Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level

Heru Susanto
Indonesian Institute of Sciences
114 PUBLICATIONS 564 CITATIONS
SEE PROFILE

Mohammad Nabil Almunawar
Universiti Brunei Darussalam
115 PUBLICATIONS 1,378 CITATIONS
SEE PROFILE

Yong Chee Tuan
YES
9 PUBLICATIONS 209 CITATIONS
SEE PROFILE

EXPLORE iJET International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level

Heru Susanto[12], Mohammad Nabil Almunawar[1], Yong Chee Tuan[1]
[1]FBEPS University of Brunei
Information System Group
[2]The Indonesian Institute of Sciences
Information Security & IT Governance Research Group

ABSTRACT

Information security challenges and breaches increasing time by time lead practitioners and experts solving that's problems. Compliance with information security standards be highly recommended to ensure all information be safe since securing information system resources is extremely important to ensure that the resources are well protected. Information security is not just a simple matter of having usernames and passwords. Actually Information security becomes a very important part for the organization's intangible assets, level of confidence and stakeholder trusted are performance indicator as successes organization. This paper will discuss the challenges and breaches in information security, we refer several surveys in the field of information security as secondary data, such as information security breaches survey and global state of information security survey, that lead us offer a framework (called by integrated solution framework, i-solution framework) for understanding information security management standards (ISMS) term and concept and also we implement it into application software on assessing readiness level of an organization toward the implementation of information security standard, ISO27001.

Key words: *I-Solution Framework, I-Solution Modelling Software, Six domain view, Information Security Assessment, ISMS*

I. INTRODUCTION

Information security has always been an interesting topic for discussion, because all the activities of our lives cannot be separated from the transfer of information from one party to another. Within information exchanges processes are expected transfer process for promoting the occurrences of a business activity. An organizational communication channel, which is using a network technology, such as intranet, extranet, internet, is a target for hackers in filtrated by. In the other hand, a vulnerability issue is one of the interconnected impacts. Recent survey on information security indicates increasing trend of information breaches, credit card pishing that led to enormous losses. Information is the lifeblood of organizations, a vital business asset in today's IT-enabled world. Thus, securing information system resources is extremely important to ensure that the resources are well protected (*Potter & Beard, 2010*). Regulations and various privacy/data protection policy impose a raft of obligations to organization.

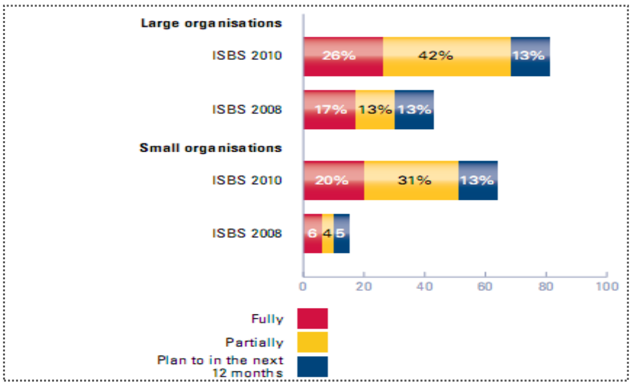


Figure 1. How many respondents have implemented ISO 27001 (ISBS, 2010)

Since information security has a very important role in supporting the activities of the organization, we need a standard as benchmark which regulates governance over information security. There are several standards for IT Governance which leads to information security such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT. However, some of these standards are not well adopted by the organizations, with a variety of reasons. The big five are ISO27001, BS 7799, PCIDSS, ITIL and COBIT. The comparative study conducted to determine their respective strengths, focus, main components and their level of adoption, concluded that ISO 27011 is most widely used standard in the world in information security area (*susanto, almunawar & tuan, 2011b*).

The main challenge on our research is gaps between high demands on implementation of information security standards, against actual implementation by an organization. Unfortunately, actual number of information security standard implemented by an organization, ISO 27001, for small organizations are 6% in 2008, increase to 17% in 2010, and while for large organization is 20% in 2008 and rising to 26% in 2010 (*Potter & Beard, 2010*). We concluded that around 6% to 26% organization have been implemented information security standard for supporting their business process and business activity [*figure 1*].

II. BREACHES, CONSTRAINTS AND CHALLENGE

Based on Information security breaches survey (Potter & Beard, 2010) Protecting customer information remains the most important driver for security, 28%. Preventing downtime and outages (19%) has increased in relative importance, perhaps in the wake of the recent wave of Internet worm attacks [figure 2].

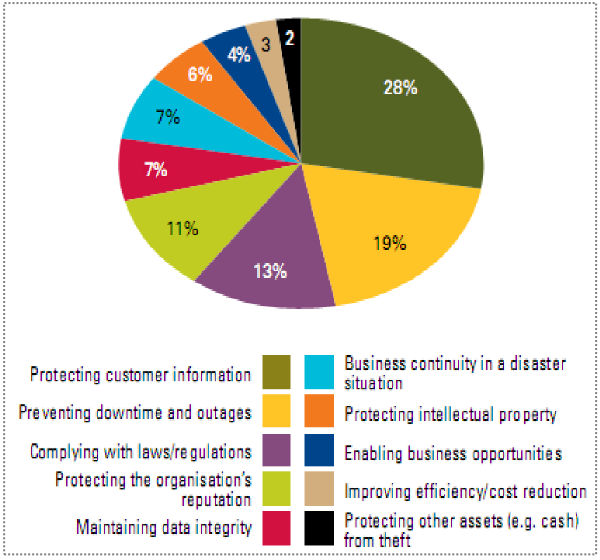


Figure 2. What is the main driver for information security expenditure? (ISBS, 2010)

Protecting the organization's reputation and maintaining data integrity have (11% and 7%). In the financial services and government sectors it was the second highest driver after protecting customer information. In contrast, compliance with regulation appears highly unlikely to drive security in the retail and manufacturing sector. It indicates customer information has a very high impact for an organization's activity, means secure information increasing customer thrush.

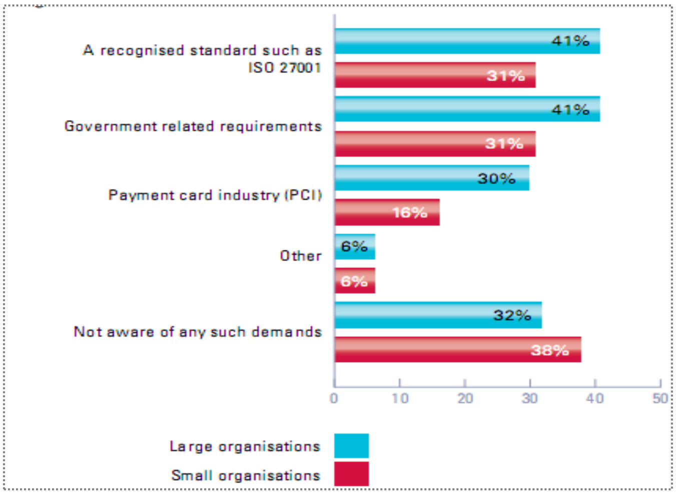


Figure 3. What standards or guidelines have respondents' customers required them to comply with? (ISBS, 2010)

Refers to the global usability of standards, indicated ISO 27001 is leading, more than 80% of the world, therefore described us the standard is more easily implemented and well recognized by stakeholders (top management, staff, suppliers, customers/clients, regulators). ISO 27001 is becoming a common standard for compliance; despite having their own sector specific standards, two-fifths of financial services and a third of government organizations are also being asked to comply with ISO 27001 *[figure 3]*. The implication is that ISO 27001 is increasingly becoming the lingua franca for information security (*ISBS, 2010*).

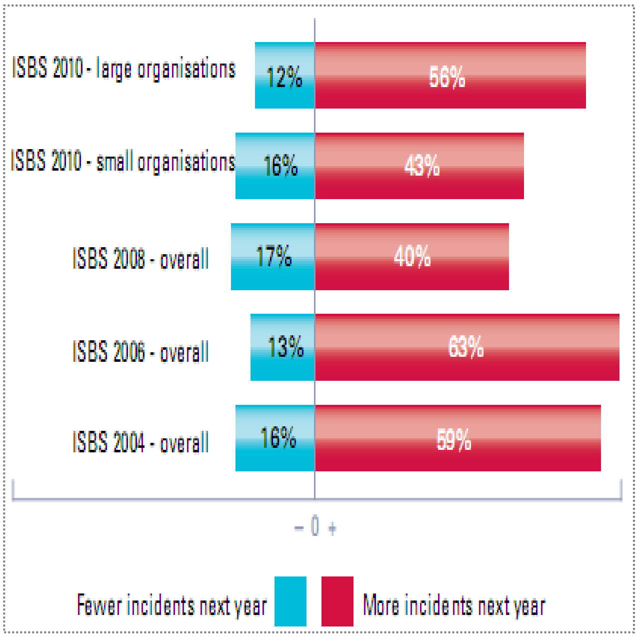
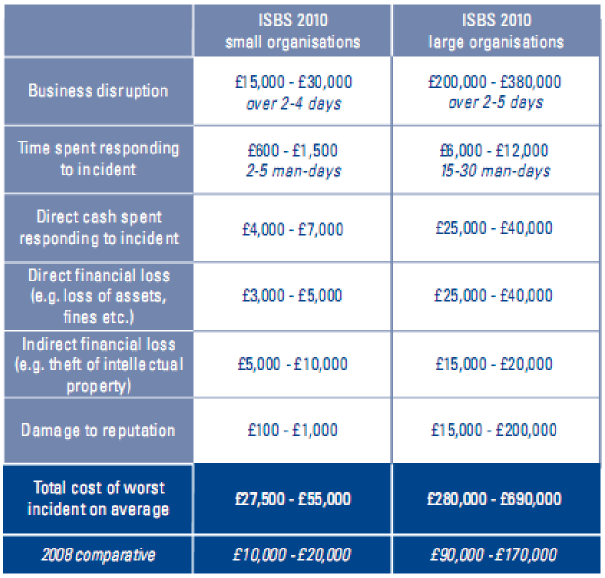


Figure 4. What do respondents expect in the future?(ISBS, 2010)

In other hand, respondents remain, on balance, pessimistic about what the future holds. Nearly three times as many respondents expect to have more security breaches next year as expect fewer breaches (*ISBS, 2010*). It indicates in future there will be increased to information security incidents, caused by increasingly interlinked computers throughout network in the world, which can improve business efficiency but also raises vulnerability to the system *[figure 4]*.

The average total cost of a small respondent's worst incident is between £27,500 and £55,000, up significantly on 2008. With the average total cost of the worst incident now up to between £280,000 and £690,000. Total cost of worst incident is increases, indicated from 2008 to 2010 300% for small organization and more than 400% for large organization (*ISBS, 2010*) *[table 1]*.



	ISBS 2010 small organisations	ISBS 2010 large organisations
Business disruption	£15,000 - £30,000 *over 2-4 days*	£200,000 - £380,000 *over 2-5 days*
Time spent responding to incident	£600 - £1,500 *2-5 man-days*	£6,000 - £12,000 *15-30 man-days*
Direct cash spent responding to incident	£4,000 - £7,000	£25,000 - £40,000
Direct financial loss (e.g. loss of assets, fines etc.)	£3,000 - £5,000	£25,000 - £40,000
Indirect financial loss (e.g. theft of intellectual property)	£5,000 - £10,000	£15,000 - £20,000
Damage to reputation	£100 - £1,000	£15,000 - £200,000
Total cost of worst incident on average	£27,500 - £55,000	£280,000 - £690,000
2008 comparative	*£10,000 - £20,000*	*£90,000 - £170,000*

Tabel 1. What was the overall cost of an organization's worst incident in the last year? (ISBS, 2010)

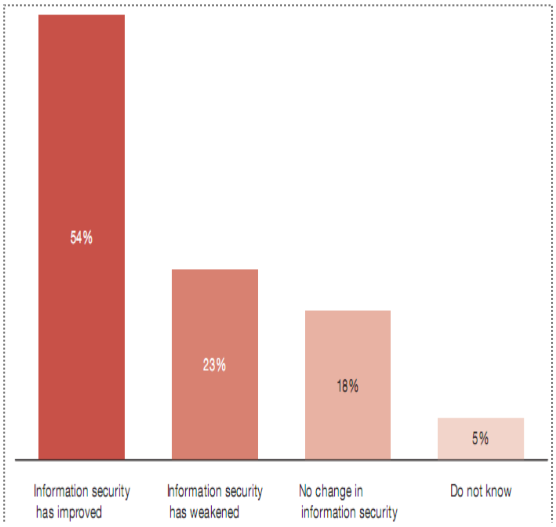


Figure 5. The Impact of cloud computing on information security (GSISS, 2012)

Nowadays is cloud computing era, which offering organization in three types of services; software-as-a-service, infrastructure-as-a-service and platform-as-a-service. Cloud computing is improving security. But many want better enforcement of provider security policies, among other priorities. Has the cloud improved security? More than half (54%) say it has, 23% believe that security has "weakened" and 18% see no change (*GSISS, 2012*) *[figure 5]*.

III. BENEFITS AND OBSTACLES ON ISO27001 IMPLEMENTATION

ISO 27001 plays a very important role in monitoring, review, maintenance and improvement of an information security management system. It works like an overall management and control framework for managing an organization's information security risks. The prime objective of this standard normally supports to establish, design, implement and manage an effective information management system which protects information of an organization from any risks (*Ali Bitazar, 2009*).

International standard ISO 27001 enables your organization to establish a security process which systematically optimizes your organization's security to a definable level. This process leads to a whole range of advantages (*TRT*):

- Proof of security to third parties (for clients, partners and legal purposes)
- Competitive advantage: 'documented quality' by an independent authority
- Cost reductions through transparent, optimized structures.
- Security becomes an integral part of business processes
- Knowledge and monitoring of the IT risks and residual IT risks
- Documentation of structures and processes
- Increased employee awareness of security
- Evaluation of the organization's processes from a security point of view.
- Prioritizing the security of the business operations: business continuity management
- Globally recognized standard
- Potential reduction in insurance premiums
- Referencing the IT process management standard (ITIL) to ISO 27001

Unfortunately, many organizations find difficulty to implement ISO 27001, including obstacles when measuring readiness level of an organizational implementation, document preparation as well as various scenarios and strategy information security deal with (*susanto et al, 2011a*) and (*siponen & willison. 2009*). Statistic shows a high gap between demand and actual implementation *[figure 1]*. An organization may face internal and external challenges to implement it, without proper planning, the following obstacles could create roadblocks for an effective information security, implementation (*Kosutic, 2010*), as follows:

- Expertise, employment, works and also translation of the term and concept of information security standards is highly required, may be beyond an organization resource. Refinement is a deterministic process, which is ubiquitously present in the world; most organizations have a number of information security controls, without a refine the controls tend to be somewhat disorganized and disjointed. A few essential controls are very difficult to understand, immeasurable and difficult to be implemented by an organizations (*susanto et al, 2011a*).
- Difficulty of information security standards selecting process within several existed standards, since every standard has unique characteristics, Each standard playing its own role and position in implementing ISMS. There are several standards for IT Governance which leads to information security such as PRINCE2, OPM3, CMMI,P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA,ITIL and COBIT (*susanto, almunawar and tuan, 2011b*).
- Necessity on provided assessment tool to measure an organization's readiness level of ISO 27001 implementation. Novelty framework to descript and viewing ISMS is required, while introducing new algorithm and mathematic models is something attracted (*susanto, almunawar & tuan, 2012b*).
- Compliance with ISO 27001 will require employees to embrace new security controls introduced by the standard. This organizational change could also affect company culture (*Kosutic, 2010*).
- The ISO 27001 compliance project may be seen as solely an initiative of the IT department rather than of importance to the entire organization (*Kosutic, 2010*).
- The project can be seen as just additional workload and its benefits may be overlooked (*Kosutic, 2010*).

Additional and proper communication at all levels of the organization about the project’s requirements, benefits, etc. will be needed (*Kosutic, 2010*).

IV. I-SOLUTION FRAMEWORK

In this section we introduced new framework to approaching object and organization, called by I-SolFramework, abbreviation from ***I***ntegrated ***Sol***ution for Information Security ***Framework***. The framework consists of six layers component *[figure 3]*: organization, stakeholder, tools & technology, policy, culture, knowledge. Let us briefly introduced the basic elements of I-SolFramework, profile as illustrated;

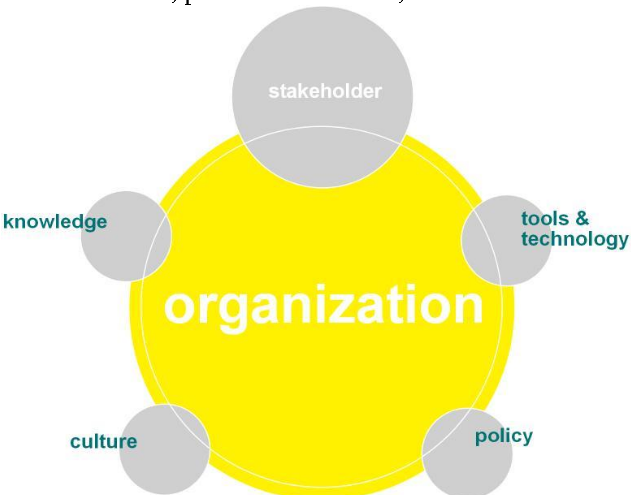


Figure 6. Integrated solution six domain framework

1. **Organization:** A social unit of people, systematically structured and managed to meet a need or to pursue collective goals on a continuing basis, the organizations associated with or related to, the industry or the service concerned (*BDO*).

2. **Stakeholder:** A person, group, or organization that has direct or indirect stake in an organization because it can affect or be affected by the organization's actions, objectives, and policies (*BDO*).

3. **Tools & Technology:** is the making, usage, and knowledge of tools, machines, techniques, crafts, systems or methods of organization in order to solve a problem or perform a specific function, divided into two categories (1) Tangible: blueprints, models, operating manuals, prototypes. (2) Intangible: consultancy, problem-solving, and training methods (*BDO*).

4. **Policy:** typically described as a principle or rule to guide decisions and achieve rational outcome(s), the policy of the country with regards to the future development of the industry or the service concerned (*BDO*).

5. **Culture:** determines what is acceptable or unacceptable, important or unimportant, right or wrong, workable or unworkable. ***Organization Culture:*** The values and behaviors that contribute to the unique social and psychological environment of an organization, its culture is the sum total of an organization's past and current assumptions (*BDO*).

6. **Knowledge:** is the sum of what is known and resides in the intelligence and the competence of people. In recent years, knowledge has come to be recognized as a factor of production (*BDO*).

Subsections follows, is described mathematical model on gaining a comprehensive and systematic overview. It starts by calculating the lowest level components of the framework, namely *assessment issues*.

$$(a) \rightarrow x_j = \sum_{k=1}^{n} \frac{[assessment\ issues]_k}{n}$$

$$x_j: assessment\ issues$$

$(\boldsymbol{a}) \rightarrow \boldsymbol{x_j}$ Indicate value of control of ISO 27001 which is resulting from *sigma* of section(s) assessment, divided by number of assessment issues on the lowest level.

$$(b) \rightarrow x_i = \sum_{j=1}^{n} \frac{[control]_j}{n}$$

$$x_i: domain$$

$(\mathbf{b}) \rightarrow \mathbf{x_i}$ Stated value of domain of ISO 27001 which is resulting from sigma of control(s) assessment, divided by number of control(s) contained at concerned level.
The new comprehensive modeling notation in a single mathematical equation, as follows;

$$\mathrm{x_h} = \sum_{i=1}^{n} \frac{[\mathrm{control}]_i}{n}$$

$$\mathrm{x_h} = \sum_{i=1}^{n} \frac{[\mathrm{b}]_i}{n}$$

$$\mathrm{x_h} = \sum_{i=1}^{n} \frac{\left[\sum_{j=1}^{n} \frac{[\text{assessment issues}]_j}{n}\right]_i}{n}$$

for six layer, or top level, equation will be:

$$\mathrm{x_h} = \sum_{i=1}^{6} \frac{\left[\sum_{j=1}^{n} \frac{\left[\sum_{k=1}^{n} \frac{[\text{assessment issues}]_k}{n}\right]_j}{n}\right]_i}{6}$$

Where;
k=assessment issues; J=control; I=domain (organization, stakeholder, tools & technology, policy, knowledge, and culture).

An algorithm is considered to be reliable and easy implementing in analyzing such problem. In addition, being able to measure readiness level of ISO 27001, can also be used to measure Multimedia Architecture (susanto & muhaya, 2010) Information Security Policy Compliance (susanto, almunawar, and tuan, 2012a).

V. SOFTWARE DESIGN & FEATURES

It should be noted here that some organizations may not only consider what ISO/IEC recommend, but they may also add to them special controls needed for the protection of their work, in order to achieve their business objectives (*Alfantookh, 2009*). It starts with the “21 essential security controls” of ISO 27001, which give the basic standard requirements of information security management. Controls are mapped on these domains and subsequently refined into “246 simple and easily comprehended elements”. These elements are subject to be reviewed and validated by specialized persons working on the field.
In general, i-Solution Modeling software consists of two major subsystems of e-assessment and e-monitoring *[figure 7]*. E-assessment to measure ISO 27001 parameters based on the proposed framework *[figure 6]* with 21 controls. Software is equipped by a login system, as user track record, as function to determined user’s patterns of assessment. Database updated automatically, query and retrieval of newest records neater structured and well organized. E-assessment utility is validating of the ISO 27001 parameters, through user interface provided by the system, follows i-solution framework rules that divided and segmented ISO 27001 essential controls into six main domains (*susanto et all, 2011c*) *[figure 8, 9 & 10]*.

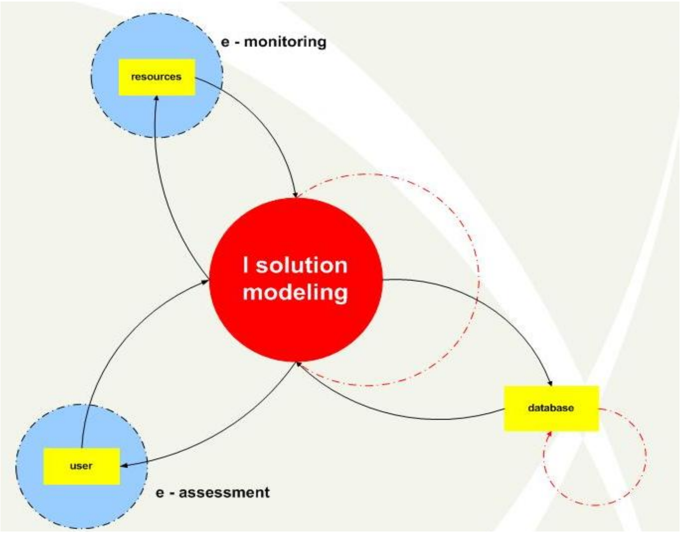
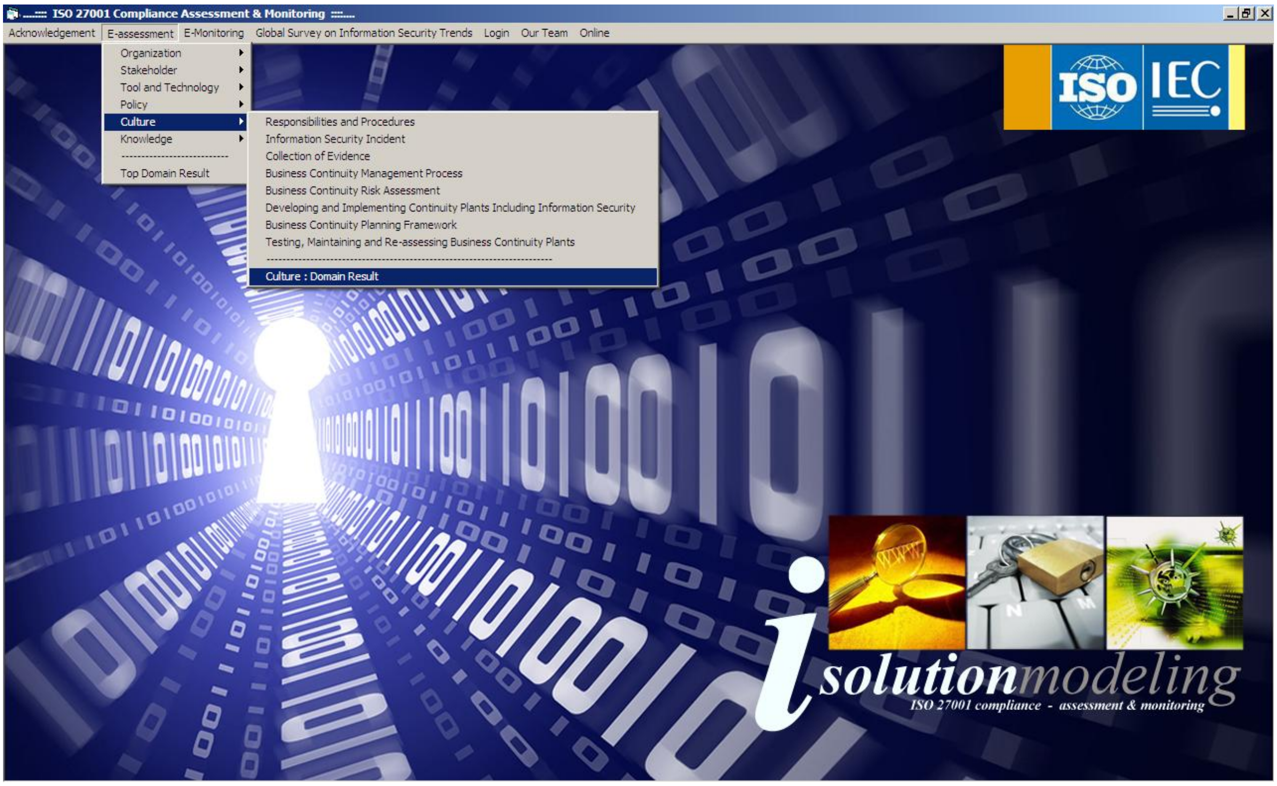
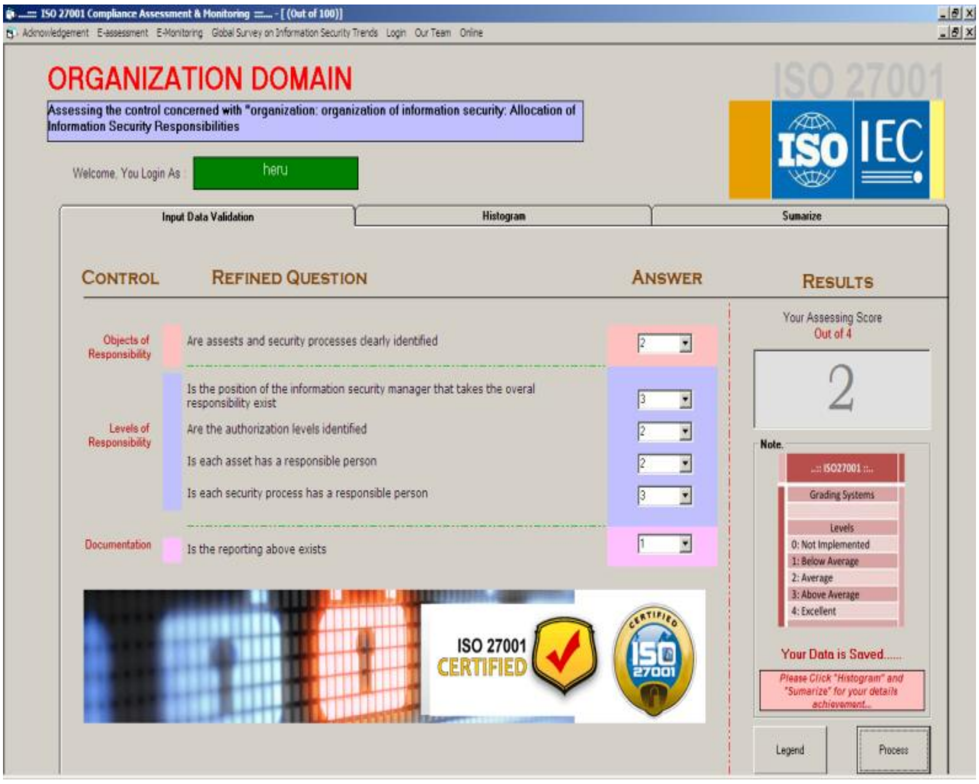


Figure 7. I-Solution Modeling diagram


.....::: ISO 27001 Compliance Assessment & Monitoring :::.....
Acknowledgement
E-assessment
E-Monitoring
Global Survey on Information Security Trends
Login
Our Team
Online
Organization
Stakeholder
Tool and Technology
Policy
Culture
Knowledge

Top Domain Result
Responsibilities and Procedures
Information Security Incident
Collection of Evidence
Business Continuity Management Process
Business Continuity Risk Assessment
Developing and Implementing Continuity Plants Including Information Security
Business Continuity Planning Framework
Testing, Maintaining and Re-assessing Business Continuity Plants
Culture : Domain Result
ISO IEC
isolutionmodeling
ISO 27001 compliance - assessment & monitoring

Figure 8. Integrated solution modeling software – ISO 27001 compliance



ORGANIZATION DOMAIN

Assessing the control concerned with "organization: organization of information security: Allocation of Information Security Responsibilities

Welcome, You Login As : heru

CONTROL	REFINED QUESTION	ANSWER
Objects of Responsibility	Are assests and security processes clearly identified	2
Levels of Responsibility	Is the position of the information security manager that takes the overal responsibility exist	3
	Are the authorization levels identified	2
	Is each asset has a responsible person	2
	Is each security process has a responsible person	3
Documentation	Is the reporting above exists	1

RESULTS

Your Assessing Score
Out of 4

2

Note.

..:: ISO27001 ::..
Grading Systems
Levels
0: Not Implemented
1: Below Average
2: Average
3: Above Average
4: Excellent

Your Data is Saved......

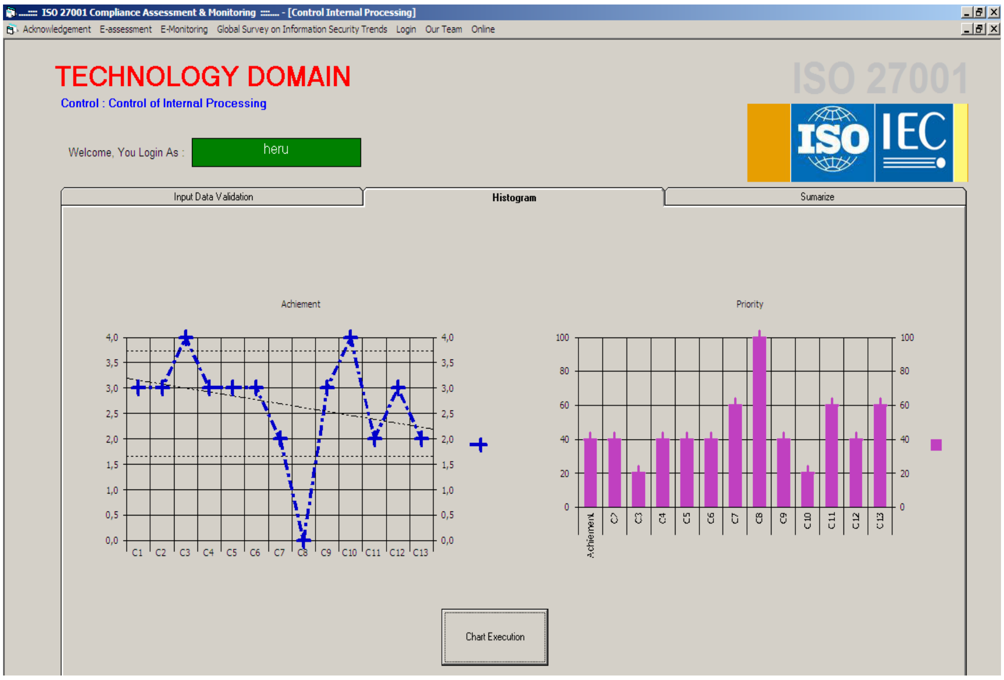
Please Click "Histogram" and "Sumarize" for your details achievement...

user is prompted to entering an achievements value based on ISO 27001 parameters, called by assessment issues. Level of assessment set out in range of 5 scales;

- *0 = not implementing*
- *1= below average*
- *2=average*
- *3=above average*
- *4=excellent*

As a measurement example, we described it in details to several steps of parameters assessment as follows [figure 6]:

- *Domain: "**Organization**"*
- *Controls: "**Organization of information security: Allocation of Information Security Responsibilities**"*
- *Assessment Issue: "**Are assets and security process Cleary Identified?**"*


.::: ISO 27001 Compliance Assessment & Monitoring :::.. - [Control Internal Processing]
Acknowledgement E-assessment E-Monitoring Global Survey on Information Security Trends Login Our Team Online
ISO 27001
ISO IEC
Input Data Validation
Histogram
Sumarize
Achiement
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0,0
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13
Priority
100
80
60
40
20
0
Achiement C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13
Chart Execution

TECHNOLOGY DOMAIN

Control : Control of Internal Processing

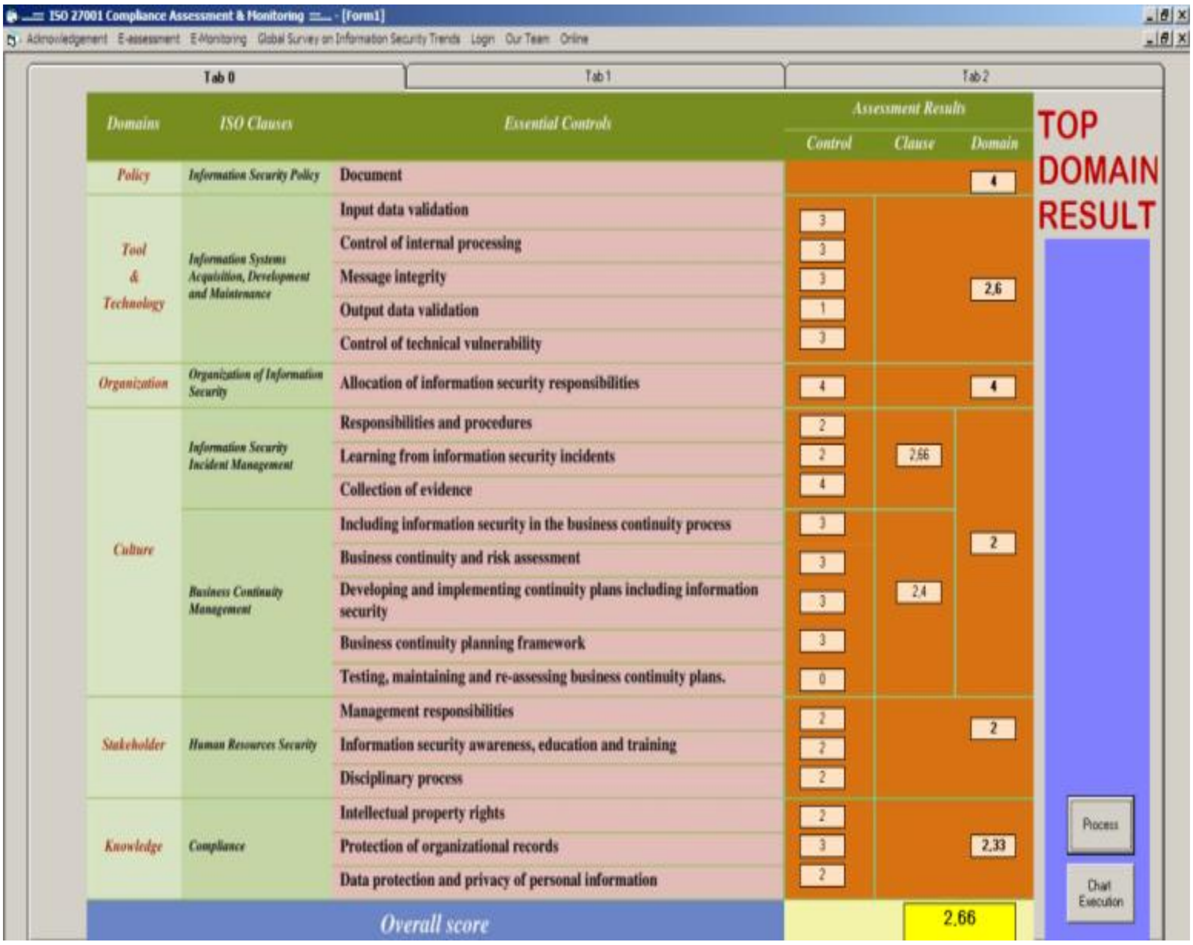
Welcome, You Login As : heru

Figure 9. Domain level measurement

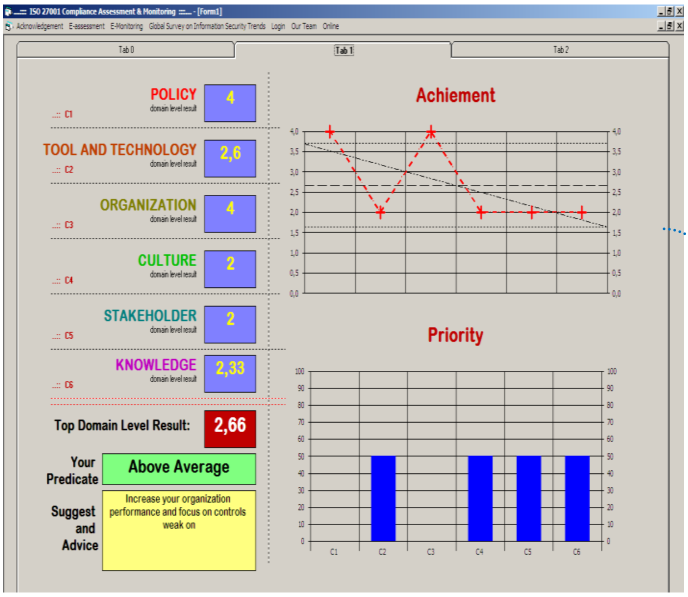
Histogram showed us details of the organization's achievement and priority. Both statuses are important in reviews of strongest and weakness point on an organization current achievement.

*As indicated is the system, "**Achievement**" declared the performance of an organization as final result of the measurement by validated by proposed framework.*

*Then another term is "**Priority**" indicated the gap between ideal values with achievement value. "Priority" and "achievement" showed inverse relationship. If achievement is high, then domain has a low priority for further work, and conversely, if achievement is low, then the priority will be high [figure 9].*


.::: ISO 27001 Compliance Assessment & Monitoring :::.. - [Form1]
Acknowledgement E-assessment E-Monitoring Global Survey on Information Security Trends Login Our Team Online
Tab 0
Tab 1
Tab 2
TOP DOMAIN RESULT
Process
Chart Execution

Domains	ISO Clauses	Essential Controls	Assessment Results		
			Control	Clause	Domain
Policy	Information Security Policy	Document			4
Tool & Technology	Information Systems Acquisition, Development and Maintenance	Input data validation	3		2,6
		Control of internal processing	3		
		Message integrity	3		
		Output data validation	1		
		Control of technical vulnerability	3		
Organization	Organization of Information Security	Allocation of information security responsibilities	4		4
Culture	Information Security Incident Management	Responsibilities and procedures	2	2,66	2
		Learning from information security incidents	2		
		Collection of evidence	4		
	Business Continuity Management	Including information security in the business continuity process	3	2,4	
		Business continuity and risk assessment	3		
		Developing and implementing continuity plans including information security	3		
		Business continuity planning framework	3		
		Testing, maintaining and re-assessing business continuity plans.	0		
Stakeholder	Human Resources Security	Management responsibilities	2		2
		Information security awareness, education and training	2		
		Disciplinary process	2		
Knowledge	Compliance	Intellectual property rights	2		2,33
		Protection of organizational records	3		
		Data protection and privacy of personal information	2		
Overall score					2,66



..::: C1 POLICY domain level result: 4

..::: C2 TOOL AND TECHNOLOGY domain level result: 2,6

..::: C3 ORGANIZATION domain level result: 4

..::: C4 CULTURE domain level result: 2

..::: C5 STAKEHOLDER domain level result: 2

..::: C6 KNOWLEDGE domain level result: 2,33

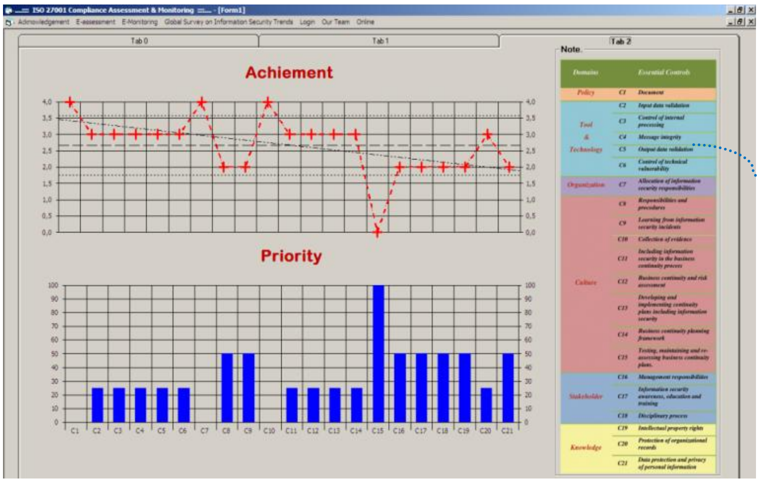
Top Domain Level Result: 2,66

Your Predicate: Above Average

Suggest and Advice: Increase your organization performance and focus on controls weak on

- ❖ *Final result out of 4 scale*
- ❖ *Final result out of 100 %*
- ❖ *Final predicate of assessment result (not implementing, below average, average, above average, excellent)*
- ❖ *Advice from the software regarding their final achievement, in which point their strongest area and also their weakness area.*

The overall score of all domains is shown in the Table to be "2.66 points". The domain of the "policy" scored highest at "4", and the domain of the "knowledge" scored lowest at "2". Ideal and priority figures are given to illustrate the strongest and weaknesses in the application of each control



Note

Domains		Essential Controls
Policy	C1	Document
Tool & Technology	C2	Input data validation
	C3	Control of internal processing
	C4	Message integrity
	C5	Output data validation
	C6	Control of technical vulnerability
Organization	C7	Allocation of information security responsibilities
Culture	C8	Responsibilities and procedures
	C9	Learning from information security incidents
	C10	Collection of evidence
	C11	Including information security in the business continuity process
	C12	Business continuity and risk assessment
	C13	Developing and implementing continuity plans including information security
	C14	Business continuity planning framework
	C15	Testing, maintaining and re-assessing business continuity plans.
Stakeholder	C16	Management responsibilities
	C17	Information security awareness, education and training
	C18	Disciplinary process
Knowledge	C19	Intellectual property rights
	C20	Protection of organizational records
	C21	Data protection and privacy of personal information

Represents condition of 21 essential controls of standards, overall condition of 21 essential controls in histogram style with current achievement and priority as well.

Figure 10. Top Domain level measurement

An illustrative example is presented to delineate usability level of its approach. Each question of the refined simple elements, a value associated with the example is given.

VI. CONCLUSION REMARKS

Protecting and guarding information on an organization is a big job that requires creativity and zero tolerance. Small breaches impact in the big effect, as seen in ISBS 2010. Producing software which helping an organizations to understand and measure is necessary. Novelty approach is proposed here as alternative formula on Measuring ISO 27001 Readiness Level. I-Solution modeling is software which has new paradigm framework, to make assessments and monitoring. Our framework and software offers convenience and measurement accuracy, also ease of analysis, so it is expected stakeholders can easily understand term and concept of ISO 27001, then perform their own assessment on readiness level of ISO 27001 implementation. It is expected to provide solutions to solved obstacles, challenges and difficulties in understanding standard term and concept, as well as assessing readiness level of an organization towards implementation of ISO 27001 for information security.

REFERENCES

[1] Abdulkader Alfantookh. An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. Computer Sciences, King Saud University. 2009.

[2] Ali Bitazar. About ISO27001 Benefits and Features. Obtained from http://www.articlesbase.com. 2009.

[3] Business Dictionary online (BDO). Obtained from www.businessdictionary.com

[4] Chris Potter & Andrew Beard. Information Security Breaches Survey 2010. Price Water House Coopers.Earl's Court,London.2010.

[5] Dejan Kosutic. 2010. ISO 27001 and BS 25999. Obtained from http://blog.iso27001standard.com

[6] Heru Susanto & Fahad bin Muhaya. Multimedia Information Security Architecture. @IEEE. 2010.

[7] Heru Susanto, Mohammad Nabil Almunawar, Wahyudin P Syam, Yong Chee Tuan, and Saad Hajj Bakry. I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution's Six Domains. Asian Transaction on Computer Journal. 2011a.

[8] Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan. Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Engineering and Computer Science. IJENS Publishers. 2011b.

[9] Heru Susanto, Mohammad Nabil Almunawar, Yong Chee Tuan, Mehmet Sabih Aksoy and Wahyudin P Syam. Integrated Solution Modeling Software: A New Paradigm on Information Security Review and Assessment. International Journal of Science and Advanced Technology. 2011c.

[10] Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan. I-SolFramework: An Integrated Solution Framework Six Layers Assessment on Multimedia Information Security Architecture Policy Compliance. International Journal of Engineering and Computer Science. IJENS Publishers. 2012a.

[11] Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan. I-SolFramework: as a Tool for Measurement and Refinement of Information Security Management Standard. On review paper. 2012b.

[12] Key fndings from the Global State of Information Security Survey®. 2012. Obtained from www.pwc.com/security. 2012.

[13] Mikko Siponen & Robert Willison. 2009. Information securitystandards: Problems and Solution. Information & Management 46(2009) 267-270. Elsevier Science Ltd.

[14] TÜV Rheinland Thailand Ltd (TRT). Advantages of ISO 27001 Certification. Obtained from http://www.tuv.com/th/en/

AUTHORS

Heru Susanto is a researcher at The Indonesian Institute of Sciences, Information Security & IT Governance Research Group, also was working at Prince Muqrin Chair for Information Security Technologies, King Saud University. He received BSc in Computer Science from Bogor Agriculture University, in 1999 and MSc in Computer Science from King Saud University, and nowadays as a PhD Candidate in Information Security System from the University of Brunei.

Mohammad Nabil Almunawar is a senior lecturer at Faculty of Business, Economics and Policy Studies, University of Brunei Darussalam. He received master Degree (MSc Computer Science) from the Department of Computer Science, University of Western Ontario, Canada in 1991 and PhD from the University of New South Wales (School of Computer Science and Engineering, UNSW) in 1997. Dr Nabil has published many papers in refereed journals as well as international conferences. He has many years teaching experiences in the area computer and information systems.

Yong Chee Tuan is a senior lecturer at Faculty of Business, Economics and Policy Studies, University of Brunei Darussalam, has more than 20 years of experience in IT, HRD, e-gov, environmental management and project management. He received PhD in Computer Science from University of Leeds, UK, in 1994. He was involved in the drafting of the two APEC SME Business Forums Recommendations held in Brunei and Shanghai. He sat in the E-gov Strategic, Policy and Coordinating Group from 2003-2007. He is the vice-chair of the Asia Oceanic Software Park Alliance.