Abstract—Technical security metrics provide measurements in ensuring the effectiveness of technical security controls or technology devices/objects that are used in protecting the information systems. However, lack of understanding and method to develop the technical security metrics may lead to unachievable security control objectives and incompetence of the implementation. This paper proposes a model of technical security metric to measure the effectiveness of network security management. The measurement is based on the effectiveness of security performance for (1) network security controls such as firewall, Intrusion Detection Prevention System (IDPS), switch, wireless access point, wireless controllers and network architecture; and (2) network services such as Hypertext Transfer Protocol Secure (HTTPS) and virtual private network (VPN). We use the Goal-Question-Metric (GQM) paradigm [1] which links the measurement goals to measurement questions and produce the metrics that can easily be interpreted in compliance with the requirements. The outcome of this research method is the introduction of network security management metric as an attribute to the Technical Security Metric (TSM) model. Apparently, the proposed TSM model may provide guidance for organizations in complying with effective measurement requirements of ISO/IEC 27001 Information Security Management System (ISMS) standard. The proposed model will provide a comprehensive measurement and guidance to support the use of ISO/IEC 27004 ISMS Measurement template.

Keywords—Security metrics; Technical security metrics model; Measurement; Goal-Question-Metric (GQM); Effective measurement; Network security management

I. INTRODUCTION (HEADING 1)

Network security is defined as the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links [2]. How much protection is required in ensuring the use of information and associated networks to conduct the business are well managed? How to identify and analyze network security controls to mitigate the network security risks? These questions have derived to implement and maintain secure and functional network is absolutely critical to the success of any organization’s business operations [2][3]. Thus, it is important to measure network security effectiveness in handling the risks from the current threats, vulnerabilities and attacks.

According to [4], the practical challenges and issues are what to measure and what information to report in facilitates the senior management for any decision making. Obviously, the reported information is often based on what is easier to measure instead of what is actually meaningful strategically [5], [6], [7]. Does network security management is among the easier information to measure?

Some organizations may be reported the measures from out of context perspective, without a baseline for comparison, or present simple measurements that do not show any kind of correlation, which greatly (or even completely) limits the value of the reported information [5][8].

A. Requirements From ISO/IEC 27001 ISMS Standard

ISO/IEC 27001:2005 Information Security Management System (ISMS) [9] is intended to bring formal specification of information security under explicit management control. It is a mandated specific requirement, where organizations can therefore be formally audited and certified compliant with the standard.

The standard provides some confidence level of information protection among business organizations. With the existence of ISO/IEC 27001 ISMS certification, these organizations can increase their protection of information by having independent assessment conducted by the accredited certification body. The certificate has proven the potential marketing to the most business organizations, where a total of 7536 organizations have already been certified worldwide [10]. Obviously, there are other 27000 series that support this standard, including ISO/IEC 27002 Code of practice for information security management [11], ISO/IEC 27003 ISMS implementation guidance [12], ISO/IEC 27004 Information security management Measurement [13] and ISO/IEC 27005 Information security risk management [14].

There are 133 security controls in Annex-A of ISO/IEC 27001 ISMS standard. ISO/IEC 27002 [11] provides the best practice guidance in initiating, implementing or maintaining the security control in the ISMS. This standard regards that not all of the controls and guidance in this code of practice may be
Information security measurement is a mandatory requirement in this standard where a few clauses are stated in [9]:

Å 4.2.2(d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results;
Å 4.2.3(c) Measure the effectiveness of controls to verify that security requirements have been met;
Å 4.3.1(g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls;
Å 7.2(f) results from effectiveness measurements; and
Å 7.3(e) Improvement to how the effectiveness of controls is being measured.Ø

Moreover, the new revision of ISO/IEC 27001:2013 [15] standard has also highlighted the importance of effective measurement in their mandatory requirement clauses 9 - Performance evaluation.

B. Summary

The standard highlighted that the organization must evaluate the information security performance and the effectiveness of the ISMS. The evaluation of the effectiveness should include but not limited to: (i) monitor and measure information security processes and controls; (ii) methods to use when monitor and analyze measurement for valid or significant result; (iii) time and personnel to perform the monitoring and measurement; (iv) determine time, duration and personnel to analyze the measurement results.

Thus, in ensuring the ISMS effectiveness, the information security measure can facilitate the management to make decision by the collection, analysis, evaluation and reporting of relevant performance-related measurements.

The importance of information security measurement is well defined and highlighted in both standards. Most of the research papers focused on information security metrics for general IT systems. However, lack of research on technical security metrics [16][17][18][19]. Thus, our research is focusing on the development of technical security measurement that will be incorporated in the technical security metric model.

II. RELATED WORK

In understanding the requirements, the security metric, measure and effective measurement must be defined.
| Security Metric | Security Measure | Effective Measurement |
|-----------------|------------------|-----------------------|
| (1) Security Objectives • Identify the adequacy of security controls | • Clearly defined acceptable value • Performance goals and objectives (efficiency, effectiveness) | • Meet security objectives and requirements • Clearly defined |
| (2) Quantifiable, computed value | • Quantifiable information • Scope of measurement (Process, performance, outcomes, quality, trends, conformance to standards and probabilities) | • The value is objective and quantifiable • Determine the Key-Performance-Indicator (KPI) |
| (3) Method of Measurement • Process of data collection, data from security assessment process | • Easily identified • Quantitative indications by some attributes of a control or process | • Simple measurement • Low cost and easy access • Capability to measure accurately |
| (4) Analysis of Data • Comparable to a scale/benchmark/Predetermined baseline • Repeatable | • Apply formulas for analysis • Track changes • Quantifiable information for comparison | • Consistent value • Accurate time and data • Comparable and reproducible results • Security controls are implemented correctly, operating as intended, and meeting the desired outcome. |
| (5) Security Indicator/Characteristics • Meaningful result (score, rating, rank, or assessment result) | • Monitor the accomplishment | • Increase confidence level • Security improvement |
| (6) Reporting relevant data | • Communicated/Reported • Intended audience | • Present to targeted audience/Stakeholder |
| (7) Decision making | • Facilitate decision making | • Facilitate corrective action |
| (8) Requirement to Standard, regulatory, financial and organizational reasons | | • Align with business goals and regulations |

d) Comparable result – ESM should produce a baseline for comparison purposes, repeatable or consistently reproducible, so that different people at different times can make the same measurement. Apparently, this supports the adequacy of in-place security controls, policies, and procedures; security controls are implemented correctly, operating as intended, and meeting the desired outcome.

e) Corrective action - ESM should provide the appropriate timeliness and frequency of measurement for the change of measurement target so that the latency of measures does not defeat their purpose. ESM should be collected and reported in a consistent manner. ESM should provide the management to decide the new investment in additional information security resources, identify and evaluate non-productive security controls, and prioritize security controls for continuous monitoring.

f) Targeted audience/Stakeholder – ESM should be easily identified by the audience/stakeholder to whom the measure is communicated. For example, provide the relevant measures that produce the significant result for the management to make decision.

g) Security Improvement – ESM should provide some indicators that could be a sign of relevant security characteristics that prescribes the meaning of obtained security values and achieves to some level of improvement.

h) Align with business goals - ESM should provide a benefit to the business it supports.

The development of our TSMM is based on the above criteria and to focus on security performance for the relevant controls (see Fig.1).
III. RESEARCH METHOD FOR DEVELOPMENT OF TECHNICAL SECURITY METRIC MODEL (TSMM)

The GQM approach was originally developed by Basili et al. [1] in evaluation and measurement of software products and development processes. Ever since developed, this approach was used consistently focus on the software measurement and processes [35]. There were also a few research studies on business processes [36][37][38] and security metrics [26][39][40][41][42][43][44]. However, there is no research study conducted for measuring the network security management using the same approach.

To achieve the objective of developing the TSMM, we propose a research method based on a combination of approaches. The outcome of this research method is the introduction of network security management metrics as attributes to the TSMM.

The first approach is to define the technical security metric (TSM). We set our goal to meet the requirements from ISO/IEC 27001 ISMS standard. The paradigm of Goal-Question-Metric (GQM) [1] is used and described further which to align with standard requirement (Fig.2).

We combine the developed Goal-Question-Metric (GQM) paradigm and data of literature review (Fig.3) as a first step. This approach is used for developing the initial TSMM in a top-down manner, from general objective to the relevant metrics or outputs and combines the inputs from the literature review. The application results in GQM models, leading to the initial TSMM. However, this initial development work remains subjective and potentially incomplete.

In the second approach (Step 2), we use the GQM method consists of four phases [45]: planning, definition, data collection, interpretation (see Fig.4). The explanation of these phases is based on the compliancy to the requirement controls of ISO/IEC 27001 standard [9] for A.10.6 Network security management (NSM); A.10.6.1 Network controls; and A.10.6.2 Secure network services.

Our implementation adopts the processes and activities by [41] and [46].

- The Planning phase: The NSM-team is established and the compliance requirement is clearly delivered. The desired improvement areas such as performance, security and monitor are identified. The team selects and characterizes the products or controls to be studied. The result of this phase is a project plan that outlines the characterization of the products or controls, the schedule of measuring, the organizational structure, and necessary awareness and training for people involved in measurements.

- The Definition phase: The measurement goals are defined. This phase is also to identify and analyze the perception and understanding of effective measurement requirement from ISO/IEC 27001 standard [9]. We will create a new template to gather all related information based on some other templates from ISO/IEC 27004 [13] and NIST SP800-55 [27]. For the purpose of this, the interviews may be conducted with people (management and technical) involved in the process or product under study. Based on the goals, relevant questions are developed to identify the

![Figure 1. Eight Criteria of Effective Security Metric](image1)

![Figure 2. Eight Criteria of Effective Security Metric](image2)
specific quality attributes and to re-define the goals precisely. For each question a hypothesis with an expected answer should be defined. Next, the metrics are defined for each question and checked on consistency and completeness. Results of this phase are an analysis of compliance plan and a measurement plan.

- The Data Collection phase - the team is required to prepare the data collection within their knowledge and availability. The data may be extracted manually or electronically and may involve automated data collection tools. Results of this phase are to develop the data support system consisting of spreadsheets, statistical tools, database applications and presentation tools.

- The Interpretation phase - the collected data is processed and analyzed according to the metrics defined. The measurements result should be able to answer the questions, and with the answers it can be evaluated if the initial goals are attained. Moreover, the measurement result should provide some values that describing the performance measurement of the security controls.

![Figure 3. Data from literature review](image3.jpg)

![Figure 4. The four phases of GQM-method [45]](image4.jpg)

The second approach is used as a validation/improvement of the first step. It is based on a literature review of security metric standards and guidelines and measurement methods for network security controls. This approach is a bottom-up, being an analysis of the literature to identify the metrics currently used. A comparative analysis is developed between the metrics and those defined through GQM. This comparison is summarized in an analysis table.

As shown in Fig.5, we map the GQM-method with ISO/IEC 27004 template for an information security measurement construct and show the synchronization link (relevant colored-box). We refer to this standard as a reference and example to form a GQM-Measurement plan.

Once the literature is completely surveyed, the development of GQM-Measurement plan should be ready. The relevant people should be interviewed to validate the initial TSMM. Finally, the TSMM is accordingly revised.
A. GQM-Measurement Plan

We develop a GQM-Measurement plan consists of goals, questions, and metrics in a hierarchical structure (see Fig. 6) based on [1][45].

In developing the goals, the security objectives of A.10.6, A.10.6.1 and A.10.6.2 of ISO/IEC 27001 requirement controls [9] are referred. At this stage, the understanding of the security control requirements is very important. The understanding can be obtained through the interview with the relevant people and checking available process or product descriptions [46]. If goals are still unclear, a reference to ISO/IEC 27002 [11], FDIS ISO/IEC 27033 [2] and NIST SP800-55 [25] can also assist.

The proposed questions shall refine the goals make them operational enough so that it would not create difficulties to reveal the relationship to the collected data and ease the interpretation of the answers towards the goals [46]. The questions are also derived from the literature reviews.

The questions are stated in a quantitative way where data can be collected by measurements. We provide the expected answers to the questions and formulated as hypotheses. Through hypotheses, we can learn the effect from measurements and compare the knowledge before and after measurements.

The GQM-Method and ISO/IEC 27004 Measurement Template

According to [1][41][46], we can define several metrics for each question. It is also possible that one metric may be used to answer different questions under the same goal. We choose metrics with quantitative level making it possible to assign numbers to a quality attribute. Metrics are defined to answer the relevant questions and should be able to support or reject the stated hypotheses (if any).

A simple Goal-Measurement plan is developed for the purpose of this discussion (as full development of plan is currently in progress). The example of GQM-Measurement plan as stated in Table II.

| Goal          | G1 | A.10.6.1 Network controls - Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. |
|---------------|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Question      | Q1 | What are the risk levels for network controls and security controls that protect your information?                                                                                                      |
| Metric        | M1.1 | Risk Assessment = Asset Value x Threat x Vulnerability                                                                                                                                              |
| Question      | Q2 | What are the monitoring mechanisms that your organization has?                                                                                                                                 |
| Metric        | M2.1 | Frequency of audit logging review                                                                                                                                                                   |
| Metric        | M2.2 | Security Incidents report (IDS/IPS/user report) - Comparison of number of total incidents with the threshold.                                                                                           |
| Question      | Q3 | How often the security assessment and/or penetration testing are conducted within a year?                                                                                                          |
| Metric        | M3.1 | Frequency of assessment conducted                                                                                                                                                                   |
| Metric        | M3.2 | Success or failure rate for corrective action                                                                                                                                                       |
| Metric        | M3.3 | Conducted by trained/experience staff                                                                                                                                                               |
| Question      | Q4 | How often your organization conduct the security updates for network controls?                                                                                                                        |
| Metric | M4.1 | Success and failure rates of security updates |
|-------|-----|-----------------------------------------------|
| Metric | M4.2 | Frequency/periodic of maintenance |
| Question | Q5 | Who is responsible to ensure the effectiveness of network controls is intact? |
| Metric | M5.1 | Rate of understanding the job description |
| Metric | M5.2 | Qualification, Training and Education attended |
| Question | Q6 | What are the authentication mechanism in accessing the network and systems used in your organization? |
| Metric | M6.1 | Password quality I manual (Number of passwords which satisfy organization\textsuperscript{\textregistered} password quality policy for each user) |
| Metric | M6.2 | Password quality - automated |
| Metric | M6.3 | Number of password being shared? |
| Metric | M6.4 | Ratio of passwords crackable within 4 hours. |
| Question | Q7 | Who is responsible to ensure the effectiveness of network controls is intact? |
| Metric | M7.1 | Rate of understanding the job function |
| Metric | M7.2 | Qualification, Training and Education attended |
| Metric | M7.3 | Ratio of responsible personnel to total number of staff |
| Question | Q8 | What are the mechanism used to authorize the relevant users to access the networks and systems? |
| Metric | M8.1 | Number of restricted access methods (network segment, IP address, MAC address, firewall, etc.) |

**IV. CONCLUSION AND FUTURE WORK**

The objective of this paper is to identify and to define a set of metrics for the TSSM with a systematic and scientific approach to comply with ISO/IEC 27001 standard. We use the GQM approach on the TSSM and review with regards to the literature. The result of this paper is the enrichment of the TSSM with suited network security management metrics.

Although the initial developed TSSM are validated through literature analysis, their testing in a real case would provide a concrete instantiation and validation of their relevance. The GQM-Measurement plan is currently being developed to suit the security objectives. The validation will be conducted with the network security experts.

As part of the next step of our future work, the metrics will be integrated into the initial TSSM and a case study is to be conducted using our GQM-Measurement plan. This will validate the final TSSM.

**ACKNOWLEDGMENT**

The authors wish to acknowledge and thank members of the research teams of the Long Term Fundamental Research Grant Scheme (LRGS) number LRGS/TD/2011/UKM/ICT/02/03 for this work. The research scheme is supported by the Ministry of Higher Education (MOHE) under the Malaysian R&D National Funding Agency Programme. This project is also supported by the CyberSecurity Malaysia and the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.

**REFERENCES**

[1] V. R. Basili, G. Caldiera, and H. D. Rombach, Goal Question Metric Paradigm. Encyclopedia of Software Engineering. John Wiley \& Sons, Inc., 1994, pp. 532–538.

[2] FDIS 27033-1:2009, FDIS 27033-1 - Information technology - Security techniques \textsuperscript{\textregistered} Network security \textsuperscript{\textregistered} Part 1: Overview and concepts,\textregistered Int. Organ. Stand. Int. Electrotech. Comm. FDIS 27033-12009, no. Final Draft, 2009.

[3] N. Schneidewind, Metrics for mitigating cybersecurity threats to networks,\textregistered IEEE Internet Comput., vol. 14, no. 1, pp. 64–71, Jan. 2010.

[4] R. Barabanov, S. Kowalski, and L. Yngström, Information Security Metrics:\textsuperscript{\textregistered}Research Directions,\textregistered Stock. Univ., 2011.

[5] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional, 2007.

[6] D. S. Herrmann, Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI, 1st ed. Auerbach Publications, 2007, p. 848.

[7] W. K. Brophy, Information Security Governance: Guidance for Information Security Managers,\textregistered Govt. Inst., 2008.

[8] R. Ayoub, Analysis of Business drivers metrics: measuring for security value,\textsuperscript{\textregistered} 2006.

[9] ISO/IEC 27001:2016, Information technology - Security techniques - Information security management systems- Requirements,\textregistered Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 27001:2016, 2016.

[10] Number of Certificates Per Country,\textregistered International Register of ISMS Certificates, 2012. [Online]. Available: http://www.iso27001certificates.com/. [Accessed: 08-Dec-2011].

[11] ISO/IEC 27002:2005, Information technology - security techniques - Code of practice for information security management,\textregistered International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27002:2005, vol. 2005, 2005.

[12] ISO/IEC 27003:2010, Information technology - Security techniques - Information security management systems- Implementation Guidance,\textregistered International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27003:2010. International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27003:2010, 2010.

[13] ISO/IEC 27004:2009, Information technology - Security techniques - Information security management systems- Measurement,\textregistered International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27004:2009. International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27004:2009, 2009.

[14] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management,\textregistered Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 27005:2011, 2011.

[15] ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems- Requirements,\textregistered Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 27001:2013, 2013.

[16] M. Stoddard, D. Bodeau, R. Carlson, C. Glantz, Y. Haines, C. Lian, J. Santos, and J. Shaw, Process Control System Security Metrics I State of Practice,\textregistered Inst. Inf. Infrastruct. Prot., vol. Research R, no. August, 2005.

[17] J. P. Pironi, Developing Metrics for Effective Information Security Governance,\textregistered Int. Syst. Control J., vol. 2, 2007.

[18] J. Hallberg, M. Eriksson, H. Granlund, S. Kowalski, K. Lundholm, Y. Monfelt, S. Pilemalm, T. Wätterstam, and L. Yngström, Controlled
Information Security: Results and Conclusions from the Research Project, FOI Swedish Def. Res. Agency, pp. 17-42, 2011.

[19] R. Savola, "Security Metrics Taxonomization Model for Software-Intensive Systems," J. Inf. Process. Syst., vol. 5, no. 4, pp. 197–206, Dec. 2009.

[20] S. Wright, "Measuring the Effectiveness of Security using ISO 27001," SANS Inst., pp. 11-15, 2006.

[21] M. P. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "A Technical Security Metrics Model in Compliance with ISO / IEC 27001 Standard," Int. J. Cyber-Security Digit. Forensics, vol. 1, no. 4, pp. 280–288, 2012.

[22] W. Jansen, "Directions in Security Metrics Research," Natl. Inst. Stand. Technol. NISTIR 7564, 2009.

[23] M. Masera and I. N. Fovino, "Security metrics for cyber security assessment and testing," Res. Cent. Eur. Comm., vol. ESCORTS D4, no. August, pp. 11-26, 2010.

[24] Y. Beres, M. C. Mont, J. Griffin, and S. Shiu, "Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes," Methodology, pp. 564–573, 2009.

[25] R. B. Vaughn, R. Henning, and A. Siraj, "Information assurance measures and metrics-state of practice and proposed taxonomy," Proc. 36th Hawaii Int. Conf. Syst. Sci., pp. 10, 2003.

[26] R. Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," in International Conference on Software Engineering Advances, 2007.

[27] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance Measurement Guide for Information Security," Natl. Inst. Stand. Technol. Spec. Publ. 800-55, no. July, 2008.

[28] F. C. Freiling, "Introduction to Security Metrics," LNCS 4909, Springer-Verlag Berlin Heidelberg, pp. 129–132, 2008.

[29] W. K. Brothby, "Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement," Auerbach Publ., 2009.

[30] H. Liu and Y. Zhu, "Measuring effectiveness of information security management," Int. Symp. Comput. Netw. Multimed. Technol. 2009, CNMT 2009., pp. 17–4, 2009.

[31] K. Lundholm, J. Hallberg, and H. Granlund, "Design and Use of Information Security Metrics," FOI, Swedish Def. Res. Agency, pp. ISSN 1650-1942, 2011.

[32] G. Jelen, "FSE-CMM Security Metrics," NIST CSSPAB Work. Washington, D.C., 2000.

[33] D. A. Chapin and S. Akridge, "How Can Security Be Measured?", Inf. Syst. Control J., vol. 2, 2005.

[34] M. H. S. Peláez, "Measuring effectiveness in Information Security Controls," SANS Inst., 2010.

[35] H. K. N. Leung, "Quality metrics for intranet applications," Inf. Manag., vol. 38, 2001.

[36] V. Basili, J. Heidrich, M. Lindvall, J. Münch, C. Seaman, M. Regardie, and A. Trendowicz, "Determining the impact of business strategies using principles from goal-oriented measurement," Proc. Wirtschaftsinformatik 2009 9th Int. Conf. Bus. Informatics, Vienna., 2009.

[37] A. Azim and A. Ghani, "Complexity Metrics for Measuring the Understandability and Maintainability of Business Process Models using Goal-Question-Metric (GQM)," vol. 8, no. 5, pp. 219–225, 2008.

[38] L. S. González, F. G. Rubio, F. R. González, and M. P. Velthuis, "Measurement in business processes: a systematic review," Bus. Process Manag. J., vol. 16, no. 1, pp. 114–134, 2010.

[39] T. Perkins, R. Peterson, and L. Smith, "Back to the Basics: Measurement and Metrics," pp. 91–12, 2003.

[40] D. Lekkas and D. Spinellis, "Handling and reporting security advisories: A scorecard approach," Secur. Privacy, IEEE, 2005.

[41] N. Mayer and E. Dubois, "Towards a Measurement Framework for Security Risk Management," Proc. Model. Secur. Work., 2008.

[42] T. Heyman, R. Scandariato, C. Huygens, and W. Joosen, "Using Security Patterns to Combine Security Metrics," 2008 Third Int. Conf. Availability, Reliab. Secur., pp. 1156–1163, Mar. 2008.

[43] R. Gonzalez, "A measurement model for secure and usable e-commerce websites," Can. Conf. Electr. Comput. Eng., no. c, pp. 77–82, 2009.

[44] K. Julisch, "Unifying Theory of Security Metrics with Applications to Applications," 2009.

[45] R. Van Solingen and E. Berghout, "The Goal/Question/Metric Method: a practical guide for quality improvement of software development," The McGraw-Hill, 1999.

[46] H. Koziolek, "Goal, Question, Metric," Dependability Metrics, LNCS 4909, Springer-Verlag Berlin Heidelberg, pp. 393–42, 2008.

AUTHORS PROFILE

Rabiah Ahmad received Ph.D in Health Informatics at University of Sheffield (UK) and Master of Science in Information Security from Royal Holloway University of London (UK). She is currently appointed as Associate Professor at Universiti Teknikal Malaysia Melaka (UTeM) and acting as Deputy Director at Centre for Research Innovation and Management. Rabiah Ahmad involved with various research in information security and health informatics. She has become project leader for 4 research projects funded by the Ministry of Science, Technology and Innovation, Malaysia and the Ministry of Higher Education, Malaysia. She has written 3 academic books, more than 5 chapters in books, 30 articles in International Indexed Journal, 2 articles in Local Indexed Journal, more than 30 in International Proceedings and 3 in Local Proceedings. She has been invited as Manuscript Reviewer for several International Journals such as International Journal of Medical Informatics, International Journal on Cryptography and Journal of Soft Computing.

Shahrin Sahib received the Bachelor of Science in Engineering, Computer Systems and Master of Science in Engineering, System Software in Purdue University in 1989 and 1991 respectively. He received the Doctor of Philosophy, Parallel Processing from University of Sheffield in 1995. His research interests include network security, computer system security, network administration and network design. He is a member panel of Expert National ICT Security and Emergency Response Centre and also Member of Technical Working Group: Policy and Implementation Plan, National Open Source Policy. He is a Professor and Deputy Vice Chancellor Office (Academy and International) at Universiti Teknikal Malaysia Melaka (UTeM).

M.P Azuwa is the Specialist of CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, Malaysia. Azuwa holds a Master degree in Computer Science from the University Putra Malaysia, Malaysia and a Bachelor degree in Computer Science from the same university. She is the holder of Certified Information Security Manager (CISM) Certified in Risk and Information Systems Control (CRISC) from ISACA, USA; Professional on Critical Infrastructure Protection (PCIP) from Critical Infrastructure Institute (CII), Canada; Certified SCADA Security Architect (CSSA) from InfoSec Institute, USA; Certified BS7799 Lead Auditor I Information Security Management System (ISO/IEC 27001); SANS GIAC Security Essential Certified (GSEC). Azuwa has been awarded Information Security Practitioner Honour in July 2011 by the (ISC)2, USA. She has contributed various publications and presented papers on topics related to information security management. She is currently pursuing his PhD at the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.