approach of audit goes beyond identification of non-conformities to requirements and audit findings are, alongside monitoring of processes and performance metrics, one of the main drivers of continual improvement of an information security management system.

This approach has a major drawback: audit focuses mainly on compliance with policies and best practices, and thus misses opportunities for proactive improvement aimed at reaching a state of security excellence. (Hohan et al., 2011; Hohan et al., 2014)

Furthermore, the effectiveness of audit as a driver for improvement is heavily dependent on the auditor’s personal skills and the quality of the process. A study, (Steinbart et al., 2012) argues that the benefits of audit depend on various factors ranging from the auditors technical knowledge and manner of audit (favouring counselling over policing), to top management support and organisational attributes such as regulatory environment or effectiveness of internal communication.

Maturity evaluation models are a structured sets of criteria that describe the capability of an organisation’s behaviours and processes to produce the desired results in a reliable and sustainable manner (ISO, 2008). Maturity can be used as a benchmark for comparison and as a tool for understanding best practices and achieving compliance with a set of requirements. (Sava et al., 2011) Ge, Yuan and Lu (2011) identify three complementary models for assessing security maturity: the International Standards Organisation’s Systems Security Engineering Capability Maturity Model (ISO, 2008), the federal information security technology assessment framework (NIST, 2013) and the Control Objectives for Information Technology – COBIT (IT Governance Institute, 2007).

The Security Engineering Capability Maturity Model (ISO, 2008) focuses on security practices and evaluates maturity by means of their reliability and sustainability, ranging from informal practices to defined, controlled and continuously improving practices.

The NIST Guide for Assessing Security Controls (NIST, 2013) focuses on policies, procedures and technical controls, and their implementations; maturity evaluation starts at definition of general rules and responsibilities (policies); at top maturity level, policies, procedures and controls are implemented, tested and improved on a regular basis, and IT security is embedded into corporate culture and everyday practices.

ISACA’s Control Objectives for Information Technology – COBIT (IT Governance Institute, 2007) focuses on risk management; information security maturity is appraised by the capability of the associated risk management framework; at basic level, risks are considered and dealt with in an ad hoc manner; at top maturity
level, risk management is a structured, organisation-wide and well-managed process, and IT security is integrated with corporate security business objectives.

The Open Information Security Management Maturity Model (Open Group, 2011) takes the maturity evaluation approach further by defining a comprehensive security process framework, with processes spanning different levels of organization governance: Generic Processes, Strategic Management, Tactical Management, Operational Management. It also defines process metrics used to assess process performance. Its definition of maturity levels is defined as a specific selection of processes in place and effective in the organisation.

Maturity / capability models clearly define a pathway to a mature information security system, but they lack in alignment with the overall organizational strategy and objectives and they are useful until a certain level of compliance with a set of rules or best practices is reached, such as a company, legal or third-party standard. After compliance is achieved, and information security is “mature”, the well of improvement goes dry and new tools are needed to seek continuous improvement and proactive alignment of security posture to new security challenges and requirements. Furthermore, the validity of the conclusions drawn from maturity assessments and the effectiveness of the incurred actions are directly influenced by the appropriateness of the reference – the set of rules, requirements and/or best practices – for the organisation and its context.

<table>
<thead>
<tr>
<th>Security Maturity Model</th>
<th>Maturity levels</th>
<th>Focus theme</th>
<th>Top maturity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Objectives for Information Technology – COBIT (IT Governance Institute, 2007)</td>
<td>0-5</td>
<td>Risk management</td>
<td>Optimized: Risk assessment as a structured, organisation-wide and well-managed process. Integration of IT security with corporate security business objectives</td>
</tr>
<tr>
<td>Information security technology assessment framework - NIST 800-53 (NIST, 2013)</td>
<td>1-5</td>
<td>Policies, procedures, controls</td>
<td>Integration: Continuous review and improvement of policies, procedures and controls. Integration of IT security into corporate culture and practices</td>
</tr>
<tr>
<td>Open Information Security Management Maturity Model (Open Group, 2011)</td>
<td>Initial, Managed, Defined, Controlled, Optimized</td>
<td>Processes</td>
<td>Specific per category of process. Definition of processes on highest level (optimized) include specific practices for implementation, testing, monitoring, planning, realisation of benefits, assessment and optimisation (continuous improvement) of the process.</td>
</tr>
</tbody>
</table>

Sources: (NIST, 2013; IT Governance Institute, 2007; ISO, 2008; Open Group, 2011)

Martin, Bulkan and Klempt (2011) argue that the plethora of standards and guidelines for information security management, the organisations face a difficult task in selecting the right mix of reference documents to drive the development and operation of an information security management system that balances regulatory compliance and reduction of risk exposure with cost optimisation and boosting organisational performance. While the choice of guidelines/standards is influenced by the organisational context and by subjective factors, the variety of references makes benchmarking of security in various environments or organisations difficult to accomplish.

The proposed approach, adopted and taken further in our research, is to link security metrics and underlying controls and processes to Enablers and Results Criteria in the EFQM Model for Business Excellence and use the RADAR logic to drive continuous improvement.

Such approach can bring further benefits in contexts in which compliance with several references is needed. In such a context a unifying approach is needed, one that can harmonize multiple models, leveraging synergies, mitigating differences and optimising resource allocation. The resulting integrated approach can take advantage
of the strengths of each model, in order to reap maximum possible benefits for the organisation (Pardo et al., 2013)

4. Research results regarding the use of the EFQM Model and its RADAR (Results, Approaches, Deploy, Assess and Refine) logic for continuous improvement of information security

The EFQM Model is a management framework that enables organizations of all types and sizes to assess their progress on the path to business excellence, helping them identify key strengths and shortcomings in relation to best practices and to their vision and mission. In several organizations, this Model is used to integrate management tools and methods into a holistic framework aimed at supporting the organizations goals (European Foundation for Quality Management, 2012; Olaru et al., 2010).

The EFQM model integrates three components:

- The fundamental concepts of excellence set of underlying principles, based on a set of European values, originating in the European Convention on Human Rights and the European Social Charter, laying the essential foundation for achieving sustainable excellence in any organization ((EFQM, 2012)
- The Excellence Model itself, a reference framework structured in 9 criteria that can be used to assess and direct the organization’s initiatives and results towards excellence. The 5 “Enabler” criteria cover the approaches of the organization, whereas the 4 “Results” criteria offer a balanced framework to assess organizational results
- The RADAR logic, and evolution of the Plan-Do-Check-Act cycle for continuous improvement offers a structured approach to reviewing organisational the performance, but also lays the foundation of a systematic continuous improvement process, as illustrated in Figure 1.

Fig. 1. Using the RADAR logic as basis for a continuous improvement process. Source: adapted from (Cucu, M., 2011)

Using the RADAR logic, the organisation validates that: It identifies the Results to be achieved to support its strategy
- It plans and fosters a suite of sound and coherent approaches to deliver the identified results on short and long term
- It implements the approaches in a systematic manner
- It assesses and refines the implemented approach using systematic monitoring and analysis activities and continuous learning from internal and external experiences. (EFQM, 2012)

The proposed methodology follows the RADAR logic to define and assess the maturity of approaches used and to structure improvement projects. Starting from the desired results stated in the Information Security Policy, information security approaches are planned and developed by mapping existing reference frameworks against the Enabler criteria of the EFQM Model, as presented below.

A possible definition of a management framework is that of a hypothetical description of a collection of processes aimed at providing guidelines for understanding and deploying it. (Ericsson et al., 2010)


<table>
<thead>
<tr>
<th>Enabler</th>
<th>Information Security Excellence</th>
<th>Reference frameworks</th>
<th>Primary reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security leadership</td>
<td>Excellent organisations have leaders who define the need for information security for the overall success of the organisation and make things happen, leading by example and inspiring trust throughout time. They are flexible, and drive of culture of risk awareness, enabling the organisation to anticipate and mitigate risks in a timely manner to ensure sustainable success.</td>
<td>EFQM Model (Leadership criteria); COBIT 5 Enabler - Culture, Ethics and Behaviour; ISO 27001:2013;</td>
<td>EFQM Model</td>
</tr>
<tr>
<td>Policy and Strategy</td>
<td>Excellent organisations develop an Information Security Strategy fully aligned with the Mission and Vision of the organisation. They develop and implement sound and integrated policies, objectives and processes to deliver the strategy.</td>
<td>ISO 27001:2013 - 4,5,6; EFQM Model; COBIT 5 Goals Cascade</td>
<td>COBIT 5 Goals Cascade</td>
</tr>
<tr>
<td>Partnerships &amp; Resources</td>
<td>Excellent organisations fully understand the impact of external partnerships, suppliers and internal resources on the effective operation of processes, and continuously calibrate security controls with the identified risks and opportunities</td>
<td>ISO 27001:2013; BSI IT Grundschutz; COBIT 5 Enabler: Services, Infrastructure and Applications</td>
<td>ISO 27001:2013</td>
</tr>
<tr>
<td>People</td>
<td>Excellent organisations drive a culture of risk awareness and security consciousness that protects company assets and objectives as well as personal privacy, liberties and interests. They develop a culture of security for the benefits of people and not against it. Security behaviours are communicated, rewarded and recognised, motivating people, building commitment and making full advantage of their skills and knowledge in support of achieving organisational goals.</td>
<td>ISO 27001:2013; COBIT 5 Enabler: People, Skills and Competencies; NIST Special Publication 800-50</td>
<td></td>
</tr>
<tr>
<td>Processes and Services</td>
<td>Excellent organisations design, manage and improve security processes to manage risks, ensure compliance and generate increasing value for stakeholders.</td>
<td>ISO 27001:2013; COBIT 5 Process Reference Model; NIST Special Publication 800-53; Open Information Security Management Maturity Model</td>
<td>ISO 27001:2013</td>
</tr>
</tbody>
</table>

Sources: (EFQM, 2012), (ISACA, 2012), (ISO, 2013)
The research has piloted a 6-steps methodology to information security self-assessment, based on the RADAR logic, aimed at driving innovation and laying the basis of continual improvement of information security based on total quality management leadership. The methodology is summarized in Table 3.

<table>
<thead>
<tr>
<th>Self-assessment step</th>
<th>Information sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Identify Information Security Excellence Approaches</td>
<td>See table 2</td>
</tr>
<tr>
<td>2 Are approaches properly implemented and effective?</td>
<td>Audit results, security incidents</td>
</tr>
<tr>
<td>3 Is there a system of processes to deploy approaches?</td>
<td>Functioning ISMS, according to ISO 27001</td>
</tr>
<tr>
<td>4 Security metrics are defined, updated and relevant, to monitor implementation and effectiveness?</td>
<td>Objectives, metrics, monitoring procedures, effectiveness of continual improvement triggered by monitoring. Use RADAR logic to assess relevance and usability of existing data</td>
</tr>
<tr>
<td>5 Is the evidence of proactive improvement, learning and innovation?</td>
<td>Cooperation with third parties, effectiveness of risk assessments, improving returns on security investments, effectiveness of improvement actions</td>
</tr>
<tr>
<td>6 Is information security performance improving sustainably?</td>
<td>Assessment of metrics using RADAR logic: positive trends (at least 3 consecutive years), existence of appropriate targets being achieved, appropriate comparisons and benchmarks, evidence of effective management of security drivers to prove the organisational capability to sustain performance in the future</td>
</tr>
</tbody>
</table>

The developed methodology was used as a basis for the independent review and continuous improvement processes at the core of the information security management system implemented in a Romanian public administration that processes vast amounts of sensitive, personal data, and that has information security deeply rooted in its organisational objectives and culture. The information security management system has passed the test of external certification against the ISO 27001 standard, and has succeed in driving management and employee commitment and aligning security and organisational objectives.

The methodology can be also used by any type of organisation wishing to go beyond compliance with the requirements for Information Security Management System defined in standards such as ISO 27001 or NIST standards, to identify opportunities for improvement and to coordinate efforts towards sustainable information security performance.

5. Conclusion

In an ever faster changing environment, the ability of organisations to turn information security management into competitive edge is closely linked to its continuous improvement capabilities. The PDCA cycle at the core of the information security management system sets the framework for continual improvement, driven mainly by monitoring processes and independent review (audits). Maturity / capability models clearly define a pathway to a mature information security system that be used both as a tool for understanding best practices and as a benchmark to evaluate progress in implementing such best practices and achieving compliance with a set of requirements, but they fail to connect security with the overall organizational strategy and objectives.

In order to go beyond compliance and aim towards information security excellence, more sophisticated tools that foster innovation and creativity and that align information security with organisation-level strategies are needed. This paper proposes a methodology based on total quality management principles that associates the EFQM’s business excellence criteria with information security processes and adapts the RADAR logic to drive innovation and continuous security improvement. The methodology was piloted in the context of implementing
an information security management system in a Romanian public administration and has proven effective in building a culture of security and driving proactive improvement.

The research results can be used by organisations wishing to go beyond compliance with the requirements for Information Security Management System defined in standards such as ISO 27001 or NIST standards, to identify opportunities for improvement and to coordinate efforts towards sustainable information security performance.

References


Cucu, M., 2011. Self-organization with the Excellence Model and RADAR Matrix for continuous improvement, Bucharest, FiaTest.


Hohan, A., Olaru, M., Pirnea, I.C., 2011. Case study regarding the implementation of an integrated risk management system in local public administration, Quality access to success Journal, II, 125, pp.246-251.


Sava, T., Moisa, C., Langa, C., 2011. Study on promoting social responsibility by SMEs in order to ensure sustainable performance, Economy Transdisciplinariness Cognition Journal, XIV, 1, pp.73-80.


ISACA, 2012, COBIT®  5. A business framework for the governance and management of enterprise IT, USA.

IT Governance Institute, 2007 CoBIT 4.1, Framework, Control Objectives, Management Guidelines, Maturity Models, pp 175-176

