REFERENCE LIST

Asia Pacific Networking Group, e-srilanka,viewed 18th May 2011, <http://www.apng.org/museum/pdf/e-srilanka.pdf >.

Behara, R, Huang, CD & Hu, Q 2005, A system dynamics model of Information Security Investments,viewed 30th January 2011, <http://www.is2.lse.ac.uk/asp/aspecis/20070016.pdf >.

Bodin, LD, Gordon, LA & Loeb, MP 2005, Evaluating Information Security Investments Using Analytical Hierarchy Process, Communications of the ACM, 48(2), pp 79-83.

Bowen, P, Kissel, R, Scholl, M, Robinson, W, Stansfield, J & Voldish, L 2009, Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process(draft),viewed 8th August 2011,<http://csrc.nist.gov/publications/drafts/800-65-rev1/draft-sp800-65rev1.pdf >.

Brent, RR & Michael, PG 2006, Private Sector Cyber Security Investment Strategies: An Empirical Analysis,viewed 7th May 2011,<http://weis2006.econinfosec.org/docs/18.pdf >.

Cavusoglu, H, Mishra, B & Raghunathan S 2004, A model for evaluating IT security investments, viewed 2nd February 2011,<http://utd.edu/~huseyin/paper/investment.pdf >.

Dancho,D 2003, Building and Implementing a Successful Information Security Policy, viewed 14th May 2011,<http://dl.packetstormsecurity.net/papers/general/security-policy.pdf >.

Darkenwald, GG 2005, “Field Research and Grounded Theory” , in Changing approaches chapter five,viewed 15th May 2011,<http://www-distance.syr.edu/cach5 .html >.

Dawson, C 2002, Practical Research Methods,viewed 20th April 2011, <http://www.uady.mx/~contadur/sec-cip/articulos/libros_online/educacion/0506PracticalResearchMethods.pdf>.

Dynes, S 2004, What drives Information Security Investment? Institute f or security technology studies,viewed 20th May 2011,<http://www.tuck.dartmouth.edu/cds-uploads/press/pdf/ISTSDynes.pdf >.

Fernandez, WD 2005, The grounded theory method and case study data in IS research:issues and design,viewed 25th May 2011,<http://epress.anu.edu.au/info_ systems/part-ch05.pdf >.

Foster, S & Pael, B 2002, *Analysis of Return on Investment for Information Security*,viewed 2nd February2011,<http://www.getronics.com/NR/rdonlyres/ejhsokxgywr3iom4mn4vq43l73fmqzsqbsnz47jd2thnvawjlceksww2zuu3yd33tnybjcjmjbtbmyfyxa2r4nhpure/wp_analysis_return_on_investment.pdf >.

Freedman, JB 2005,Information Security: Is Silence Golden?,Boston University School of Management,viewed 15th May 2011,<http://people.bu.edu/jfreedma/Information%20Security%20Activism%20final.doc>.

Friedman,G, & Sage, AP 2003, Case studies of systems engineering and management in systems auqisition,viewed on 18th September 2011,<http://sse.stevens .edu/fileadmin /sse/academics/resources/Developing_an_SE_Case_Study.pdf >.

Gordon, LA & Loeb, MP 2002a, The Economics of Information Security Investment, ACM Transactions in Information & Systems Security, pp 438-457.

Gordon, LA, & Loeb, MP 2002b,*Return on Information Security Investments: Myth vs. Reality*, pp 26-31.

Hancock, B 1998, An Introduction to Qualitative Research, viewed 8th July 2011,<http://faculty.uccb.ns.ca/ pmacintyre/course_pages/MBA603/MBA603_files /IntroQualitativeResearch.pdf >.

Hancock, B, Ockleford, E & Windridge, K 2007, An Introduction to Qualitative Research by Hancock,viewed 10th July 2011,<http://www.rds-eastmidlands.nihr. ac.uk/resources/doc_download/4-introduction-to-qualitative -research.html>.

Hash, J, Bartol, N, Rollins, H, Robinson, W, Ables, J & Batdorff, S 2005,Integrating IT Security into the Capital Planning and Investment Control Process,viewed 10th August 2011,<http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf>.

Herath, HSB, Herath, TC 2008, Investments in information security: A real options perspective with Bayesian postaudit. Journal of Management Information Systems 25(3) pp337-375

Japan's e-Government initiatives, Ministry of Internal affairs and communication, viewed 10th January 2011,<http://www.e-gov.go.jp/doc/e-government.html>.

Jonas, S 2007,The Costs of Enterprise Information Security, viewed 14th May 2011,<https://eeweb01.ee.kth.se/upload/publications/reports/2007/XR-EE-ICS _2007_018.pdf>.

Kruger, HA, & Kearney WD 2006,*A prototype for accessing information security awareness*,viewed 25 November 2010,<http://www.puk.ac.za/opencms/export/PUK/html/fakulteite/natuur/comp/hakruger_research4.pdf>.

Marshall, C & Rossman, GB 2006, Designing Qualitative Research (4th edition), Thousand Oaks, CA: Sage Publications.

Mikko, TS 2001, Five Dimensions of Information Security Awareness, University of Oulu,viewed 2nd February 2011,<http://portal.acm.org/citation.cfm?id=503348>.

Mizzi, A 2005,Return on Information Security Investments, viewed 30th January 2011,<http://hosteddocs.ittoolbox.com/ AM031805.pdf >.

Mizzi, 2008, A. Return on Information Security Investment– The Viability of An Anti-Spam Solution in a Wireless Environment. International Journal of Network Security, 10(1), pp. 18 – 24.

Rosnequist, M 2007, Measuring the return on IT security investments,viewed 2nd February 2011,<http://www.intel.com/it/pdf/measuring-the-return-on-it-security-investments.pdf>.

Sheen , JN 2010,Fuzzy Economic Decision-models for Information Security Investment, Department of Electrical Engineering, Cheng-Shiu University,viewed 5th October 2010,<http://www.wseas.us/e-library/conferences/2010/Hangzhou/IMCAS/IMCAS-24.pdf>.

Shoban, R 2006,e-Sri Lanka: An Integrated Approach to e-Government Case Study, viewed 17th May 2011,<http://www.apdip.net/projects/e-government/capblg/casestudies/SriLanka-Rainford.pdf>.

Shuttleworth & Martyn, 2008, Qualitative Research Design,viewed 8th July 2011,<http://www.experiment-resources.com/ qualitative-research-design.html>.

Vicente, A 2006,Return on Security Investment, viewed 14th May 2011,<http://www.issa.org/Library/Journals/2006/December/Aceituno%20-%20Return%20on%20Security%20Investment.pdf >.

Wes, S, Jason, A & Bruce, S 2005,*Return On Security Investment (ROSI): A Practical Quantitative Model***,** SageSecure, LLC ,viewed 4th October 2010,< ttp://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf>.

Whitley, R , Crawford, M 2005, Qualitative research in Psychiagry,viewed 9th July 2011,<http://ww1.cpa-apc.org:8080/ Publications/Archives/CJP/2005/february/cjp-feb-05-V10-whitley-RP.pdf>.

Xin, L & Merrill, W 2004, *Assessment of Information Security spending and costs of failure***,** Mississippi State University,viewed 4th October 2010,<http://www.information-institute.org/security/3rdConf/Proceedings/96.pdf>.

Young, S 2007 ,Comparing Best Practice Cases in Creating an Environment Conducive to Development Benefits, Growth and Investment-developing a case study methodology viewed 7th July 2011,<http://vi.unctad.org/digital-library/?task=dl_doc&doc_name=qualitative-versus>.

APENDIX-I

Guide for the Unstructured Interview (Step 1)

Purpose:

The purpose of this questionnaire is to guide the unstructured interviews which will be conducted to gain a preliminary understanding of the information security awareness and investment level in the particular government organization.

These unstructured interviews will be done for the top management officers of the particular organization.

The Questionnaire:

This questionnaire will only be used to guide the unstructured interviews so that the interviewee will not move out of the area of this research.

The questionnaire for the step2 will be modified based on this unstructured interviews.

Q1-1. what is the importance of information security for your organization?

Q1-2. What are the information security initiatives that you have done during the past?

Q1-3. Are you satisfied with the information security awareness level of your employees?

Q1-4. How do you allocate budget for information security projects?

Q1-5. Are you satisfied with the current level of information security in your organization?

Q1-6. What are your future plans to improve the level of information security against the emerging threats?

Q1-7. What do you think about spending on information security for your organization?

Q1-8. What are the problems of investing for information security?

Q1-9. What are your suggestions to overcome the above problems?

APENDIX-II

Guide for the Semi-Structured Interview (Step 2)

Purpose:

The purpose of this questionnaire is to guide the semi-structured interviews which will be conducted to gain in depth understanding of the information security awareness and investment level in the particular government organization.

These unstructured interviews will be done for the second level of management officers who are directly involved in the information security related activities of the particular organization.

The Questionnaire:

This questionnaire will only be used to guide the semi-structured interviews so that the interviewee will not move out of the area of interest and more detailed understanding can be gained.

This questionnaire will be modified based on the answers received in the previously conducted interviews and the continuous literature review.

Interviews will be conducted until a saturation point is reached.

Inputs

1 .What are the information security initiatives that you have done during the past?

2 .Do you do continuous monitoring to identify information security needs of your organization?

3 .Do you have any plan of action and milestones for information security investments?

4 .Do you normally take specialist advice to identify information security requirement?

5 .What will be the contribution of a IS policy for the investment process?

6 .How often do you do external IS evaluations?

7 .Have you experienced with any mandate changes which may require information security investments? If so what are those?

8 . Do you consider evolving threats for your information systems continuously and take action?

9 .What else do you consider when deciding on IS investments?

10 .How do you prioritize the IS investment?

11 .Do you have a prioritization criteria for this purpose?

12 . Who will be the stakeholders to develop such criteria?

13 .What do you consider when developing a prioritization criteria for your organization?

14 .Have you ever done an information security risk assessment for your organization? If not what are the reasons?

15 .What positions are designated for IS Management?

16 . Who makes the final decision on the IS investment? What is the IS awareness level of such people?

17 . How do you take funding for IS investments?

18 . What is the process to allocate funds?

Control

19 .Do you check the performance of Information security systems periodically?

20 . Who involves with the performance checking of IS systems?

21 .What was your estimated list of security systems (equipment, applications, etc.)? Out of the estimated list of equipment, how many were approved and purchased?

22 .Do you document and analyze the cost benefits of each IS investment?

23 .Do you assess milestones completion at each phase of investment?

24 .Do you analyze achievement of goals for IS investments?

Evaluation

25 .How do you evaluate IS investment? Do you compare it with earlier projections such as cost,benefit, risk, return etc?

26 .How do you decide the continuity of IS investment? Do you normally do continuous adjustments?

27 .What is the importance of lessons learned for your future planning?

28 .Did you have any problems with justifying information security investments when auditing is done? If so what are your suggestions to overcome those problems?

IS awareness and responsibilities

29 .What is the importance of awareness on IS for different levels of staff in your organization?

30 .Are you satisfied with the information security awareness level of your subordinates?

31 .What steps were taken to educate the employees regarding IS sec.? What costs were involved with this?

32 .Do you think that it is important to have a IS policy for your organization?

33 .What are the reasons for not having a information security policy for your organization?

34 .What do you think about the responsibilities of different level of staff on information security investments?

35 . Do you have an incident reporting mechanism?

36 .Have you experienced any information security breaches during the past?

i If so what was the damage it created for your organization?

ii Were you able to manage such incidents by yourself? If not how did you manage them?

iii How do you allocate funds for sudden incidents?

37 .What maintenance agreements were signed with security providers?

38 .How effective are they?

APPENDIX III

Collected Data

1.) Data Collected from Department A

Questions and answers collected at the interview related to each area of the conceptual frame work is listed below.

Inputs

1 .What are the information security initiatives that you have done during the past?

Have invested for anti virus solutions to protect the DMT computer network. There is a data center for driving license project. Have invested for physical security implementations such as biometric door locks, virus guards, firewalls etc in this project.

When connecting to the wide area network VPN s are used with firewalls.

2 .What was the information security investment for those projects?

Information security investments are not calculated separately. The security requirements are incorporated in the projects and funds are taken from the IT budget if the system is within the premises of DMT such as registration system which is not connected to the WAN.

At the moment information security budget allocations are considered as one component of the IT budget.

3 .Do you do continuous monitoring to identify information security needs of your organization?

Until today there is no issues with the systems except one or two incidents. When there was a virus issue, precautions were taken to avoid such incidents in future.

4 .When you were taking such precautions did your information security policy describe those?

There are documents prepared to take necessary precautions to avoid information security breaches. But they were given as internal circulars/orders and still there is no comprehensive IS policy.

But expecting to develop a comprehensive IS policy in future.

5 .Do you have any plan of action and milestones for information security investments?

At the moment the two systems which are running in the DMT are very stable. IS security has been provided to the fullest possible.

In future when e-motoring project is running it is expected to open it to the Internet and hence it may need to consider the information security than today.
It is already planned, but for the moment there is no such requirement to prepare a action plan and milestones.

The requirements may be identified when e-motoring project is running.

6 .Do you normally take specialist advice to identify information security requirement?

Most of the time advices are taken from ICT agency of Sri Lanka. When projects are outsourced advices are taken from those vendors.

For some projects such as driving license there are agreements with third party organizations to take the total responsibility of the projects including information security requirements. There is a BOT (build, operate,transfer) agreement with them and according to that they have to take necessary steps to preserve information security. So DMT doesn't have to worry about that since there is a risk transfer.

7 .What will be the expected contribution of a IS policy for the investment process?

Investments that are necessary for providing data access with different privileges should be identified. Proper password policy with enforcement because at the moment still there are unlocked computers with unatteneded.

Penalties should be defined for irresponsible behaviors.

8 .How often do you do external IS evaluations?

There is a requirement to do that. Some security assessments were done with the help of Sri Lanka CERT.

For the driving license project also it should be done because it is totally depend on electronic document management process. It should also be done with the help of a third party which is still not selected.

9 .Have you experienced with any mandate changes which may require information security investments? If so what are those?

Definitely we have to invest on such requirements. There was a government mandate to enable credit card transactions for the automated systems. But still our driving license systems does not have such facility because we have though about the possible security issues which may arise upon introducing this. There will a huge investment when implementing this with proper security measures.

10 .Do you have a prioritization criteria for this purpose?

At the moment we don't have such criteria. Both systems that we have are important for the department. So there is no requirement to prioritize. But if we have such criteria sometimes a low priority will be given for the web site because it is only an information site which don't have any capability to do transactions.

11 . Who will be the stakeholders to develop such criteria?

CIO, Head of IT, Commissioner general, member of ICTA

According to e-Gove policy we have to consult ICTA for any projects which may need an investment over 2 million. At the moment also we request the involvement of ICTA for any projects,as a precaution.

So when developing such criteria we have to take a member from ICTA as well.

12 .What do you consider when developing a prioritization criteria for your organization?

We have to consider the impact level.

13 .Have you ever done an information security risk assessment for your organization? If not what are the reasons?

We have done a system audit for the vehicle registration system and identified the weak point that should be improved specially for Information security.

The findings and recommendations are documented well and it will be implemented as a future project.

14 .Are there any barriers to implement those recommendations?

There is a vendor locking situation with some systems and vendors. They are the only people who know about the system and sometimes they reject to do changes which are required to preserve information security or else they charge too much for such changes. If the the cost is not justifiable we do not implement those changes even though it is recommended a security requirement.

Some agreements with the vendors doesn't support for changes to the systems because they are too old, and at the moment of preparing those agreements information security requirements has not been considered seriously.

15 .What positions are designated for IS Management?

There is no such designated person, but CIO is looking after those. CIO can take inputs from any resource and then evaluate the requirement. Advices of ICTA is taken for the process.

16 . Who makes the final decision on the IS investment? What is the IS awareness level of such people?

Commissioner General.

He has a good understanding about information security since he was a past officer in this department as well. There is no barrier from him to implement information security requirements when it is justifiable.

17 . How do you take funding for IS investments?

We don't ask funding for information security separately. But for the projects which are planned to be implemented in the next year, IS is considered as a component. Funding is requested for the whole project.

In the project documents there is a defined requirement for information security. But required investment to implement those requirements are not calculated separately. However final project output should comply with the predefined security requirements in that document. So, IS investment is automatically included in the project cost.

18 . What is the process to allocate funds?

First we have to identify the requirement and then prepared the proposal. Then is included into the budget. However there is no proposals for information security investments since this always goes as a component of a particular project.

Control

1 .Do you check the performance of IS systems continuously? Who involve in this process?

For some of our projects we do continuous performance checks with the support of vendors and the department staff.

For the driving license project which was done recently it happens.

But for the vehicle registration system which is older than 10 years, those checks are not done periodically. There are security issues with this systems but fixing those finding is not done properly. E-motoring will be the ultimate solution for this problem.

2 .What was your estimated list of security systems (equipment, applications, etc.)?

This is estimated per project. But not done in annual basis. Sometimes a list of equipments is prepared depending on the identified requirements.

3 .Out of the estimated list of equipment, how many were approved and purchased?

I don't agree with the IT budget concept which is mentioned in the e-Gov policy. An organization should have a business strategy and ICT enable should be a component in that. If we take our department it is difficult to prepare a business budget and IT budget separately because we have an ICT enabled business.

So there is not point of preparing a separate list of required equipments and take approvals. Everything is included in the projects.

4 .Do you document and analyze the progress , cost-benefit of IS investments?

We have outsourced most of our information systems. So the vendors give us updates on the progress of our investments. But it is not done separately for IS investments. Once the contract is awarded to a particular vendor we continue with the project throughout the contract period without considering cost-benefit.

5 .Do you assess milestones completion at each phase of investment?

We don't do any assessment for the completion of phases of our projects. But it is done at the end of the project.

6 .Do you analyze achievement of goals for IS investments?

We analyze the achievement of goals for the total project. Information security is one of the component in it. But there is no separate analysis for achievement of goals for IS since we don't invest for it directly.

Evaluation

1 . How do you evaluate IS investment? Do you compare it with earlier projections such as cost,benefit, risk, return etc?

Cost-benefit analysis is done for the whole project. Since information security investments are a part of that, it is also covered automatically.
But information security investments are never evaluated separately.

2 . How do you decide the continuity of IS investment? Do you normally do continuous adjustments?

Most of the projects are tendered out to third party organizations. So they have to take care of those projects during the whole period of the tender. After the tender period , the department take over the project decides whether to continue with the project by ourselves or again call for tenders, at least for maintenance.

3 . What is the importance of lessons learned for your future planning?

It definitely helped us specially when drafting the agreements with outside organizations. For example it is decided how to overcome information security breaches, what are the IS requirements etc are considered very seriously with the help of lessoned learned with previous projects.

4 . Did you have any problems with justifying information security investments when auditing is done? If so what are your suggestions to overcome those problems?

The internal auditors check only whether the procurement guidelines are followed or not. They don't audit the functionality of the security systems purchased. I think that even the general auditors are not capable of doing that.

IS awareness and responsibilities

1. What is the importance of awareness on IS for different levels of staff in your organization?

There are different level of knowledge with various levels of staff. But the problem is sometimes the people who knows about information security is behaving without caring on that. For example they share passwords with others,some executive officers has given access to their computer to some trusted subordinates etc. So it is very important to have proper awareness on IS.

2. What steps were taken to educate the employees regarding IS sec.? What costs were involved with this?

There are internal circulars to aware the staff on information security.

3. What are the reasons for not having a information security policy for your organization?

There are some guidelines that can be considered as a part of the IS policy. Those are issued as internal circulars and are followed by the staff. But there is no comprehensively documented policy for the department.

4. Do you think that it covers all the IS domains?

I can't think so. What we have is a reactive guidelines. It is not a proactive policy which is more comprehensive.

5. What do you think about the responsibilities of different level of staff on information security investments?

There are several groups with different privileges. Their responsibilities are defined so that they have to act accordingly.

6. Have you experienced any information security breaches during the past?

Yes. There was a problem with computer viruses and some internal incidents as well. In the vehicle registration system also there were reported incidents which were done by internal people and exposed in audit quaries.

7. If so what was the damage it created for your organization?

System didn't function for few days due to virus problem.

8. Were you able to manage such incidents by yourself? If not how did you manage them?

With the help of third party organization.

9. How do you allocate funds for sudden incidents?

There is a component is the annual budget called “computer services and maintenance”. It is possible to extract funds under this component because it is a main component in the budget.

10. What maintenance agreements were signed with security providers?

For the vehicle registration system there is no such agreements. We handle it internally.

For the driving license project the third party organization is given the total responsibilities to handle the system with proper security. This company has agreements with other security vendors to provide security for the system. We don't monitor those. But we have given our security requirements and guidelines for them to comply.

11. How effective are they?

At the moment there is no issues with their services.

2.) Data Collected from Department B

Questions and answers collected at the interview related to each area of the conceptual frame work is listed below.

Inputs

1. What are the information security initiatives that you have done during the past?

We haven't done significant investments for information security in our e-pensions project since it is still evolving and only the pilot operation is running. But we have started it in several ways such as providing access controls to the system with various privilege levels, introducing password policy for the users etc.

The vendor has provided necessary security controls according to the initial agreement. Most of the physical security controls are done.

At the moment the server room and IT room is adequately secured with physical security controls. But we are expecting to implement biometric entry controls, fire alarms etc which we couldn't continue as we could not reserve funds for that in this year. In the next year we are expecting to reserve funds for this purpose.

We could implement separate electricity supply with security controls for which we had to spent lot of funds.

2. Do you do continuous monitoring to identify information security needs of your organization?

This is done only within the IT section. We have two main responsibilities. They are Mon-functional and supportive-functional. Those are highlighted in each officer's duty list as follows.

Conducting the duties according to the e-government policy

Conducting the duties according to the department's information security policy

New investment requirements are identified with this process from the inputs of the staff.

3. Do you have any plan of action and milestones for information security investments?

We don't have any plan of action and milestones in the existing system. But in the e-pensions system it is defined up to some extent. It has 6 processes each having own stretch goals.

At the moment the e-pensions system is the infant stage. Staff is in the process of learning the system and hence it is not possible to achieve milestones for information security investments.

4. Do you normally take specialist advice to identify information security requirement?

We take advises from ICT agency of Sri Lanka as the primary source Then we take advises from our service providers/vendors who are involved with the ongoing projects.

5. What will be the contribution of a IS policy for the investment process?

It is not happening at the moment. The main problem I have is how to convince the staff the necessity of information security with the new system. Currently only the IT staff has understood that. Rest of the staff does not care about it.

At the moment we have developed the IS policy for the department. But it is necessary to change the thinking pattern of the staff to absorb it properly. Specially the requirement of such policy should be understood by the top management. It is not enough to aware them by the internal officers such as CIO but it should be done by external parties as well. Then only they will accept it.

6. How often do you do external IS evaluations?

It is not happening at the moment.

7. Have you experienced with any mandate changes which may require information security investments? If so what are those?

We don't have any such past experience. For example according to the government data privacy policy the pensioner's data should be protected by the department. It is considered in the e-pensions implementations. But the top management has different views on that and as a result it is very difficult to do it practically.

We have past incidents due to this kind of implementation issues.

8. How do you prioritize the IS investment?

We consider the currently most wanted requirement and invest on that.

9. Do you have a prioritization criteria for this purpose?

There is no such criteria. We have to take decisions with the level of our understanding as we don't have any consultants to get advices. If there is someone to advise us on prioritizing the investments it will help us because we sometimes work on lessons learned.

10. Who will be the stakeholders to develop such criteria?

There should be several parties involved for this purpose such as

Staff of the department

External organizations such as ICTA, CERT

This can't be done alone since we don't have sufficient knowledge in this domain even though we have knowledge in our subjects.

11. What do you consider when developing a prioritization criteria for your organization?

No. clear idea for developing such criteria for IS investments.

12. Have you ever done an information security risk assessment for your organization? If not what are the reasons?

No. we haven't done any.

The reasons are still we are in the pilot project for e-pensions and identifying problems of that. The requirement of such risk assessment will be arisen depending on such findings in future.

13. What positions are designated for IS Management?

CIO is designated for the IS management process, according to the IS policy of the department.

But I think that there should be a group of people for the implementation of such investment projects.

The group should consists of

Ground level staff who operate on the IS project

Organizational level decision makers

14. Who makes the final decision on the IS investment? What is the IS awareness level of such people?

Final decision is taken by the director general of pensions. The IT department do the justification for that.

The awareness level of IS of the DG is not so sufficient. It has made lot of problems when implementing IS systems.

15. How do you take funding for IS investments?

We don't have a allocated budget for information security and even for IT. Most of our information systems are funded by ICTA.

Control

1. Problems with investments for information security

The main problem of implementing the server room is lack of funds.

2. Do you check the performance of IS systems continuously? Who involve in this process?

It is not happening at the moment

3. Do you prepare an estimated list of security systems (equipment, applications, etc.)?

We started preparing a list of required systems from this year. But we don't prepare it separately for security systems.

4. Out of the estimated list of equipment, how many were approved and purchased?

Still we are preparing this.

5. Do you document and analyze the progress , cost-benefit of IS investments?

We haven't done that. But it should be done.

6. Do you access milestones completion at each phase of investment?

We are still at a basic level for information security implementations. At the moment no such milestones are defined.

Most of our information systems are done as projects under ICTA. So in those projects we have some defined milestones.

7. Do you analyze achievement of goals for IS investments?

It is not done separately for IS investments but for the whole project.

Evaluation

1. How do you evaluate IS investment? Do you compare it with earlier projections such as cost,benefit, risk, return etc?

Since most of our information system projects are done by ICTA, they are doing that.

2. How do you decide the continuity of IS investment? Do you normally do continuous adjustments?

IT section and the CIO can do recommendation on the continuity and necessary adjustments for the ongoing projects. But the final decision is taken by the Director General.

3. What is the importance of lessons learned for your future planning?

We have learn lot of things by experience. For example we build our network infrastructure before the e-pensions project without thinking about the compatibility of both systems. From that we learn lot of things and did modifications needed with that experience.

4. Did you have any problems with justifying information security investments when auditing is done? If so what are your suggestions to overcome those problems?

It is very difficult to justify it to our director general since he is not so keen on information security controls.

Hence we always justify the security requirements with the support of ICTA.

IS awareness and responsibilities

1. What is the importance of awareness on IS for different levels of staff in your organization?

In our department it is very difficult to implement security controls because the commissioner general is not so supportive for some of the necessary controls such as access to control to computers, use of licensed copies of software etc. It is very difficult to convince him about the necessity of such controls because of lack of knowledge in information security.

It is important to have awareness on information security and IT for each and every level of staff. For example a peon will be able to identify and shut down the computers which are forgotten to switch off by mistake if they have the knowledge to do that.

2. Are you satisfied with the information security awareness level of your subordinates?

The main problem we have is information security awareness and the negligence of the employees. For example our system get locked after 3 login attempts. Then the system administrator has to reset the password for that user. In each day the administrator is requested to reset at least 10 passwords since users forget their password and system get locked.

3. What steps were taken to educate the employees regarding IS sec.? What costs were involved with this?

The problem of conducting awareness programs for our staff is that we have to conduct them with the implementation of the e-pensions project. Because it is useless to conduct such programs without a practical usage of the system. For example if we aware them on password policy without the usage of the system they will forget it at the time of usage. The training programs should be aligned with the implementation and the usage of the system.

Just providing awareness is not sufficient. Some controls should be enforced and monitored for illegal activities.

4. Do you think that it is important to have a IS policy for your organization?

Yes. We have an information security policy. But still it is not fully implemented in the organization. With the introduction of e-pensions project the policy will be applied.

5. What do you think about the responsibilities of different level of staff on information security investments?

Every body has a responsibility for information security requirement of the organization.

6. Have you experienced any information security breaches during the past?

There were some suspicious activities in our internal network. But couldn't verify whether those are compromises for our information systems.

7. Were you able to manage such incidents by yourself? If not how did you manage them?

We try to handle it by ourselves. If not we contact ICTA and Sri Lanka CERT.

8. How do you allocate funds for sudden incidents?

We can take funding internally for such incidents from the allocations under “office equipment” in the annual budget.

9. What maintenance agreements were signed with security providers?

For some of the projects there are maintenance and license agreements with service providers. But the cost is bared by the project.

But in future those agreements will come under our department and then we may have to allocate funds for that.

10. Do you have an incident reporting mechanism?

It should be informed to the IT section of the department. It can be any incident and not limited to information security incidents.
Then we take necessary action to overcome the situation.

3.) Data Collected from Department C

Questions and answers collected at the interview related to each area of the conceptual frame work is listed below.

Inputs

1. What are the information security initiatives that you have done during the past?

We haven't done it systematically. Generally we have systems implemented in a ad-hoc manner. So our first intention is to develop the system and after that we realize the security issues.

We have funding problems and issues with justifying such investments to the top management.

At the moment what we do as information security is like installing virus guards, deploying firewalls etc. But with the introduction of new IT systems we have noticed that there are increasing number of incidents because of not having proper security controls.

As a result of that we have to consider IS in parallel to implementing the new systems.

2. Do you do continuous monitoring to identify information security needs of your organization?

We don't have sufficient staff capable of monitoring such security needs. If we take any government organization there is a limited number of people who are aware of those things. Even if they recruit as IT officers they have to do some other works as well. Security monitoring is a different responsibility and we don't have IT carder to take that challenge.

So I don't think that it is happening in any of the government organizations as it is happening in private sector.

Organizations like ICTA should make the management aware about the need of doing that.

3. Do you have any plan of action and milestones for information security investments?

For the IT investments we have a plan. For the security investments we don't have such. But IS investment are incorporated within the IT investment plan.

4. Do you normally take specialist advice to identify information security requirement?

It is very difficult to justify the need of such consultant to the top management. Also it will be very expensive to have such consultants.

For example most of the time top management think that only installing a virus guard will provide the information security to the organization. Then don't know that there are IS risks beyond that

5. How do you overcome the problems of not having a information security policy?

We issue internal circulars to introduce new security controls to the users. But this is limited to some processes like passport printing. But for the systems in the Airport we don't have such policy or circulars issued.

6. What will be the contribution of a IS policy for the investment process?

If we adapt a proper information security policy it will be a advantage to do the IS investments.

7. How often do you do external IS evaluations?

It is happening very rarely in the government sector. As I know we are having lot of information systems, but not doing such evaluations which need investments. But sometimes we use our personal contacts to do that without any cost.

8. Have you experienced with any mandate changes which may require information security investments? If so what are those?

We may have to do necessary investments with the introduction of such changes.

9. How do you prioritize the IS investment?

We normally don't have prioritization issues because we are a large government organization having a IT department and resources to do the investments. But a small government organization may need some kind of prioritization mechanism.

10. If you are going to develop such criteria who will be the stakeholders?

The people with proper knowledge in each area should be involved.

11. What do you consider when developing a prioritization criteria for your organization?

We have to fulfill the need of people first.

12. Have you ever done an information security risk assessment for your organization? If not what are the reasons?

No. We don't do such risk assessments for IS. The reason is we don't have a proper knowledge in IS and time. We realize the need of such assessment only after a incident. But there may be incidents which are not known to us and we haven't take any actions to mitigate.

13. What positions are designated for IS Management?

The expectation from a CIO is not properly defined by the ICTA. As a department we have a IT staff who are in alert to some extent for IS issues. There is no designated officer for IS management.

14. Who makes the final decision on the IS investment? What is the IS awareness level of such people?

First we have to take the approval for the concept by giving proper justifications. Then the investment can be approved by the head of the department.

15. How do you take funding for IS investments?

We take funding through annual budget and can be under “office and equipments” or “communications” titles. For the IT or information security we don't have a separate section/title in the budget.

16. What is the process to allocate funds?

We have discussions for the next year's budget. In those discussions we decide on what we are going to purchase in the next year.

Control

1. Do you check the performance of IS systems continuously? Who involve in this process?

We don't have such sophisticated information systems to monitor. But it is happening with the support of IT staff.

2. Do you prepare an estimated list of security systems?

Yes. We prepare a list for all the required items.

3. Out of the estimated list of equipment, how many were approved and purchased?

We purchase the equipments depending on the availability of funds. We don't have issues for taking approvals and funds because we don't ask for extra equipments. But we have issues when we move to the procurement process.

4. heard that in some organizations they are having problems with the vendors when purchasing equipments. Is it true for you?

Yes. Sometimes they don' t deliver the items which they bid.

5. Do you access milestones completion at each phase of investment?

Normally when it is for IT project, there is a project plan for security implementations as well.

Other than that if we purchase a equipment like firewall we put dead lines for delivery, installation etc in the tender conditions.

6. Do you document and analyze the progress, cost-benefit of IS investments?

No. we don't do such documentation for such investments.

7. Do you assess milestones completion at each phase of investment?

No. It is not happening at the moment.

8. Do you analyze achievement of goals for IS investments?

For some investments like purchasing firewalls, virus guards etc. we analyze whether it fulfills our need. Other than that we don't invest directly for IS.

Evaluation

1. How do you evaluate IS investment? Do you compare it with earlier projections such as cost,benefit, risk, return etc?

There is no such system implemented for government organizations.

2. How do you decide the continuity of IS investment? Do you normally do continuous adjustments?

We normally do it with the renewal of contracts or maintenance agreements. But at the moment of renewal we don't do any evaluations to take that decision, simply because it is easier to move forward with the same vendor rather than selecting a new vendor for the same task.

3. What is the importance of lessons learned for your future planning?

We have realized most of the security issues only after some incidents. They are good lessons for us. Also we take advices from our vendors to implement/ enhance security controls.

4. Did you have any problems with justifying information security investments when auditing is done? If so what are your suggestions to overcome those problems?

Most of the time we take strategic approach to convince the top management about he need of such investments. Sometimes we take the help of ICTA to move forward with the justifications.

IS awareness and responsibilities

1. What is the importance of awareness on IS for different levels of staff in your organization?

It is very important for each and every level. But not sufficient at the moment.

2. Are you satisfied with the information security awareness level of your subordinates?

Most of the staff in the department has come for 5 years. As a result of that there are security awareness issues with them.

3. What steps were taken to educate the employees regarding IS sec.? What costs were involved with this?

Actually we should educate the staff on information security issues properly. At the moment it is not happening.

4. What is the problem with investing on those?

We have works with more priority and hence it is difficult to take staff for such trainings. At the moment IS has leased priority since top management is not so IT savvy.

Since IS trainings are bit expensive than normal IT trainings we have the issue for convincing the management for the requirement.

5. Do you think that it is important to have a IS policy for your organization?

It is very important to have such policy. It is a need of any government organization. Then we can easily take decisions to do required investments with the help of IS policy as we have to obey with that policy.

6. What are the reasons for not having a information security policy for your organization?

Still there is no feeling to have a IS policy because the awareness on IS is very poor. Also we didn't receive any guidance from relevant parties to have such a policy.

The continuity of awareness programs are very important with proper examples.

7. What do you think about the responsibilities of different level of staff on information security investments?

For the usage of computers there is no such considerable levels in the government sector organizations. For example if we give Internet access to users it is same for any staff level. But as a control we haven't give Internet access for all the staff.

8. What is the incident reporting mechanism in your organization?

IT unit take the such complains from the users and take necessary actions by connecting with relevant vendors and ICTA.

9. Have you experienced any information security breaches during the past?

Yes. we had such issues like hacking our web site etc.

10. Were you able to manage such incidents by yourself? If not how did you manage them?

We take support from the companies who did the implementations of such systems. Also we have taken support from ICTA and SLCERT. Most of the time we use our private contacts to do this.

11. How do you allocate funds for sudden incidents?

Government organization doesn't have a proper procedure to face this kind of situations. Most of the time we try to seek help from a external organization for which we don't have to spent. That is because it is very difficult to do the job if there is a cost involved.

12. What maintenance agreements were signed with security providers?

Yes. We have.

13. How effective are they?

Most of the time vendors are not capable of handling issues that comes with IS systems. That is because their IT teams are not consistent and changing very frequently. Sometimes we do considerable amount to purchase equipments like firewalls but vendors don't configure them properly as their staff of not capable of doing that.

4.) Data Collected from Department D

Questions and answers collected at the interview related to each area of the conceptual frame work is listed below.

Inputs

1. What are the information security initiatives that you have done during the past?

We are using security dongles for the passport printing purpose. Head office and regional offices are connected through VPNs with encrypted data transfer.

Surveillance cameras are installed for the areas which should be highly secured. Internet connections to the local network is protected using firewalls.

As the current passport handling system is not connected to the outside it is not protected using firewalls.

2. Do you do continuous monitoring to identify information security needs of your organization?

Yes. It is happening. For example if we identify a security issue with a dongle actions are taken immediately.

All the access control systems and monitored and take necessary steps to update them. CCTV systems are used to monitor physical security issues.

3. Do you have any plan of action and milestones for information security investments?

Yes. We have an action plan for some investments. For example we are going to purchase new CCTV cameras from the next budget since we don't have sufficient number of cameras installed.

4. Do you normally take specialist advice to identify information security requirement?

Some projects are done with the advices of the external organizations. For example CCTV system installed with the help of Australian IOM.

For the passport processing system we internally identified the requirement and did the selection.

For some projects we take the advices of external consultants.

5. How do you overcome the problems of not having a information security policy?

We issue internal circulars to introduce new security controls to the users. But this is limited to some processes like passport printing. But for the systems in the Airport we don't have such policy or circulars issued.

6. How often do you do external IS evaluations?

If we are going to acquire a new system we do IS evaluations to identify the suitability of such systems.

7. Have you experienced with any mandate changes which may require information security investments? If so what are those?

We are having discussions with ICTA and some other external government organizations to implement new projects to access our data. So in future we may have to invest on those.

8. How do you prioritize the IS investment?

We normally invest on a total solution in which IS is included. Those solutions are consulted by external consultants. As a result of that we don't have a prioritization problem.

9. Do you have a prioritization criteria for this purpose?

NO. we don't have a prioritization criteria.

10. In future will you feel the need of such criteria?

Yes. Definitely we may need it.

11. Who will be the stakeholders to develop such criteria ?

People with the knowledge in this domain should involve with this. Since we are closely working with ICTA we should have their contribution as well.

12. What do you consider when developing a prioritization criteria for your organization?

Cost-benefit analysis should be done.

13. Have you ever done an information security risk assessment for your organization? If not what are the reasons?

We did one such assessment when we are introducing the dongles for the printing service and when connecting the system to regional offices.

14. What positions are designated for IS Management?

There is a deputy controller for the IT and information security comes under him.

15. Who makes the final decision on the IS investment? What is the IS awareness level of such people?

Technical evaluation committee takes the decision. The chair person of the TEC can be the Controller General or the consultant of that project.

16. How do you take funding for IS investments?

We allocate funds for the total solution/project. IS is a one component under that project. So there is no separate funding for IS.

17. What is the process to allocate funds?

If we have identified new security requirements we include them to the annual budget and take the funds.

But most of the time it is done for the whole project.

Control

1. Do you check the performance of IS systems continuously? Who involve in this process?

Yes. We do. The IT department staff involves with this. We do it on daily basis. All the airport systems are monitored for the performance from here.
2. Do you prepare an estimated list of security systems?

If we have identified new requirements we include them to the estimated list.

3. Out of the estimated list of equipment, how many were approved and purchased?

All the staff from the deputy controller are involved in this process and hence we don't have issues with taking approvals.

4. Do you document and analyze the progress, cost-benefit of IS investments?

We do it for some projects. But it is not done separately for IS investments.

5. Do you assess milestones completion at each phase of investment?

Normally it is done by the vendor.

6. Do you analyze achievement of goals for IS investments?

Information security is only one of the requirement of our information system projects. After the completion of the project we analyze whether the IS requirements are addressed properly in the project.

Evaluation

1. How do you evaluate IS investment? Do you compare it with earlier projections such as cost,benefit, risk, return etc?

NO. we don't do such evaluations. We normally continue with the projects which are planned for years.

2. How do you decide the continuity of IS investment? Do you normally do continuous adjustments?

IT department take the inputs from the system users before deciding the continuity of the projects.

3. What is the importance of lessons learned for your future planning?

We have started security implementations about 3 years ago. We have moved forward with the lessons learned during the past.

IS awareness and responsibilities

1. What is the importance of awareness on IS for different levels of staff in your organization?

We have segregated the duties. The information security needs are different at each level.

2. Are you satisfied with the information security awareness level of your subordinates?

Most of the staff in the department has come for 5 years. As a result of that there are security awareness issues with them.

3. What steps were taken to educate the employees regarding IS sec.? What costs were involved with this?

For the new staff we do awareness training. But for the existing staff it is not happening.

4. Do you think that it is important to have a IS policy for your organization?

It is very important to have such policy. Then we can improve our service and continue with it.

5. What are the reasons for not having a information security policy for your organization?

There is no special reason for that.

6. What do you think about the responsibilities of different level of staff on information security investments?

Various level of staff has different responsibilities. But all of them are protecting the information owned by the organization.

7. What is the incident reporting mechanism in your organization?

IT team take the such complains from the users and take necessary actions.

8. Have you experienced any information security breaches during the past?

No. we didn't have such issues.

9. How do you allocate funds for sudden incidents?

If we have remainig funds we can do it with that. Otherwise we have to wait until next budget cycle.

10. when you introduce new systems, is there a possibility for such breaches?

We are expecting to implement a e-motoring unit to minimize such IS breaches.

11. What maintenance agreements were signed with security providers?

Yes. We have.

12. How effective are they?

We pay them quarterly and monitor their service.

5.) Data Collected from Department E

Questions and answers collected at the interview related to each area of the conceptual frame work is listed below.

Inputs

1.What are the information security initiatives that you have done during the past?

All of our internal systems are enabled with proper authentications systems. Nobody can enter the systems without authentication. Also each user is provided with different levels of privileges which is required for their relevant job. They can' t go beyond that without requesting the permission to the next level of access.

2.when I was discussing with the commissioner general it is found that most of your systems are built in-house. When developing such systems do you consider about the security features as well?

When developing the systems in house we consider the security features as the first requirement.

3.Do you do continuous monitoring to identify information security needs of your organization?

Yes. We do continuous monitoring our systems. But we don't have an information security policy which is developed or implemented to support this purpose.

We have issued internal circulars to cover the security needs of our systems as a result of not having a security policy.

4.Do you have any plan of action and milestones for information security investments?

We have identified the IS need of our organization and now we have to develop such plans and milestones.

5.Do you normally take specialist advice to identify information security requirement?

Yes. We take advices from external consultants. Most of the time they are from University of Moratuwa.

6.What will be the contribution of a IS policy for the investment process?

If we have a proper IS policy then it will be easy for us to take investment decisions and approvals.

7.What are the current issues for the IS investments?

We don't have funds for investments. The amount allocated in the last budget is over and have to wait until the next budget.

8.How often do you do external IS evaluations?

At the moment we haven't expose our systems to the out side. So we don't feel that we need such external evaluations.

But exposure is done up to some extent through LGN system. We don't do such evaluations for that system since they are taken care of LGN staff.

When e-nic project is implemented the external evaluations will be a must.

9.Have you experienced with any mandate changes which may require information security investments? If so what are those?

Depending on those changes we have to act and comply with new IS investments.

10.How do you prioritize the IS investment?

Decision is taken by considering the demand. For example if we need to buy 10 computers and a firewall the priority will go for computers because we have to provide our service to the public first.

This prioritization issues normally arise at the end of the year. Otherwise we don't have such issue and can procure any item that is required and budgeted without any problem.

11.Do you have a prioritization criteria for this purpose?

No clear criteria. It depends on the demand of such requirement.

12.What do you consider when developing a prioritization criteria for your organization?

Demand is the main consideration.

13.Have you ever done an information security risk assessment for your organization? If not what are the reasons?

NO. we haven't done any.

14.What positions are designated for IS sec. Management?

CIO is designated and there is a team under him for this.

15. Who makes the final decision on the IS investment? What is the IS awareness level of such people?

The Commissioner General of RPD takes the final decision as the chairman of the tender board. It is the general procedure for government procurements.

16. How do you take funding for IS investments?

There is no budget for information security or information technology. We take funds from the annual allocations under the heading “machines and equipments” of the annual budget for any IT investments.

17. What is the process to allocate funds?

We estimate the budget for the next year before the end of this year. Then it will be approved for the next year. Most of the time we don't get approvals for each and every item in the budget. For example if asked for hundred thousand rupees only eighty thousand will be approved.

Control

1. Do you check the performance of IS systems continuously? Who involve in this process?

At the moment we don't do such performance checks because we don't have sophisticated security systems to do so. But there is a plan to deploy a firewall for the internal network which may need this kind of performance checks.

2. What was your estimated list of security systems (equipment, applications, etc.)?

We prepare a list of all the items that is going to be procured in the next year.

3. Out of the estimated list of equipment, how many were approved and purchased?

Normally very few items are approved. For example in the last year we have requested few millions and got the approval for nearly one million.

But in the year 2009 we got the approval for all the requested items for the procurement. But the selected vendor failed to deliver the items. As a result of that there were some unused allocations in that year.

There are problems with selecting the proper vendors for security appliances.

4. Do you document and analyze the progress , cost-benefit of IS investments?

At the moment we don't do so.

5. Do you assess milestones completion at each phase of investment?

We have divided our internal developments in to several phases and do assessments for the completion of each phase with the support of users.

But there is no milestones defined for information security separately.

6. Do you analyze achievement of goals for IS investments?

We give priority for IS needs of our information systems. After the development we test the systems for security issues and take necessary actions.

Evaluation

1. How do you evaluate IS investment? Do you compare it with earlier projections such as cost,benefit, risk, return etc?

NO. we don't do.

2. How do you decide the continuity of IS investment? Do you normally do continuous adjustments?

We decide it with the help of technical evaluation committee.

3. What is the importance of lessons learned for your future planning?

We have learn a lot with the past experience and don't allow to happen the same fault twice. Some examples are power installations and Air conditioner selections from which we have learn lot of things. The situation is same for selecting proper servers, virus guards, power generators etc.

4. Did you have any problems with justifying information security investments when auditing is done? If so what are your suggestions to overcome those problems?

We haven't done considerable investments for information security. So I can't comment on the justification issues. But I think that there won't be any problems in future for justification process.

5. Is there a annual audit for the department?

Yes. We do a general audit. But it does not cover information security. They only check the availability of the procured appliances.

IS awareness and responsibilities

1. Are you satisfied with the information security awareness level of your subordinates?

NO. It is very poor.

2. what about the IS awareness of management staff?

Some people have general awareness on IS.

3. What steps were taken to educate the employees regarding IS? What costs were involved with this?

When introducing the systems discussions are done with the staff about the security issues of that particular system. Precautions and countermeasures are taken whenever necessary.

When new security control is introduced all the staff members who use the system is informed about that.

When users are trained to use the system the security is incorporated with that. But it is not taught as a separate subject.

4. Do you think that it is important to have a IS policy for your organization?

Yes. Definitely we should have it.

5. What are the reasons for not having a information security policy for your organization?

There are peak times for issuing identity cards. As a result of that we don't have time to spend on developing IS policy.

6. What do you think about the responsibilities of different level of staff on information security investments?

Everybody has responsibilities for information security in the department. For example if we take a driver who is transporting documents here to there he has a responsibility to protect them. At the delivery to the next officer everything is checked for integrity. There are properly defined controls to do that.

7. Have you experienced any information security breaches during the past?

The only problems we had during the past with our information systems is virus infections through USB drives.

But in the manual process of issuing identity card have various issues like producing fake documents. It is very difficult to trace them when it is done in planned and organized manner. There is no proper verification process for physical documents.

8. Were you able to manage such incidents by yourself? If not how did you manage them?

During the past we could manage them by ourselves.

9. How do you allocate funds for sudden incidents?

We can ask for funds under the title "maintenance" in the annual budget when it does not cost significant amount.

10. What maintenance agreements were signed with security providers?

We don't have any agreements with security vendors. But for servers we have maintenance agreements with the vendor.

11. How effective are they?

Averagely they are OK with the service provided.