# Secure e-Government Services: Towards A Framework for Integrating IT Security Services into e-Government Maturity Models

Geoffrey Karokola, Stewart Kowalski and Louise Yngström
Department of Computer and Systems Sciences
Stockholm University/Royal Institute of Technology
Forum 100, SE-164 40 Kista, Sweden
Tel: +46 (0)8 16 1697, Fax: +46 (0)8 703 90 25
E-mails: {karokola, stewart, louise}@dsv.su.se

*Abstract*— **e-Government maturity models (eGMMs) lack security services (technical and socio/non-technical) in its critical maturity stages. The paper proposes a comprehensive framework for integrating IT security services into eGMM critical stages. The proposed framework is a result of integrating information security maturity model (ISMM) critical levels into e-government maturity model (eGMM) critical stages. The research utilizes Soft Systems Methodology (SSM) of scientific inquiry adopted from Checkland and Scholes. The paper contributes to the theoretical and empirical knowledge in the following ways: firstly, it introduces a new approach that shows how government's can progressively secure their e-government services; secondly, it outlines the security requirements (technical and non-technical) for critical maturity stages of eGMM; and thirdly, it enhances awareness and understanding to the governments and stakeholders such as practitioners, experts and citizens on the importance of security requirements being clearly defined within eGMM critical stages.**

***Keywords— e-Government, Information Security, Maturity Model, Security Requirements, Technical and Non-technical Security aspects***

## I. INTRODUCTION

Dependency on Information and Communication Technology (ICT) for supporting core operations to both government and private sector is increasing [5]. Similarly, organization's critical information has developed into a key strategic asset in a competitive world [23]. Nevertheless, the pace of ICT advancement such as development, deployment and use of e-government infrastructures[1] is much faster than the development and deployment of security services, including technical and socio/non-technical [5]. As a result government organizations appear to suffer from the existing and new emerging security risks [8, 21]. Technical security aspects include hardware and software solutions such as Access control and Antivirus mechanisms [10, 15, 16]. Non-technical security aspects include ethical and cultural norms, legal and contractual frameworks, administrative and managerial policies, operational and procedural guidelines, and awareness programmes [1, 7, 8, 9, 13, 14, 22, 23]. Security is a quality issue driven by a set of objectives [11]. It is imperative that confidentiality, integrity and availability of critical information being stored, processed, and transmitted between e-government domains be enhanced [8, 9, 10, 11, 15].

In light of the above, there are several models called "e-Government Maturity Models (eGMMs)" developed by the international organizations, consulting firms, academia, and individual researchers with the purpose of guiding and benchmarking stage-wise e-government systems implementation and service delivery [7, 8]. A maturity stage in eGMM reflects the level of e-government maturity; degree of technology complexity; degree of systems sophistication; and the level of interaction with users. Also, it offers governments the abilities to measure the progress of e-government implementation [7, 8, 26]. However, the findings from a comparative analysis of eGMMs [8] show that the models were designed with main foci on functionalities. They rather measure quantity of e-government implementation and service delivery than quality – hence lack aspects of security services (technical as well as non-technical).

On the other hand, there are a number of Information Security Maturity Models (ISMMs) developed by the international organizations, consulting firms, academia, and individual researchers with main foci on offering security services to the organisations. ISMMs are defined as the structured collection of security elements that describe different maturity levels in the organization. Maturity levels are meant for describing different levels of technology and security sophistication that help organizations to easily identify and understand existing security gaps; monitor the progress of security implementation, practices, policies and quality; and monitor security investment, management and organizational audit [3, 4, 9, 11, 25]. Despite the fact that these models rather measure quality than quantity of services offered, they also lack much of non-technical security services [9].

[1] e-Government is defined as "A government-owned or operated systems of information and communication technologies that transform relations with citizens(C), the private sector (B) and other government agencies (G) so as to promote citizens' empowerment, improve government efficiency…" [26].

Therefore, given the fact that eGMMs lack aspects of security services in its critical stages [7, 8], in this paper, we attempt to integrate an ISMM [9] as a qualitative metrics of security into eGMM [8] which is based on quantitative metrics of e-government services, and propose a framework for integration IT security services into eGMM critical stages. The framework will address both the quality of security and the quantity of e-government services.

The reminder of the paper is organized as follows: section two presents the research approach; section three proposes the framework. Section four presents discussion and research contribution. Finally, conclusion and further research direction is given in section five.

## II. Reseach Approach

The research approach used in this study is based on the Soft Systems Methodology (SSM) of scientific inquiry/ learning cycle adopted from Checkland and Scholes [19]. The methodology was chosen because it can be used to extensively analyze complex situations in its real-world settings. Moreover, the model is designed such that it forms repetitive cycles of scientific inquiry until the real-world situation is improved. The approach phases are: *Reflection, Planning, Action,* and *Observation*. Based on the nature and magnitude of this study, the above mentioned phases were employed throughout the entire research process.

*The reflection phase* involved understanding of the magnitude and complexity of the real world problem. Being part of the on-going research work – the identified problem in the real world settings was lack of security services (technical and non-technical) in e-government maturity models (eGMMs) [7, 8].

*The planning phase* involved conducting an extensive literature review to explicitly understand the magnitude of the security problem identified above, and the possible security measures. Also, it involved building a knowledge-base using existing documents, theories, methods and structures. Finally, it was observed that adoption of the concepts of information security maturity models (ISMMs) seemed to be the appropriate approach towards mitigating the above identified security issue. Therefore, criteria for ISMMs identification and selection were prepared. Also, procedures for the models' analysis were developed, and the appropriate ISMM was identified [9]. In addition, integration processes for the identified ISMM [9] into eGMM [8], including strategies for enhancing security services for the new model was prepared. Further, general system theory [20] was chosen for providing detection and sufficiently deterrent measures for security issues and challenges posed to e-government services (information security target (IST)[2] and its operating environment (OE)).

*The action phase* involved implementing the above plans. Identified ISMM critical levels were integrated into eGMM critical stages as shown in figure 1, table II and figure 2. In addition, generic security requirements for the lowest and highest critical stages of eGMM were developed as depicted in Annex 1 and II. The security requirements development, matching and testing processes involved a group of 43 Masters and 5 PhD students in the area of Information and Communication Systems Security (ICSS) from the department of computer and systems sciences, Stockholm University/Royal Institute of Technology, in Sweden. The development process utilizes existing security standards and best practices documents [2, 11, 12, 17, 24]. Some are made part of this paper as Annex III, IV, V and VI.

*The observation phase* is one of the most important phases. Comparison and establishment of relationship between the knowledge-base and reality of the research problem was established. The outcome is shown in figure 1 & 2 and Annex I & II. This stage marked end of cycle 1. We repeated the process until we were satisfied with our research findings. Validation and verification of research findings (for the proposed model) to the earlier studied organizations [6] is scheduled to be conducted at the later stage.

## III. The Proposed Framework

This section presents the proposed comprehensive framework for integrating IT security services into eGMM critical stages. Based on the previous studies, the section begins by introducing the identified *critical stages* of the eGMM [8] followed by the identified *critical levels* of the ISMM [9]. Finally, the proposed framework is presented.

### *A. The Identified Critical Stages of e-Government Maturity Model (eGMM)*

The following were the identified eGMM critical stages [8]:

*Maturity Stage 1 – Web-presence:* this is the initial stage where communication is one way. Government disseminates information to the citizens via static websites. Information is accessible online – mostly basic and limited options to citizens, including reports and publications.

*Maturity Stage 2 – Interaction:* this is the advanced stage of maturity stage 1. Government provides enhanced interactive websites with more capabilities. Websites are used as tools for interaction between government and citizens. Available services include search engines, documents downloading, filling forms online, chart rooms, and emails.

*Maturity Stage 3 – Transaction*: this is the third stage, enhanced with more sophisticated technologies. Citizens (users) can conduct complete on-line transactions of values. Available services include taxes assessment and payment, such as paying of licenses and permits fees.

*Maturity Stage 4 – Transformation:* this is the advanced and more enhanced stage than stage 3. Government operational processes are integrated, unified, and personalized. Government systems are integrated at different levels between central, regional and local governments – vertically and horizontally. Available services include centralized government's human resources and payroll system.

*Maturity Stage 5 – Continuous Improvement:* this is assumed to be the highest stage of e-government systems

[2] In this context, IST reffers to security requirements for the given information system or product in question [2, 11].

implementation and service delivery. More sophisticated technologies are used to enhance government service delivery and interaction with citizens. Government involves citizens in decision making and democratic processes activities such as political participation and online voting.

### *B. The Identified Critical Levels of Information Security Maturity Model (ISMM)*

The following were the identified ISMM critical levels [9]:

*Maturity Level 1 – Undefined:* this is the lowest maturity level of information security model meant for organizations with low information security targets (IST) in a low security risk environment – where process metrics are not compulsory. Security policies may be available. Adequate user awareness is necessary. Security risk reduction from technical and non-technical security threats occur.

*Maturity Level 2 – Defined:* is the second maturity level meant for organizations with normal information security targets (IST) in a normal security risk environment. Process metrics may be used but not compulsory. At this level, security policies including awareness, visions, and strategies are reviewed and updated. More security risk reduction from technical and non-technical security threats occurs. Information security is slowly imbedded into organization culture.

*Maturity Level 3 – Managed:* this is the more advanced level than level 2. It is meant for organizations with high information security targets (IST) in a normal or high security risk environment. Also, high risk reduction from technical and non-technical security threats occurs. At this level process metrics may be used. In addition, security policies including awareness, visions, and strategies are regularly reviewed and updated.

*Maturity Level 4 – Controlled:* is the fourth maturity level of information security model meant for organizations with higher information security targets (IST) in a normal or higher security risk environment. Highest security risk reduction from technical and non-technical security threats occur. Uses of process metrics are compulsory. Information security is embedded into the culture of the organization. Additionally, Security policies, awareness, visions, and strategies are regularly reviewed and updated.

*Maturity Level 5 – Optimized:* this is assumed to be the highest maturity level. It is meant for organizations with higher information security targets (IST) in higher security risk environment. Highest security risk reduction from technical and non-technical security threats occur. Uses of process metrics are compulsory. Like in the previous maturity level – security policies, awareness, visions, and strategies are regularly reviewed and updated. Information security is embedded into the culture of the organization.

### *C. The Proposed Framework for Integrating IT Security Services into eGMM Critical Stages*

Based on the model's theoretical foundation and concepts presented above – we integrate ISMM [9] into eGMM [8] and propose a comprehensive framework for integrating IT security services into eGMMs so as to have a secured e-government maturity model (SeGMM). To achieve that we followed the following steps:

*Step one:* we arranged the ISMM critical levels on the X – axis and eGMM critical stages on the Y – axes. Then we mapped each critical maturity level to the critical maturity stage, this is seen in figure I. Furthermore, figure I allows two interpretations: (i) each of the maturity stage can ideally reach the highest maturity level "optimised". This is presented as capital letters (E, J, O and T) in the *progression* between one stage to another; (ii) in totality for eGMM to reach the highest stage of the critical maturity level (for its security) – security requirements for each of the critical maturity stages may need to be developed progressively from "Undefined" to "Optimized", we name this as *maturity sub-levels*. This is presented as capital letters (A – E, F – J, K – O, P – T, and U – Y) in the continuum within stages. These maturity levels and stages depicted in figure I are all in ordinal scales.

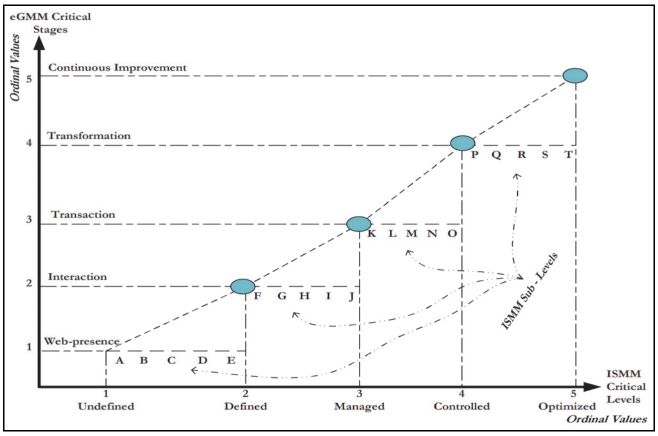


Figure 1. Integration of ISMM critical levels into eGMM critical stages

Further, we present the above interpretation into a tabular form as shown in table I below. The table introduces one aspect of maturity stages in relation to security in maturity levels. All maturity levels are divided into technical "*referred to as Te"* and socio/non-technical *"referred to as So"* security requirements.

*Step two*: to effectively identify security requirements for each maturity stage of eGMM – we integrate the maturity sub-levels, presented as capital letters in figure 1 "A – Y", into maturity stages. Table I below shows the integrated maturity sub-levels of ISMM into maturity stages of eGMM.

TABLE I. MATRIX SHOWING INTEGRATION OF ISMM SUB-LEVELS INTO EGMM STAGES WITH TECHNICAL (TE) AND NON-TECHNICAL (SO) SECURITY REQUIREMENTS - TRANSLATED FROM FIGURE 1

| **ISMM** | **Maturity Levels are divided into Technical (Te) and Non-technical (So) Security Requirements** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **eGMM** | **Undefined** | | **Defined** | | **Managed** | | **Controlled** | | **Optimized** | |
| **Maturity Stages** | **Te** | **So** | **Te** | **So** | **Te** | **So** | **Te** | **So** | **Te** | **So** |
| Web-presence | A | | B | | C | | D | | E | |
| Interaction | F | | G | | H | | I | | J | |
| Transaction | K | | L | | M | | N | | O | |
| Transformation | P | | Q | | R | | S | | T | |
| Continuous Improvement | U | | V | | W | | X | | Y | |

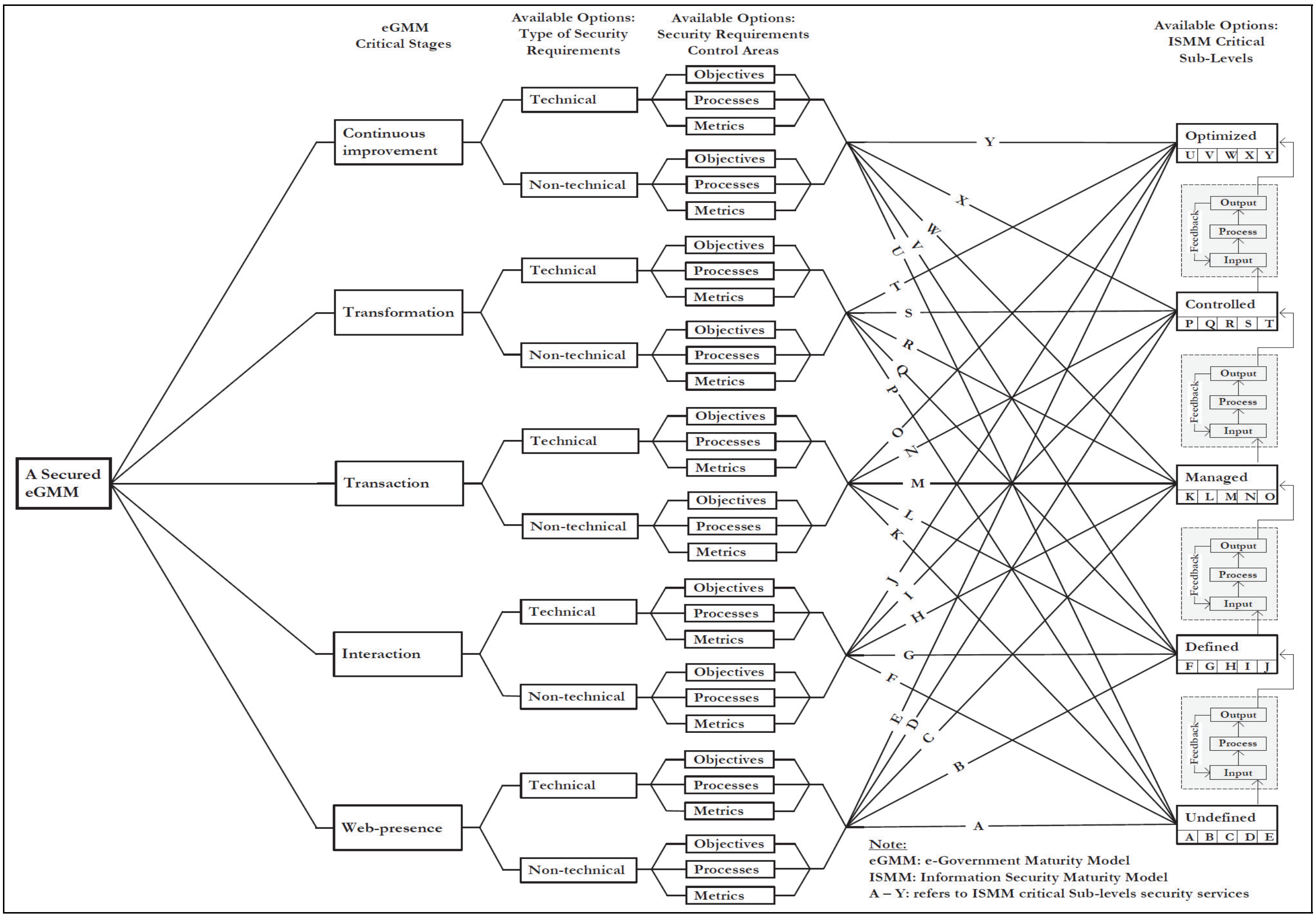
*Step three:* to comprehensively integrate security requirements/services into maturity stages of eGMM – we identify the *Security requirements control areas (SRCA)* required at each of the maturity sub-levels. The identified security requirements control areas were: *Security Objectives (Requirements), security processes and assurance patterns,* and security *metrics assessment* [2, 11, 12, 18, 24]. *Security objectives* refer to intent to achieve confidentiality, integrity and availability of services*; Security processes and assurance patterns* refer to activities that define information security implementation practices and confidence*;* and *security metrics* refer to indicators which provide qualitative and quantitative measures of security maturity.

Additionally, to accommodate the identified security requirements control areas within a table - we need to introduce additional three rows for each maturity stage. Then we insert the identified *security requirements control areas* into the table and arrange them accordingly as shown in table II.

TABLE II. DETAILED MATRIX SHOWING INTEGRATION OF THE SECURITY CONTROL AREAS INTO EGMM STAGES AND ISMM SUB-LEVELS

<table>
<tr><th>ISMM<br>eGMM</th><th colspan="10">Maturity Levels are divided into Technical (Te) and Non-technical (So) Security Requirements</th></tr>
<tr><th></th><th colspan="2">Undefined</th><th colspan="2">Defined</th><th colspan="2">Managed</th><th colspan="2">Controlled</th><th colspan="2">Optimized</th></tr>
<tr><th>Maturity Stages</th><th>Te</th><th>So</th><th>Te</th><th>So</th><th>Te</th><th>So</th><th>Te</th><th>So</th><th>Te</th><th>So</th></tr>
<tr><td rowspan="4">Web-presence</td><td colspan="2">A</td><td colspan="2">B</td><td colspan="2">C</td><td colspan="2">D</td><td colspan="2">E</td></tr>
<tr><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td></tr>
<tr><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td></tr>
<tr><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td></tr>
<tr><td rowspan="4">Interaction</td><td colspan="2">F</td><td colspan="2">G</td><td colspan="2">H</td><td colspan="2">I</td><td colspan="2">J</td></tr>
<tr><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td></tr>
<tr><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td></tr>
<tr><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td></tr>
<tr><td rowspan="4">Transaction</td><td colspan="2">K</td><td colspan="2">L</td><td colspan="2">M</td><td colspan="2">N</td><td colspan="2">O</td></tr>
<tr><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td></tr>
<tr><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td></tr>
<tr><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td></tr>
<tr><td rowspan="4">Transformation</td><td colspan="2">P</td><td colspan="2">Q</td><td colspan="2">R</td><td colspan="2">S</td><td colspan="2">T</td></tr>
<tr><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td></tr>
<tr><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td></tr>
<tr><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td></tr>
<tr><td rowspan="4">Continuous improvement</td><td colspan="2">U</td><td colspan="2">V</td><td colspan="2">W</td><td colspan="2">X</td><td colspan="2">Y</td></tr>
<tr><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td><td colspan="2">Objectives</td></tr>
<tr><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td><td colspan="2">Processes</td></tr>
<tr><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td><td colspan="2">Metrics</td></tr>
</table>

Additionally, to facilitate understanding of the above table – we transform it into pictorial presentation shown in figure 2 below.



Note:
eGMM: e-Government Maturity Model
ISMM: Information Security Maturity Model
A – Y: refers to ISMM critical Sub-levels security services

Figure 2. A Simpliefied Framework Showing flow Processes for Integrating IT Security Services from ISMM critical levels into eGMM Critical Stages

Figure 2 above shows a simplified framework for integrating IT security services from ISMM critical sub-levels into eGMM critical stages, named "*A Framework for integrating IT Security Services into eGMM critical stages"*. In the figure, the second column presents critical maturity stages of eGMM, the third column presents available options for security requirements (technical and non-technical), and the fourth column presents the security requirements control areas. The last column gives the available options for selecting security requirements from the ISMM critical maturity sub-levels.

*Step four:* Based on the general system theory [20] we treated our security problem in e-government (eGMM critical stages) as an open system that interacts with its environment (operating environment). An *open system* refers to systems which its boundaries permit flows of information in and out of the system. It consists of inputs, processes and outputs [20]. From figure 2 above, the security requirements patterns (technical and non-technical), i.e Web-presence maturity stage, could ideally progressively be from undefined, defined, managed, controlled to optimised sub-levels of ISMM referred to (in capital letters) as A, B, C, D and E respectively. This suggests that the security requirements for upper sub-levels build from the lower sub-levels. Meaning that output from the lower sub-level, after being processed, became an input to upper sub-level. This is shown in figure 2, last column, the under ISMM critical sub-levels.

*Step five:* we developed a comprehensive generic security requirements patterns listing for the identified maturity sub-levels, for the lowest (Web-presence) and highest (Continuous improvement) critical maturity stages of eGMM, depicted as Annex 1 and II respectively. In the Annexes, the first column presents the ISMM sub-levels; the second column presents the security requirements areas denoted as technical *"Te"* and non-technical *"So";* and the third column depicts the security requirements control areas pattern, namely security objectives, security processes and assurance, and security metrics. Further, the fourth column shows the detailed description of the security requirements/services for both technical and non-technical. The last column presents mapped security requirements activities referenced from Annex III, IV, V and VI.

Further, the security requirements development, matching, and testing processes involved a group of 43 Masters and 5 PhD students in the area of Information and Communication Systems Security (ICSS) from the department of computer and systems sciences, Stockholm University/Royal Institute of Technology, in Sweden. It is important to note that most of the referenced security patterns were adopted from the existing security standards and best practices documents. Some are made part of this paper in a summarised form as Annex III, IV V and VI.

## IV. Discussion and Research Contribution

Secure e-government services can effectively be achieved by ensuring that both technical and non-technical security requirements are adequately addressed. Also, security should be built-in from the beginning and should not be applied at the later stages [10, 14]. In this regard, we developed a comprehensive framework for integrating IT security services into eGMM critical stages. The framework is the result of integrating information security maturity model (ISMM) critical levels into e-government maturity model (eGMM) critical stages as shown in figure 1, 2 and table II. Also, based on the analysis (descriptive and analytic statistics) of the collected data, we developed generic security requirements for the lowest and highest e-government maturity stages i.e Web-presence and continuous improvement depicted as Annex I and II respectively. However, due to paper space limitations, detailed data analysis on the development of security requirements and preliminary testing processes are not shown here. It is important to note that organization may not sequentially follow all five security maturity sub-levels when implementing and delivering e-government services. This will depend much on, at least, the following: the security maturity level of an organisation at that particular time, and the complexity and technological sophistication of e-government system to be implemented.

We are of the view that this is one of the earlier studies that proposes this approach. The approach can stimulate the current trends of research in the area "secure e-government services". Therefore, using the proposed framework government's organizations can achieve at-least the following:

- Clearly understand, define and implement both e-government services and security requirements (technical and non-technical) in the correct order; maximize measures of quantity of e-government services against quality of security services; and consequently offers better and secure e-government services.
- Applying the model as a checklist for identifying, developing and implementing e-government security requirements;
- Easily identify, establish and plan for security requirements of a given e-government services projects - prior, during and after its implementation, consequently avoiding under or over protecting particular e-government services (security target); and
- Enable organisations to position and ranks themselves for the maturity stages of e-government services against respectively security measures that are in place, and to plan for security maturity enhancement.

## V. Conclusion and Further Research Work

In conclusion, comprehensive security measures that address both technical and non-technical security requirements for securing e-government services are critically needed. this will enable governments to efficiently and effectively mitigating emerging e-government security challenges in a constantly increasing risk environment. In the paper, we developed a comprehensive framework for integrating IT security services into eGMM critical stages shown in figure 2. The framework addresses both technical and non-technical security aspects. The framework provides an approach by which government's organization can achieve secure e-government services. Further research work will include testing and validating the proposed framework into one of the earlier studied government organizations [6].

## REFERENCES

[1] A. Martins, & J. Eloff, “Information security culture”. Proceedings of IFIP TC11, 17th international conference on information security (SEC2002) Cairo, Egypt (2002).

[2] CC. “The Common Criteria - PART1V3.1R3, PART2V3.1R3 and PART3V3.1R3”, (2009), [Available at http://www.commoncriteriaportal.org/, Last accessed February, 2011].

[3] D. Chapin, & S. Akridge, “How can security be measured?” (2005), Information system control journal, volume 2.

[4] Fraunhofer, “Security Maturity Model (SMM)”, Institut Software und Systemtechnik, Germany (2002), [Available at http://www.isst.fraunhofer.de/Images/Jahresbericht_2002_tcm8123346.pdf, Last accessed March, 2011].

[5] G. Dhillon, “Challenges in managing Information Security in the millennium”, Idea Group Publisher pp. 1-8, (2000), ISBN: 978-1-87828-978-0.

[6] G. Karokola, & L. Yngström, "State of e-Government Development in the Developing World: Case of Tanzania – Security View". Proceedings of the ICEG 2009, 5th International Conference on e-Government. Boston, USA, (2009b), ISBN: 978-1-906638-49-8.

[7] G. Karokola, & L. Yngström, “Discussing e-Government Maturity Models for the Developing World – Security View”. Proceedings of the 8th ISSA 2009 conference on Information Security, Johannesburg, South Africa, pp. 81-98, (2009a), ISBN: 978-1-86854-740-1.

[8] G. Karokola, L. Yngström, & S. Kowalski, “A Comparative Analysis of e-Government Maturity Models for Developing Regions: The Need for Security Services”. Unpublished paper – submitted to the International Journal of Electronic Government Research (IJEGR) - IGI, (Aug. 2010).

[9] G. Karokola, S. Kowalski, & L. Yngström, “Towards an Information Security Maturity Models for Secure e-Government Services: A Stakeholders View”. Proceedings of the 5th HAISA2011 Conference, London, UK, pp. 58–73, (2011), ISBN: 978-1-84102-284-0.

[10] G. McGraw, “Software Security” Addison-Wesley software security series, ISBN: 978-0-321-35670-3 (2005).

[11] ISM3 Consortium. “Information Security Management Maturity Model, Consortium version 2.10”, (2007), [Available at http://www.ism3.com/, last accessed September, 2010].

[12] ISO-27K, ISO 27002 (2005) [Available at http://www.iso27001security.com/html/iso27000.html, Last accessed September, 2009].

[13] K. Henry, “The human side of information security” – information security handbook, 5th edition Boca Raton, London, New York, Washington, DC (2004).

[14] L. Yngstrom, “A Systemic-Holistic Approach to Academic Programmes in IT Security”, PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm; (1996), ISBN: 91-7153-521-7.

[15] M. Bishop, “Computer Security – Arts and Science” – Addison-Wesley, (2006). ISBN: 978-0-201-44099-7.

[16] M. Wimmer, & B. Bredow, “e-Government: Aspect of Security on different layers” (2001), [Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=953086, last accessed March, 2011].

[17] NIST-IR7358, "Program Review for Information Security Management Assistance - PRISMA" (2007). [Available at http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf, last accessed March, 2011].

[18] Owasp, “Software Assurance Maturity Model (SAMM); A Guide to Building Security into Software Development, Version 1.0”. (2009). [Available at http://www.opensamm.org/, Last accessed Dec. 2010].

[19] P. Checkland, & J. Scholes, “Soft Systems Methodology in Action”, Chichester: Wiley (1990). [Available at http://jespersimonsen.dk/Downloads/SSM-IntroductionJS.pdf, Last accessed 2010].

[20] P. Schoderbek, C. Schoderbek, & A. Kefalas, “Management Systems, Conceptual Considerations”, (1985). ISBN: 0-256-03075-8.,

[21] P. W. Anderson, "Information security governance", information security technical report, volume 6, Number 3. pp. 60 – 70 , (2001).

[22] S. Kowalski, “IT Insecurity: A Multi-disciplinary Inquiry”, PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm (1994). ISBN: 91-7153-207-2

[23] S. Woodhouse, “Information Security: End User Behavior and Corporate Culture”, Proceedings of the IEEE 7th International Conference on Computer and Information Technology (2008).

[24] SSE-CMM. “Systems Security Engineering Capability maturity Models (SSE-CMM) ver. 3” (2003), [Available at http://www.sse-cmm.org/docs/ssecmmv3final.pdf, last accessed March, 2011].

[25] V. Rao, & R. Jamieson, “An Approach to Implementing Maturity Models in IT Security”, Proceedings of the 14th Australasian conference on information systems (2003).

[26] WorldBank, “Issue Note: E-Government and the World Bank" (2001), [Available at http://www.worldbank.org/reference/, Last accessed 2010].

## APPENDICES

**Annex I:** A Detailed Matrix for the Generic Security Requirements (Technical and Non-technical) for the Lowest Maturity Stage (Web-presence) – Expansion of table II and figure 2

| **Matrix for a Generic Security Requirements for the Web-presence Maturity Stage** | | | | | | |
|---|---|---|---|---|---|---|
| **ISMM Levels** | **Security Areas** | **Control Areas** | **Description of Security Requirements Control Areas: Objectives, Processes and Assurance, and Metrics Patterns** | **Mapped Security Activities Referred from Annexes: III, IV, V and VI** | | |
| | | | | **Annex III** | **Annex IV** | **Annex V & VI** |
| Undefined: [A] | Technical (Te) | Objectives | Establish and develop basic technical security objectives for the information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22 TSP.3,5,6, SSP.4 | PA.1,6, 7, 9, 10 CC.F1 CC.A1 |
| | | Processes | Establish, develop, and implement basic security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27 TSP.2, 4, 5, 7, 12, 13 SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9 CC.F2 CC.A2 |
| | | Metrics | Establish, develop, and implement basic security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10,13, 15, 18, 22, 25, 27 TSP.4, 7, 13 SSP.5 | PA.8,11 CC.F3 CC.A3 |
| | Non-technical (So) | Objectives | Establish and develop basic non-technical security objectives for the information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1, TSP.1,4, 8, SSP.1, 3, | PA.7 CC.F1 CC.A1 |
| | | Processes | Establish, develop, and implement basic security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1, TSP.1,4, 9-11 SSP.1, 2, | PA.7 CC.F2 CC.A2 |
| | | Metrics | Establish, develop, and implement basic security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4 SSP.5 | PA.11 CC.F3 CC.A3 |
| | | | | | | |
| Defined: [B] | Technical (Te) | Objectives | Continuous improve technical security objectives for the information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22 TSP.3,5,6, SSP.4 | PA.1,6, 7, 9, 10 CC.F1 CC.A1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10,13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Managed:[C] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10, 11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10,13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Controlled:[D] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10,13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Optimized: [E] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10,13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |

**Annex II:** A Detailed Matrix for a Generic Security Requirements (Technical and Non-technical) for the Highest Maturity Stage (Continuous improvement) – Expansion of table II and figure 2

| **Matrix for a Generic Security Requirements for the Continuous improvement Maturity Stage** | | | | | | |
|---|---|---|---|---|---|---|
| **ISMM Levels** | **Security Areas** | **Control Areas** | **Description of Security Requirements Control Areas: Objectives, Processes and Assurance, and Metrics Patterns** | **Mapped Security Activities Referred from Annexes: III, IV, V and VI** | | |
| | | | | **Annex III** | **Annex IV** | **Annex V & VI** |
| Undefined: [U] | Technical (Te) | Objectives | Establish and develop advanced technical security objectives for the information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Establish, develop, and implement advanced security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Metrics | Establish, develop, and implement advanced security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10, 13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Establish and develop advanced non-technical security objectives for the information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Establish, develop, and implement advanced security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Establish, develop, and implement advanced security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Defined: [V] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10, 13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Managed:[W] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10, 11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11.1; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11.1; P12.3-4 | OSP,9,10, 13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Controlled:[X] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11; | OSP.2,3,5-10, 12-21, 23-27;<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11; P12.3-4 | OSP,9,10, 13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |
| | | | | | | |
| Optimized: [Y] | Technical (Te) | Objectives | Continuous improve technical security objectives for information security targets (IST) and the operating environments (OE) | P1; P2.3; P6.5; P7; P8.1; P9.1; P10.2; P11.1; | OSP.2,3,4, 10,11,15,17, 21, 22<br>TSP.3,5,6,<br>SSP.4 | PA.1,6, 7, 9, 10<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P1; P3.1; P3.3-4; P4.2; P6; P7.4-10; P8.2-7; P9.2-6; P10.2; P11; | OSP.2,3,5-10, 12-21, 23-27<br>TSP.2, 4, 5, 7, 12, 13<br>SSP.4, 6 | PA.1- 4 , 6, 7, 8, 9<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P1.1-2; P4.2; P7.10; P8.1; P9.3, 6; P10.2; P11; P12.3-4 | OSP,9,10, 13, 15, 18, 22, 25, 27<br>TSP.4, 7, 13<br>SSP.5 | PA.8,11<br>CC.F3<br>CC.A3 |
| | Non-technical (So) | Objectives | Continuous improve non-technical security objectives for information security targets (IST) and the operating environments (OE) | P2; P3.2; P4.1; P5.4; P7; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 8,<br>SSP.1, 3, | PA.7<br>CC.F1<br>CC.A1 |
| | | Processes | Continuous improve and implement security processes and assurance patterns for the identified security objectives for the IST and OE | P2; P3.2; P4.1; P5.1-3; P7.1-3; P10.1; P12.1; | OSP.1,<br>TSP.1,4, 9-11<br>SSP.1, 2, | PA.7<br>CC.F2<br>CC.A2 |
| | | Metrics | Continuous improve and implement security metrics mechanisms for the implemented security objectives for the IST and OE | P3.2; P7.1; P10.1; P12.1-2; | TSP.4<br>SSP.5 | PA.11<br>CC.F3<br>CC.A3 |

**Annex III**: Matrix of ISO 27002 Security Control Principles and its Elements [12]

| Matrix of ISO 27002 Security Control Principles and its Elements [12] | | | |
|---|---|---|---|
| **Code No** | **Security Control Principles** | **Best Practice Security Control Elements** | **Principle Code No** |
| P1 | Risk Assessment and Treatment | Security risk assessment | P1.1 |
| | | Security risk analysis | P1.2 |
| | | Security risk mitigation | P1.3 |
| P2 | Security Policy | Policies | P2.1 |
| | | Guidelines and Procedures | P2.2 |
| | | Principles and Standards | P2.3 |
| P3 | Organization of Information Security | Security Structures | P3.1 |
| | | Security Reporting | P3.2 |
| | | Security of third parties access | P3.3 |
| | | Security outsourcing | P3.4 |
| P4 | Assets Management | Accountability for Assets | P4.1 |
| | | Information classification | P4.2 |
| P5 | Human Resource Security | Security prior to employment | P5.1 |
| | | Security during employment | P5.2 |
| | | Security after change of employment | P5.3 |
| | | Security awareness, training, and education | P5.4 |
| P6 | Physical and Environment Security | Physical access control | P6.1 |
| | | Physical access monitoring | P6.2 |
| | | Display media access control | P6.3 |
| | | Equipment security control | P6.4 |
| | | Environmental Control | P6.5 |
| P7 | Communications and Operations Management Security | Operational procedures and responsibilities | P7.1 |
| | | Third party service delivery management | P7.2 |
| | | Systems planning and acceptance | P7.3 |
| | | Protection against malicious software | P7.4 |
| | | Back-up | P7.5 |
| | | Network security management | P7.6 |
| | | Media handling security | P7.7 |
| | | Information exchange security | P7.8 |
| | | Electronic services security | P7.9 |
| | | Monitoring logging and system use | P7.10 |
| P8 | Access Control | Business Requirement for access control | P8.1 |
| | | User access management | P8.2 |
| | | User responsibilities | P8.3 |
| | | Network access control | P8.4 |
| | | Operating systems access control | P8.5 |
| | | Application and information access control | P8.6 |
| | | Mobile computing and teleworking | P8.7 |
| P9 | Information Systems Acquisitions, Development and Maintenance | Security requirements of systems | P9.1 |
| | | Security in application systems | P9.2 |
| | | Cryptographic control | P9.3 |
| | | Security of system files | P9.4 |
| | | Security in development and support processes | P9.5 |
| | | Technical vulnerabilities management | P9.6 |
| P10 | Information Security Incident Management | Reporting security events and weaknesses | P10.1 |
| | | Management of security incidents and improvements | P10.2 |
| P11 | Business Continuity Management | Disaster Recovery Planning | P11.1 |
| | | Resilience | P11.2 |
| P12 | Compliance | Legal requirements | P12.1 |
| | | Security Policies | P12.2 |
| | | Security Standards and Technical | P12.3 |
| | | Systems Audit considerations | P12.4 |

**Annex IV**: Matrix of ISM3 Security Controls [11]

| Matrix of Security Controls extracted from Information Security Management Maturity Model - ISM3 [11] Document | | | |
|---|---|---|---|
| **Code No** | **Operational Specific Practice (OSP)** | **Code No** | **Operational Specific Practice (OSP)** |
| OSP.1 | Report to Tactical Management | OSP.26 | Enhanced Reliability and Availability Management |
| OSP.2 | Security Procurement | OSP.27 | Archiving Management |
| OSP.3 | Inventory Management (Mgt) | | |
| OSP.4 | Information System Environment Change Control | **Code No** | **Tactical Specific Practices (TSP)** |
| OSP.5 | Environment Patching | TSP.1 | Report to Strategic Management |
| OSP.6 | Environment Clearing | TSP.2 | Manage Allocated Resources |
| OSP.7 | Environment Hardening | TSP.3 | Define Security Target and Objective |
| OSP.8 | Software Development Lifecycle Control | TSP.4 | Service Level Management |
| OSP.9 | Security Measures Change Control | TSP.5 | Define Property Group |
| OSP.10 | Backup Management. | TSP.6 | Define Environment and Lifecycles |
| OSP.11 | Access Control | TSP.7 | Background Checks |
| OSP.12 | User Registration | TSP.8 | Personnel Security |
| OSP.13 | Encryption Management | TSP.9 | Security Personnel Training |
| OSP.14 | Physical Environment Protection Management | TSP.10 | Disciplinary Process |
| OSP.15 | Operations Continuity Management | TSP.11 | Security Awareness |
| OSP.16 | Segmentation and Filtering Mgt | TSP.12 | Select Specific Processes |
| OSP.17 | Malware Protection Management | TSP.13 | Insurance Management |
| OSP.18 | Insurance Management | | |
| OSP.19 | Internal Technical Audit | **Code No** | **Strategic Specific Practices (SSP)** |
| OSP.20 | Incident Emulation | SSP.1 | Report to stakeholders |
| OSP.21 | Information Quality and Compliance Probing | SSP.2 | Coordination |
| OSP.22 | Alerts Monitoring | SSP.3 | Strategic Vision |
| OSP.23 | Event Detection and Analysis | SSP.4 | Define Rules for the Division of Duties |
| OSP.24 | Handling of Incidents and Near-incidents | SSP.5 | Compliance Check of SSP-4 |
| OSP.25 | Forensic | SSP.6 | Allocate Resources for Information Security |

**Annex V**: Matrix of SSE-CMM Security Controls [24]

| Matrix of Security Controls extracted from Systems Security Engineering Capability Maturity Model - SSE-CMM [24] | | | |
|---|---|---|---|
| **Code No** | **Security Best Practice Areas** | **Code No** | **Security Best Practice Areas** |
| PA.1 | Administer Security Controls | PA.7 | Coordinate Security |
| PA.2 | Assess Impact | PA.8 | Monitor Security Posture |
| PA.3 | Assess Security Risk | PA.9 | Provide Security Input |
| PA.4 | Assess Threat | PA.10 | Specify Security Needs |
| PA.5 | Assess Vulnerability | PA.11 | Verify and Validate Security |
| PA.6 | Build Assurance Argument | | |

**Annex VI**: Matrix of Common Criteria (CC) Security Controls [2]

| Matrix of Security Controls extracted from the Common Criteria (CC) [2] | | | |
|---|---|---|---|
| **Code No** | **CC-PART2V3.1R3: Security Functional Requirements - Best Practice Areas** | **Code No** | **CC-PART3V3.1R3: Security Assurance Requirements - Best Practice Areas** |
| CC.F1 | Security Functional Objectives for the IST/TOE and OE | CC.A1 | Security Assuarance Objectives for the IST/TOE and OE |
| CC.F2 | Security Functional Requirements | CC.A2 | Security Assuarance Requirements |
| CC.F3 | Security Functional Conformance | CC.A3 | Security Assuarance Conformance |