IT Security and IT Governance Alignment: A Review

Norli Shariffuddin
Faculty of Computer and Mathematical Sciences,
Universiti Teknologi MARA (UiTM),
Shah Alam, Malaysia.
norli.shariffuddin@gmail.com

Azlinah Mohamed
Faculty of Computer and Mathematical Sciences,
Universiti Teknologi MARA (UiTM),
Shah Alam, Malaysia.
azlinah@tmsk.uitm.edu.my

ABSTRACT

This paper review and align IT Security (ITS) and IT Governance (ITG) that would address ITS strategic and its operational issues. These issues if not addressed accordingly, would lead to a financial aftermath that would put the business at risk and jeopardize the organization's sustainability in both short and long run. There have been studies that show, the lack of technical controls, lack of solid governance and improper oversight at the enterprise stakeholders' level would result to disastrous events. Thus, ITS and ITG has to go hand in hand in order to fortify the security posture of an enterprise. The goal is to roll out an ITS program that would have the best of ITG and ITS best practices. Rather than reinventing the wheel, the affected managers or organizations can adopt and adapt the existing frameworks available easily. There are a few common frameworks available, however there is lack of essential elements especially on ITS management and technical controls. This paper will look into these common ITS frameworks and lists its shortcomings to further understand the need for a better framework. In addition, frameworks that govern ITG will also be studied looking at its advantages and disadvantages. Thus, elements from ITS frameworks will be identified, analyzed and certain aspects extracted as common themes. The analysis shows, the themes depicted are strong management support, fit for purpose context that suits the organization, essential risk management, clearly defined of roles and responsibilities, the importance of training and awareness and the implementation of a quick win strategy. These five themes will be put into ITG practice blocks with respect to the Structure, Process and Relational Mechanisms that spans across People, Process and Technology domains. Finally, the construct named NORLI is proposed to align both ITG and ITS. In the future, NORLI will be tested for its ease of use, effectiveness and efficiency.

CCS CONCEPT

•Security and privacy → Formal methods and theory of security → Security requirements

Keywords

Framework; IT Governance; IT Security; Challenges; Problems; Strategic; Alignment; Value; Delivery; Management; Resources; Performances; Risks.

NISS2020, March 31-April 2, 2020, Marrakech, Morocco
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7634-1/20/03...$15.00
https://doi.org/10.1145/3386723.3387843

1. INTRODUCTION

ITG is such an interesting and a hot topic that had been discussed in yesteryears since the mid-90s. It had evolved into its own disciplines and rights from Corporate Governance. The definitions are broad and mainly discussed across researchers and authors in the recent years. The most agreed points among them is that ITG is the responsibility and the accountability of top management and board of directors, having the exact same commitment weightage as Corporate and Enterprise Governance in an organization. It is within their means of control to ensure that IT brings strategic approach and values to the organization [1,2,3,4]. These can be obtained through the ITG blocks which are Structure, Process and Relational Mechanisms. These blocks are defined by [3] and [5], where Structures points the responsibility and functions of IT executives and the related IT committees. Process on the other hand is interrelated with strategic decision making and monitoring. Relational Mechanisms promotes collaboration, participation and inclusion between IT, business and the stakeholders. Example of each blocks are illustrated in the figure below: -

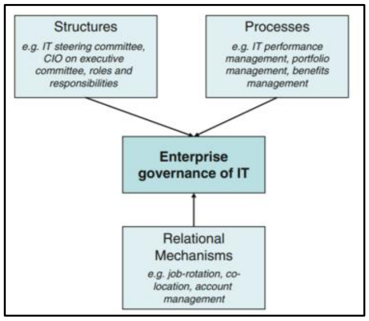

Structures
e.g. IT steering committee, CIO on executive committee, roles and responsibilities
Processes
e.g. IT performance management, portfolio management, benefits management
Enterprise governance of IT
Relational Mechanisms
e.g. job-rotation, co-location, account management

Figure 1. ITG Blocks as described by De Haes, S., & Van Grembergen, W. (2015).

ITG that comprises of these 3 blocks of practice had been proven to drive business performance and gain substantial competitive edge in the market. Numerous studies had proven such outcome [6,7,8,9,10]. However, in the recent years we've seen the emerging of cyberattacks that rampaging maliciously in both personal and enterprise cyberspace that could impose negative impacts to the organizations. Business could be bleeding monies [11,12,13] due to such threat and suffer reputational damage that could possibly lead to business loss forever. Two main examples such as data security breach [14] and ransomware [15,16] had caused such a global impact in the past three years due to its outrageous harm that has affected electronics tycoon [17], hospitals [18], retailers [19], social media (Facebook) [20] and others [21].

The best instance to illustrate was the WannaCry [16] ransomware attack that hit worldwide back in May 2017.It was a such a big wake up call for the organizations to step up and protect their organizations further. In order to combat these cyber-attacks and threats, ITG within organizations need to be coupling together with elements from IT Security framework as ITG alone is insufficient [21,22,23,24] and requires integration [25,26,27,28]. There are many ITS frameworks in the market to be adapted and adopted, but there would not be much clarity and clear cut on which framework to be used with the exception of Financial Service Industry (FSI) and Healthcare. These 2 sectors are heavily regulated by its own compliance control such as Sarbanes-Oxley Act (SOX) [29,30,31] and Health Insurance Portability and Accountability Act of 1996 (HIPAA) [29,32,] due to their sector's sensitivity, criticality and impact of their infrastructure to the people's lives.

But when it comes to the remaining industries mainly Hospitality, Government sectors, Property, Agriculture, Education, Aerospace, Transport, Telecommunication, Pharmaceutical, Food, Entertainment, News Media, Energy, Manufacturing, Electronics, there is no regulations and compliance in the centre to govern it all in terms of ITS elements. This is where framework like ISMS [33,34,35] and NIST [36,37,38] become quintessential. With not so far-fetched, organizations such as ISACA [39] (previously known as Information Systems Audit and Control Association which now goes by its acronym only) and International Information System Security Certification Consortium (ISC)2 [40] do have their own set of ITS framework that can be adopted through their certifications programmes namely Certified Information Security Manager (CISM) [41,43,44] and Certified Information Systems Security Professional (CISSP) [42,43,44] respectively. These frameworks have its own limitations in terms of adoption, complexity, competencies and capabilities required as well as the amount of resources needed.

In addition, when it comes to ITS framework, it should not be duplicated directly as it might be insufficient and inadequate to that specific organization, across horizontal and vertical industries. Each organization has its own distinct processes, rules, laws and regulations. The IT Security framework shall be developed and manifested within the organization itself, by itself based on the culture, belief, operation, environment and policy requirement. It is indeed a need to bridge both ITS and ITG in order to protect organization's interest against cyber-attacks and threats. [45,46,47,48].

Thus, this paper will focus into assessing existing ITG components and ITS frameworks based on research and academic papers. The end game with the ultimate goal is to proposed a customized framework that would align both ITG and ITS on the same page.

The rest of this article is structured as follows: Section 2 looks into related reviews of IT Governance while Section 3 provides the necessary background on the existing IT Security frameworks. Section 4 describes the research methodology carried out while in Section 5 presents a qualitative assessment on the frameworks highlighted and covers the constructs on the proposed framework. We will conclude the study in Section 6.

2. IT GOVERNANCE

ITG is all about due care and due diligence from the senior management level [49]. Both executive management and board of directors are totally responsible in ensuring IT for the organization would be sustainable and extendable in terms of fulfilling organization's strategies and objectives. ITG can occur at various different layers, bottom-up and top down directions as long as the objectives, strategic goals and directives are cascaded down from top management and board of directors. ITG has to come into play as IT is so intrinsic and embedded deeply within the organizations due to its dual-role criticality and complexity as business enabler [5,50,51] and to support business itself. It opens up a whole new world of opportunities and risks for the organizations that require actions to be taken prudently.

ITG also can be described as a process [52], in which without the recognition of both ownership and responsibility can be useless and meaningless. From the process, ITG can churn out set of rules, policies, procedures, regulations that would define and provide the assurance of the effectiveness, controlled and valuable operation of an IT entity. [53]

Other definitions on ITG according to Peterson [54] is an organization's IT systems portfolio under controlled and directed in an encapsulation of enterprise management systems. He also added that IT decision making is a shared responsibilities and rights across enterprise shareholders, in which inclusive of procedures and mechanisms as well in lieu with IT strategic decisions.

From another perspective, there is no specific ITG can be deployed and adopted as each of the set of ITG is tailored according to the industries or the business itself. This is mainly due to the reason of IT need to react and respond to the existence of the environment it resides on [55]. The review discussed five focus areas in ITG [56, 57,58] namely Strategic Alignment, Value Delivery, Risk Management, Performance Management and Resource Management.

Gashgari, et. al [59] worked quite a complete list of Critical Success Factors (CSFs) in their research. These CSFs are totally imperative in ensuring all the impacted concerns are addressed accordingly especially on how shall we start, how can we measure, what prioritizes and should be done in the first place. Based on their collective data gathered and findings (a total of 17), a framework was proposed that would map and align IT Governance values with the critical successful factors found. These factors alongside top management support is indeed crucial towards the ITG practicality within organizations.

In April 2012 COBIT version 5 was released. It had been hailed since then as the crown jewel when it comes to ITG [60]. According to ISACA, "COBIT 5 provides a comprehensive framework that assists enterprises to achieve their objectives for the governance and management of enterprise IT. COBIT 5 enables IT to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders." However, there seems to be a gap in terms of ITS management and technical controls in COBIT. A few studies [61,62] were carried out but unfortunately no evidence of both can be found.

When it comes to formulating ITS with ITG, [63] proposed IT Security Governance framework, spans through Leadership and Governance, Security Management and Organization, Security Policies, Security Program Management, User Security Management, and Technology Protection and Operations. These modules are then classified into 3 main domains – Strategic, Managerial and Operational, and Technical. This found framework was formulated based on the data comparisons between ISMS [33,34,35] and other findings [64,65] as well.

It is pretty much obvious that one approach alone is not the sole answer in governing information security, but an integrated method is indeed desired, and should be adopted accordingly in steering a successful outcome. Besides People, Process and Tool (Technology), one more segment [67] can be considered to cater the inclusion of Policy, Processes and Standard as well. It is believed that this additional component would strengthen the posture and exercise of IT Security Governance within organizations. It is also worth to note that People is the weakest link found across these studies [67,68,69,70,71]. All the above can be addressed through good policy, procedures and even standards if done thoroughly and accordingly that would be in sync with ITS and ITG.

The final significant key point of bridging ITS and ITG is to have all the related controls, which can be People, Process and Technology that is to be tailored in accordance to the business, organizations, industries and operating environments in order to support and meet the intended objectives [72].

3. IT SECURITY FRAMEWORKS

ISMS [33,34,35] laid out the methods and practices with the necessary controls of how organizations shall carry out and implement IT security practices. With Confidentiality-Integrity-Availability as their holy triad and the epitomic centre of such implementation activities, the aim is to secure and make reliable of communications and data exchange within organizations. The latest version based on year 2013 (numerous revisions had followed suit since then) which included the showcase of risk-based approach that proven to be super beneficial in this cyber resiliency era. Each of the controls highlighted in a list called Annex A [73,74] that comes with its own Control Objectives, highlighting on 'WHY' do we need to do this. It provides an interesting take and perspectives for those who responsible in understanding what and why they do it in such a way. However, even though it is perceived as richness and comprehensiveness of a framework, the ISO had its own pitfalls and it is indeed a standalone approach and doesn't integrate well with or into other larger ecosystems.

Subsequently, NIST [36,37,38] which consists of five main functions divided into several categories that covers specific technical and management activities (outcomes). This NIST [36,37,38] cybersecurity framework was intended as a collaboration guideline for both public and private sector in United States of America (USA). It is structured in a way that itself will allow organizations to describe their environment as it relates to cybersecurity at any given time, and what their current vulnerabilities are as a target for cybercriminals. It also has a risk management framework, in co-existence to support and supplement NIST [36,37,38]. Federal agencies in USA are required to implement this NIST [36,37,38] as part of their May 2017 Executive order. From the looks of it, NIST [36,37,38] seems to have it all under one roof. Due to such complex structures and advanced modules behind it, it can be such a huge roadblock to the newcomers and beginners that would want to explore both ITS and ITG together.

ISACA CISM [41,43,44] and ISC2 CISSP [42,43,44] on the other hand are the competitive head-to-head IT Security certification modules offered by private organizations with the best interest to serve the Cyber Security world. CISM offerings is solely management focused that covers four domains of knowledge while CISSP with 8 domains are both technical and managerial approach. Despite the competitiveness, IT professionals around the world tend to see that both certifications modules are actually complementing each other to a better a secure digital cyberspace. CISM domains are Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management and Information Security Incident Management. CISSP on the other hands have more in-depth and specific domains which are control-oriented such as Security Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations and Software Development Security. Both CISM and CISSP are great but seems to miss the finesse part when it comes to the intention to bridging them as part of IT Governance.

All in all, based on the above, it is indeed a challenge and can become a huge dilemma of which to choose as the correct framework and standards for IS governance and Information Security. Those highlighted frameworks are really promising and yet impose a fairly difficult options in terms of varieties of choices to be adopted and adapted within organizations. As highlighted earlier, the lack of a single standards framework is a completely exhaustive and it is expected for the organizations to run through numerous available frameworks, do their own due care and due diligence of analysis to see what suits and what works for them. We acknowledge that those frameworks are different in many aspects but they do have some overlap and similarities. For more value added to the framework development, the necessary aspects also need to be weighed in and diversified in accordance to People, Process and Technology spectrum.

4. RESEARCH METHODOLOGY

Research Methodology carried out for this paper was qualitative method based on secondary data. In collecting the needed information, a scoping review technique was adopted based on relevant sources such as ScienceDirect, Scopus, ACM and Springer. The keywords used for the search process ranging from such as IT Governance, IT Security, frameworks, cybersecurity in ensuring that the most relevant and appropriate articles are selected and cited in this writing. Once all those are collected, core elements of IT Governance are the entities examined as well as the essence of IT Security frameworks available in the cyberspace. The reviews are collating into elements namely ISMS with 7 clauses and 114 controls, NIST CSF 5 core elements with 23 sub nodes, CISM and its 4 domains and CISSP with 8 domains of knowledge. These security elements then will be analyzed in identifying consistent themes, in which then be mapped (where applicable) according to Strategic Alignment, Value Delivery, Risk Management, Resources Management and Performance Management, segregated according to Structure, Process and Relational Mechanisms blocks that will be part of the construct intended as the outcome of this study as shown in Figure 2 below.

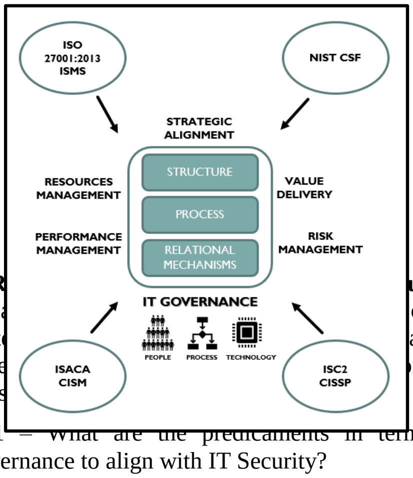


Figure 2. R utshell

The main resea can be an imperative int ance as a whole sensible ns rise to the occasions s

- RQ1 – What are the predicaments in terms of IT Governance to align with IT Security?

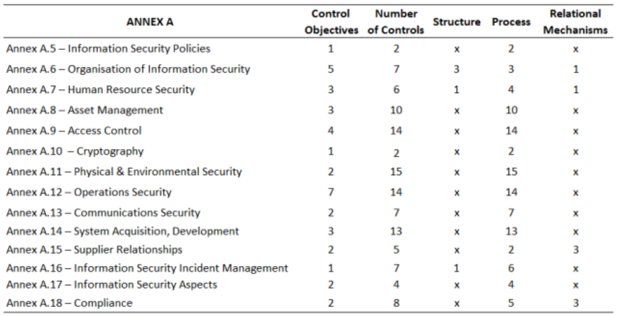
- RQ2 – What are the IT Security frameworks being used right now?
- RQ3 – What are the quintessential elements that can bridge IT Governance and IT Security to become a whole tailored framework?

5. ANALYSIS AND DISCUSSIONS

ISMS [33,34,35] has a total of 10 clauses and 114 controls in so called ANNEX A [73,74] to be reviewed and adapted accordingly. They're broken down into 3 defined blocks which are Structure (covers Leadership, Roles and Responsibilities), Process and Relational Mechanisms (Collaborations, Trainings, Stakeholders, Partnerships) based on all the controls involved.

It was identified that quite a handful to be under Process classifications at total of 101 controls to be exact. Relational Mechanisms comes second with 8 controls while Structure is at the lowest with 5 controls. However, it is not the contest of champions of many but rather the significant of such controls play in influencing and empowering the IT Security and Governance in organizations. Based on the figure analyzed, Structure is the most important in executing the security governance programmes. Next is to identify the related stakeholders involved, in which then all the necessary processes and controls will follow suit to make a cycle. The breakdown is illustrated in the Table 1 below.

Table 1. ISMS [33,34,35] Governance Posture by Structure, Process and Relational Mechanisms



ANNEX A	Control Objectives	Number of Controls	Structure	Process	Relational Mechanisms
Annex A.5 – Information Security Policies	1	2	x	2	x
Annex A.6 – Organisation of Information Security	5	7	3	3	1
Annex A.7 – Human Resource Security	3	6	1	4	1
Annex A.8 – Asset Management	3	10	x	10	x
Annex A.9 – Access Control	4	14	x	14	x
Annex A.10 – Cryptography	1	2	x	2	x
Annex A.11 – Physical & Environmental Security	2	15	x	15	x
Annex A.12 – Operations Security	7	14	x	14	x
Annex A.13 – Communications Security	2	7	x	7	x
Annex A.14 – System Acquisition, Development	3	13	x	13	x
Annex A.15 – Supplier Relationships	2	5	x	2	3
Annex A.16 – Information Security Incident Management	1	7	1	6	x
Annex A.17 – Information Security Aspects	2	4	x	4	x
Annex A.18 – Compliance	2	8	x	5	3

As shown above, Management and Leadership support is essential in order to make things work for ISMS [33,34,35]. The stakeholders in the relevant business units and partnerships comes second in influencing the organizational situation and directions. Last but not least, all the required processes and controls need to be in place in order to improve both governance and IT Security posture within organizations.

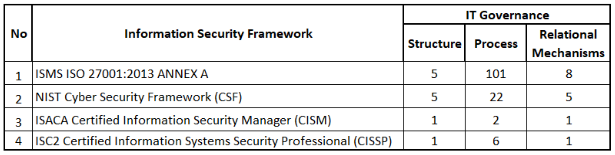
For NIST [36,37,38] cybersecurity framework, it encompasses and focuses on Identify-Protect-Detect-Response-Recover model. Each of the functions has its own process/technical controls. With Risk Management to supplements and complements such framework, the author can simplify and concluded that such framework is risk-based approach, where controls that can come through via People, Process and Technology are deployed and implemented based on the risks identified. To oversee these risks, management and leadership support is a total must or else the model won't be working effectively as intended at all. Each of the functions require Plan, Develop and Implement (PDI) and if there is indeed lacking of overview and oversight from the management, it will fail indefinitely. Hence, the key takeaway for NIST [36,37,38] cybersecurity would be Management Buy in and Risk Management.

Moving onto ISACA CISM [41,43,44], it is more management and strategy oriented and have lesser technical coverage in a cursory way. It provides more holistic understanding on information security systems and management. All in all, through the 4 domains ISACA CISM emphasizes on the Management involvement with a defined roles and responsibilities required for a successful IT Security programmes. Risk Management plays a key role in such module as well and CISM definitely fulfills the Strategic Alignment and Value Delivery within IT Governance space.

ISC2 CISSP [42,43,44] on the other hand, is much more focusing on technical controls. All these technical controls can be deployed and implemented as per Technology aspects within the People-Process-Technology spectrum. It has the best technical controls in details and highly sought after by IT Security practitioners throughout the world. These controls are elaborated in the forms of Preventive, Detective, Corrective and Deterrent forms that would be beneficial in strategic planning phase as well as in day to day operations.

Summing up all the above frameworks from the 3 defined blocks in IT Governance would result to the following table below.

Table 2. IT Governance Posture by Structure, Process and Relational Mechanisms between IT Security Frameworks



No	Information Security Framework	IT Governance		
		Structure	Process	Relational Mechanisms
1	ISMS ISO 27001:2013 ANNEX A	5	101	8
2	NIST Cyber Security Framework (CSF)	5	22	5
3	ISACA Certified Information Security Manager (CISM)	1	2	1
4	ISC2 Certified Information Systems Security Professional (CISSP)	1	6	1

A consistent theme throughout the 4 frameworks is that Management Support is the center of the universe when it comes to IT Security. It is vital to understand the business and the organization itself so that a fit for purpose context can be established to avoid unnecessary investments and resources allocations. Next is Risk Management comes into play, where all the controls that reacts to the risk are deployed and implemented accordingly across People, Process and Technology segments. Another insight gained through the analysis is that Roles and Responsibilities are imperative to make both IT Governance and IT Security work. Building up the right capabilities and competencies is one of the main highlights that comes hand in hand with education and awareness programmes as People is often perceived and proven to be the weakest link in IT Security. Last but not least, all the controls need to be invested, planned, executed and monitored via People, Process and Technology aspects.

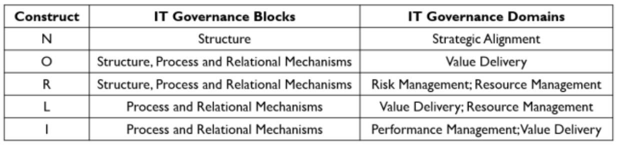
Based on this findings and discussion, a customized construct is then developed, which covers 5 main security themes that can be integrated into ITG. They are: -

- Need management buy in, support and directions for successful outcomes.
- Organizational context that would deliver the best values.
- Risks, Roles and Responsibilities must be defined.
- Learning is imperative for awareness and competencies buildup.

- Implement quick wins strategy.

In summary, this construct in abbreviation is ‘NORLI’, can be the kick-starter for lean-type of approach, that is bridging both ITS and ITG. It is illustrated in the table below.

Table 3. The NORLI construct



Construct	IT Governance Blocks	IT Governance Domains
N	Structure	Strategic Alignment
O	Structure, Process and Relational Mechanisms	Value Delivery
R	Structure, Process and Relational Mechanisms	Risk Management; Resource Management
L	Process and Relational Mechanisms	Value Delivery; Resource Management
I	Process and Relational Mechanisms	Performance Management;Value Delivery

The construct is complementing the ITG posture according to the defined blocks and domains by incorporating ITS themes from the assessed ITS frameworks in the earlier part. The construct was tested on an IT project and the results of the preliminary testing are as discussed below.

5.1 [N]eed management buy in, support and directions for successful outcomes

Management support is mandatory in ensuring the right drive are behind any IT investments and portfolio in organizations. Failing in such will resulted to more catastrophically failures that would impact the business growth. ITS is a new challenge to the executive management level and some even take such thing into granted. Hence the need to have the management buy in as the main priority in the construct. In the preliminary testing executed, this construct is the main number one key as the affected organization doesn’t have IT as its core business. However, the management understands that both ITG and ITS is significant towards business sustainability and growth, hence great commitment and support were provided in terms of financial and strategic directions in building up a hybrid ITG/ITS portfolio in the company

5.2 [O]rganizational context that would deliver the best values

Rather than spending lavishly and implement all available technological solutions out there in market, it is vital to have the necessary understanding of the business and organizational context in the first place. It will definitely be helpful especially when it comes to the required planning and the roll out of controls, as they can be done accordingly fit-for-purpose to avoid excessive resource utilization in terms of money, people and time. It doesn’t make any sense to deploy the same as Fort Knox’s setup, as we need to benchmark across horizontal industries and vertical sectors as well. From the preliminary testing, the needed implementations carried out on both ITG and ITS were deemed beneficial. The support, fulfill and achieve the strategic alignments through fit for purpose goals. A great example would be question as such – Do we need a Web Application Firewall (WAF)? If you know your environment, depending on the organizations there will be feedback where some might say ‘Yes’ and some ‘No’.

5.3 [R]isks, Roles and Responsibilities must be defined

Risk management is oftenly neglected and is not a usual practice across organizations. However, when it comes to ITS, the business and the organizations need to be aware of risk. ITS is all about risk and control. Once all these 3 had been prioritized and in place, we shall look into having the needed roles and responsibilities defined in order to have those three managed effectively. For the preliminary testing, risk and control is something out of the norm for the daily IT Operational Support activities. Thus, in order to be ITS/ITG centric, it has to be a risk-control approach as well. A risk register was developed for a better visibility towards any gaps and vulnerabilities. With the findings, required controls are assessed and evaluated for further improvements. Such approach would also justify the Return-On-Investment (ROI) of controls deployed, be it in terms of technologies, processes or people. When it comes to people that involved with ITS/ITG, its s a rule of thumb to have job segregations to avoid any conflicts of interests. With the support from management earlier, roles and responsibilities related to ITS/ITG are now can be defined. Related job functions were established, and with such came the relevant metrics and monitoring for ITS/ITG hybrid portfolio.

5.4 [L]earning is imperative for awareness and competencies build up.

The learning part has to come in 2-pronged approach in terms of awareness and competencies development. Awareness is targeted to the mass public, all employees within the organization and the competencies is concentrating on getting the right ITS/ITG technical knowledge and skills to the IT staff. This is proven to be true as per preliminary testing performed. As more and more awareness materials in terms of posters and weekly email update related to ITG/ITS were communicated to the mass public, the number of incidents related to ITS especially phishing went down over time. As for the IT staff, when they have more exposure towards ITS/ITG and gain competencies through formal training, more deployed controls can be revisited for improvements. They as well can take up and rolling out new security controls in order to improve the security posture in the said organization.

5.5 [I]implement quick wins strategy

The last theme which is implementing quick wins strategy is to kick off with what we have at the current capacity and strength to spearhead ITS/ITG programmes in the organization. Based on the preliminary testing result, such strategy has immediate benefit and can be delivered quickly as it leveraged on the existing controls (people, process and technology) at hand. As example, application whitelisting, server hardening policy, both Windows and Anti-Virus (AV) updates roll out can be triggered, tracked, monitored and the results can be obtained and managed even with a skeleton crew in a short period of time.

6. CONCLUSIONS

The main motivation behind this paper is to review the alignment between ITG and ITS and develop a construct as an outcome of such study. The biggest challenge is that there are many frameworks available and most of the times had driven the affected managers and implementers to the wall in identifying what really suits and works for their organizations.

Rather than building a comprehensive and extensive framework, the author intends to look at the basic principles across the ITS frameworks available, then move on to identify consistent and similar theme that would be the siren song. These elements are then established into a separate 5 pillars in their own circles of power, influence and control to be executed with, called NORLI construct. It is a lean approach and has been tested in a preliminary testing wit promising outcome. Further testing to be validated, where subsequent studies might follow suit that would cover both quantitative and qualitative method that would make such framework acceptable and feasible in the future.

7. ACKNOWLEDGMENTS

We would like to express our thanks to the Faculty of Computer and Mathematical Sciences, UiTM for the support rendered thus far, and to anonymous reviewers for their useful suggestions.

8. REFERENCES

[1] ISACA Board Briefing on IT Governance 2nd Edition. (2003) Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx

[2] Weill, Peter and Ross, Jeanne W., IT Governance on One Page (2004). MIT Sloan Working Paper No. 4517-04; CIS Research Working Paper No. 349

[3] S. De Haes and W. Van Grembergen (2005), "IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group," Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, , pp. 237b-237b.

[4] P. M. A. Ribbers, R. R. Peterson and M. M. Parker (2002), "Designing information technology governance processes: diagnosing contemporary practices and competing theories," Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Big Island, HI, , pp. 3143-3154.

[5] De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of IT. Enterprise Governance of Information Technology, pp11–43

[6] Shelly Ping-Ju Wu, Detmar W. Straub and Ting-Peng Liang (2015), “How Information Technology Governance Mechanisms And Strategic Alignment Influence Organizational Performance: Insights From A Matched Survey Of Business And It Managers.” MIS Quarterly Vol. 39 No. 2, pp. 497-518

[7] Lazic, Miroslav; Groth, Martin; Schillinger, Christian; and Heinzl, Armin (2011), "The Impact of IT Governance on Business Performance"Association for Information Systems AIS Electronic Library (AISeL).

[8] Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). “The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms.” International Journal of Accounting Information Systems, 15(1), pp. 66–81.

[9] Zhang, P., Zhao, K., & Kumar, R. L. (2016). “Impact of IT Governance and IT Capability on Firm Performance.” Information Systems Management, 33(4), pp. 357–373.

[10] Ryu, K. S., Park, J. S., & Park, J. H. (2015). “The Influence of IT Investment and IT Governance on Corporate Performance of Multibusiness Firms.” Proceedings of the 2015 International Conference on Big Data Applications and Services - BigDAS ’15.

[11] Smith, G. S., & Amoruso, A. J. (2006). “Using real options to value losses from cyber attacks”. Journal of Digital Asset Management, 2(3-4), pp. 150–162.

[12] Antonescu, M., & Birău, R. (2015). “Financial and Non-financial Implications of Cybercrimes in Emerging Countries”. Procedia Economics and Finance, 32, pp. 618–621

[13] Maria Cristina Arcuri, Marina Brogi and Gino Gandolfi (2017). "How does cyber crime affect firms? The effect of information security breaches on stock returns". In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)

[14] Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. The European Physical Journal B, 89(1).

[15] Brewer, R. (2016). “Ransomware attacks: detection, prevention and cure. Network Security”, 2016(9), pp. 5–9.

[16] Savita Mohurle Manisha Patil 2017 . “ A brief study of Wannacry Threat: Ransomware Attack “ International Journal of Advanced Research in Computer Science.

[17] Sigi Goode, Hartmut Hoehle, Viswanath Venkatesh and Susan A. Brown (2017). “User Compensation As A Data Breach Recovery Action: An Investigation Of The Sony Playstation Network Breach”.MIS Quarterly Vol. 41 No. 3, pp. 703-727

[18] Collier, R. (2017). NHS ransomware attack spreads worldwide. Canadian Medical Association Journal, 189(22), E786–E787. doi:10.1503/cmaj.1095434

[19] Manworren, N., Letwat, J., & Daily, O. (2016). “Why you should care about the Target data breach”. Business Horizons, 59(3), pp.257–266.

[20] The Guardian Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[21] Lawrence Trautman, Jason Triche & James Wetherbe (2013). “Corporate Information Technology Governance Under Fire”. Journal of Strategic Information and Studies

[22] Savtschenko, M., Schulte, F., & Voß, S. (2017). “IT Governance for Cyber-Physical Systems: The Case of Industry 4.0”.

[23] Debreceny, R. S. (2013). “Research on IT Governance, Risk, and Value: Challenges and Opportunities”. Journal of Information Systems, 27(1), pp. 129–135.

[24] Dawes, S. S. (2008). “The Evolution and Continuing Challenges of E-Governance.” Public Administration Review, 68, pp. S86–S102.

[25] Mathew Nicho, Suadad Muamaar (2016). "Towards a Taxonomy of Challenges in an Integrated IT Governance Framework Implementation.Journal of International Technology and Information Management Volume 25 Issue 2

[26] Selig, G. J. (2018). “IT Governance — An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Competitive Advantage.” 2018 Portland International Conference on Management of Engineering and Technology (PICMET).

[27] Carcary, M., Renaud, K., McLaughlin, S., & O’Brien, C. (2016). “A Framework for Information Security Governance and Management.” IT Professional, 18(2), pp.22–30.

[28] Bobbert, Y., & Mulder, H. (2015). “Governance Practices and Critical Success Factors Suitable for Business Information Security”. International Conference on Computational Intelligence and Communication Networks (CICN).

[29] Lewis, K. (2017). “Security Certification and Standards Implementation”. Computer and Information Security Handbook, pp.557–563.

[30] Karanja, E. and Zaveri, J. (2014), "Ramifications of the Sarbanes Oxley (SOX) Act on IT governance", International Journal of Accounting & Information Management, Vol. 22 No. 2, pp. 134-145

[31] Westland, J. C. (2019). “The Information Content of Sarbanes-Oxley in Predicting Security Breaches”. Computers & Security.

[32] Cousins, K. (2016). “Health IT Legislation in the United States: Guidelines for IS Researchers”. Communications of the Association for Information Systems.

[33] Shojaie, B., Federrath, H., & Saberi, I. (2015). “The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001”. 10th International Conference on Availability, Reliability and Security.

[34] Gritzalis, S., Weippl, E. R., Katsikas, S. K., Anderst-Kotsis, G., Tjoa, A. M., & Khalil, I. (Eds.). (2019). “Trust, Privacy and Security in Digital Business”. Lecture Notes in Computer Science.

[35] Humphreys, E. (2018). The Future Landscape of ISMS Standards. Datenschutz Und Datensicherheit - DuD, 42(7), pp. 421–423.

[36] Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). “A security review of local government using NIST CSF: a case study”. The Journal of Supercomputing.

[37] Srinivas, J., Das, A. K., & Kumar, N. (2018). “Government regulations in cyber security: Framework, standards and recommendations.” Future Generation Computer Systems.

[38] Aminzade, M. (2018). “Confidentiality, integrity and availability – finding a balanced IT framework”. Network Security, 2018(5), pp. 9–11.

[39] About ISACA (2019). Retrieved from https://www.isaca.org/about-isaca/Pages/default.aspx

[40] (ISC)²: The World’s Leading Cybersecurity Professional Organization. (2019) Retrieved from https://www.isc2.org/About

[41] Certified Information Security Manager (CISM) Retrieved from http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

[42] CISSP – The World's Premier Cybersecurity Certification Retrieved from https://www.isc2.org/Certifications/CISSP

[43] Furnell, S., Fischer, P., & Finch, A. (2017). “Can’t get the staff? The growing need for cyber-security skills.” Computer Fraud & Security, 2017(2), pp. 5–10.

[44] Benslimane, Y., Yang, Z., & Bahli, B. (2016). “Information Security between Standards, Certifications and Technologies: An Empirical Study”. International Conference on Information Science and Security (ICISS).

[45] Lidster, W., & Rahman, S. S. M. (2018). “Obstacles to Implementation of Information Security Governance”.17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

[46] De Smet, D., & Mayer, N. (2016). “Integration of it governance and security risk management: A systematic literature review.” International Conference on Information Society (i-Society).

[47] Borgman, H., Heier, H., Bahli, B., & Boekamp, T. (2016). “Dotting the I and Crossing (out) the T in IT Governance: New Challenges for Information Governance.” 49th Hawaii International Conference on System Sciences (HICSS).

[48] De Bruin, R., & von Solms, S. H. (2016). “Cybersecurity Governance: How can we measure it?”IST-Africa Week Conference.

[49] ISACA Board Briefing on IT Governance 2nd Edition. (2003) Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx

[50] Amit Ghildyal and Elizabeth Chang (2017) “IT Governance, IT/Business Alignment and Organization Performance for Public Sectors”. Journal of Economics, Business and Management, Vol. 5 (6).

[51] Tim Huygh,Steven De Haes,Anant Joshi,Wim Van Grembergen (2018). “Answering Key Global IT Management Concerns Through IT Governance and Management Processes: A COBIT 5 View”. Proceedings of the 51st Hawaii International Conference on System Sciences

[52] Rahimi, F., Møller, C., & Hvam, L. (2016). “Business process management and IT management: The missing integration.” International Journal of Information Management, 36(1), pp. 142–154.

[53] Robert Wayne Gregory, Evgeny Kaganer, Ola Henfridsson & Thierry Jean Ruch (2018). “IT Consumerization And The Transformation Of IT Governance.” MIS Quarterly Vol. 42(4)

[54] Ryan Peterson (2004) “Crafting Information Technology Governance”. Information Systems Management, 21:4, 7-22

[55] Agarwal, R., & Sambamurthy, V. (2002).”Principles and Models for Organizing the IT Function”. MIS Quarterly Executive, 1.

[56] Van Grembergen, W., De Haes, S. and Guldentops, E.

(2004), “Structures, Processes and Relational Mechanisms for IT

Governance” Strategies forInformation Technology Governance

[57] Aasi, P., Rusu, L., & Vieru, D. (2017). “The Role of Culture in IT Governance Five Focus Areas”. International Journal of IT/Business Alignment and Governance, 8(2), pp. 42–61.

[58] Tsai, W.-H., Chou, Y.-W., Leu, J.-D., Chen, D. C., & Tsaur, T.-S. (2013). “Investigation of the mediating effects of IT governance-value delivery on service quality and ERP performance”. Enterprise Information Systems, 9(2), 139–160.

[59] Gashgari, Ghada & Walters, Robert & Wills, Gary. (2017). A Proposed Best-practice Framework for Information Security Governance. 295-301.

[60] Bartens, Y., Haes, S. de, Lamoen, Y., Schulte, F., & Voss, S. (2015). “On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5.” 48th Hawaii International Conference on System Sciences.

[61] Laksono, H., & Supriyadi, Y. (2015). “Design and implementation information security governance using Analytic Network Process and cobit 5 for Information Security a case study of unit XYZ.” International Conference on Information Technology Systems and Innovation

[62] Durachman, Y., Chairunnisa, Y., Soetarno, D., Setiawan, A., & Mintarsih, F. (2017). “IT security governance evaluation with use of COBIT 5 framework: A case study on UIN Syarif Hidayatullah library information system.” 5th International Conference on Cyber and IT Service Management (CITSM).

[63] A. Da Veiga PhD & J. H. P. Eloff PhD (2007) “An Information Security Governance Framework” Information Systems Management, 24:4, pp.361-372

[64] Eloff, J. H. P. & Eloff, M. (2005). “Integrated Information Security Architecture”, Computer Fraud and Security, 2005 (11), 10–16.

[65] McCarthy, M. P. & Campbell, S. (2001). “Security Transformation”.McGraw-Hill: New York.

[66] Tudor, J. K. (2000). “Information Security Architecture—An integrated approach to security in an organization”. Boca Raton, FL: Auerbach.

[67] M. Asgarkhani, E. Correia and A. Sarkar, "An overview of information security governance," 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, 2017, pp. 1-4.

[68] Asgarkhani, M (2013).: “Corporate ICT Governance: A Tool for ICT Best Practice.” Proceedings of the International Conference on Management,Leadership, and Governance.

[69] BBC. The Chernobyl disaster (2006). Retrieved from http://www.bbc.co.uk/dna/h2g2/A2922103.

[70] Franz, M., Miller, D., Byres, EJ (2004).: “The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. IEEE Conf. International Infrastructure Survivability Workshop

[71] Nicholson A., Webber S., Dyer S., Patel T. and Janicke H (2012).: “SCADA security in the light of Cyber-Warfare”, Journal of Computers & Security, 31, pp. 418-436.

[72] Robert S. Coles & Rolf Moulton (2003) – “Operationalizing IT Risk Management: Operationalizing IT Risk Management”. Computer Security 22, pp. 487-493.

[73] Rukh, L., & Malik, A. A. (2017). “Swiss army knife of software processes generic framework of ISO 27001 and its mapping on resource management.”International Conference on Communication Technologies (ComTech).

[74]Carvalho, C., & Marques, E. (2019). “Adapting ISO 27001 to a Public Institution.” 14th Iberian Conference on Information Systems and Technologies (CISTI)