An Assessment Strategy to Measure effectiveness of ISG Implementation in the Institutes of Higher Education

D.S. Bhilare
Head Computer Centre Devi Ahilya University, Indore, India

Abstract

Establishing a resilient information security mechanism, in the institutes of higher education (IHE) requires not only understanding of expectations of the academic environment, but a thorough understanding of legal aspects and obligations of the institute in protecting information assets. It is essential to have an Information Security Governance (ISG) plan in place. However, an existence of Information Security Governance plan is not the end of the process. Rather, it is an essential first step to secure information systems and strengthen overall information security. It is equally important to have an effective assessment strategy to measure performance of the ISG implementation.

In this paper due attention is given to the assessment activity and a quickly deployable assessment strategy is proposed, which provides a broad view of the institutes present state of information security. The Information Security Governance (ISG) Assessment strategy is intended to help IHE ascertain the effectiveness of existing ISG Framework. The objective is not to provide an exhaustive checklist of information security policies or practices. The quick assessment allows assessment of key elements in quantitative terms and takes less time to evaluate.

The proposed assessment plan is adaptable, easy to deploy, and based upon industry best practices and standards. The plan by virtue of its design enforces integration with the ISG plan. The implementation of the assessment strategy is carried out for a local university and the results and analysis are also presented.

KEYWORDS: Information security, ISG, Assessment

INTRODUCTION

Information Security Governance Assessment provides a comprehensive view on the current state of an institutions security posture. Existing security processes are assessed for adequacy and operational effectiveness. The scope of assessment encompasses analyzing applicable security controls for critical business processes, IT operations, outsourcing, business continuity, network and applications. Information security governance is a coherent system of integrated security components (products, personnel, training, processes, policies, etc.) that exist to ensure that the institution survives and provides desired services.

Trends of Information Security Governance: Initially the focus was on security controls, which was purely of technical nature. Later the focus shifted to management of the Information Security, and at present the focus is on its governance. Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting, and accountability.

Generally, the instructional and research environment of colleges and universities is more open than in government or corporate training departments and

research laboratories. The academic culture tends to favor experimentation, tolerance, and individual autonomy. These characteristics make it difficult to create a culture of computer and network security [1]. The isolated campus network is a thing of the past. Faculty and students with laptops and wireless technology means the University network has no boundaries. VPN remote access, Web-based applications available directly from the Internet also contribute to the end of the traditional network perimeter [2] [3].

The university fraternity needs to be aware of implications of the security breaches. As it threatens the reputation of institutions; and increases the risk and associated liability for unauthorized access or disclosure of information, protected by IT Act. It also increases the risk of law suits being filed by commercial organizations affected due to unprotected campuses. The compromised infrastructure wastes publicly-funded network & system resources and may result in premature disclosure of research outcomes.

Although information security is often viewed as a technical issue, however, it is also a governance challenge that involves risk management, reporting and accountability [4]. It requires an active and committed engagement of executive management. Information security governance is the responsibility of the top management. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. [5].

Information security governance is all of the tools, personnel and business processes that ensure that security is carried out to meet an organization's specific needs. It requires organizational structure, roles and responsibilities, performance measurement, defined tasks and oversight mechanisms [6].

Various studies [7] of academic environment suggest that, in several ways IHE characteristics are different from corporate environment and securing an academic campus requires consideration of these differing factors. Corporate Intranets have advantage of strict policy formulation and implementation, whereas educational institutes demand more flexibility and freedom. Corporate users are well trained during induction, where as its relatively difficult for an educational institution, due to large intake every year. Availability of funds is also an important issue while selecting appropriate solution.

Information security involves risk management, reporting, and accountability. In order to secure information assets, information security measures must be periodically assessed. A formal assessment strategy is also needed to effectively monitor and assess the Information Security efforts in the Institution.

RELATED WORK

To achieve the desired level of success, institutions must make enterprise security the responsibility of executives at the highest level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance [8]. The Information Technology Governance Institute (ITGI) claims that Corporate Governance and IS Governance can no longer be seen as two separate disciplines [9]. Therefore, IT can no longer be seen as an issue that is only of a technical nature. Security is more than selection and deployment of technology. “if you think that technology can solve your problem, than you don’t understand the problems and you don’t understand the technology”, Bruce Schneider.

Because security is now a business problem, the organization must activate, coordinate, deploy, and direct many of its core resources and competencies so security

risks are managed and aligned with the entity's strategic goals, operational criteria, compliance requirements, and technical system architecture. To sustain enterprise security, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals [10]. Such a process needs to account for the fact that policies, procedures, and technologies are dynamic.

ISO 17799 and ISO 27001 provide a top-down and consistent approach to address all compliance, risk, and governance issues related to information security. Most of what is needed to address compliance best practices, and standards are the same and ISO has unified these into one framework. The direct and indirect benefits are shown below. While other frameworks have value in managing information security, only ISO 27001 goes beyond a framework to provide an international standard that information security practices can be independently certified against.

There are some significant contributions based upon the IT Act 2000/2008, which are available as Indian Information Security Framework (IISF-309), which is built under the following principles [11].

- The framework is flexible enough for users in different user segment with different operational sizes to adopt practices which are appropriate and affordable. It does not mandate any specific security standard such as ISO 27001 or any other.
- It incorporates the best practices in current usage but makes fine changes as required by ITA 2008.
- It gives value for "Disclosure" and "Accountability". Accordingly, it recommends a security policy to be announced by the organization and that a "Compliance officer" to be designated.
- It banks on a "Client Consent" which makes framework legally binding on the prospective victim and hence meets the first of the three criteria suggested by Section 43A under explanation(ii)

PROPOSED ASSESSMENT STRATEGY

Methodology

The proposed methodology for developing an appropriate assessment strategy considers the following design objectives and constraints: The proposed Assessment Strategy should be flexible, which can be adapted according to existing institutional structure and resources. The assessment strategies should facilitate quick assessment, which can be repeated frequently.

The study is qualitative in nature and essentially divides into two distinct components: a literature review and the application of the findings from literature in the development of a model for practical implementation. The majority of the study is a literature research of the selected best practices and related documents regarding Corporate Governance, Information Technology Governance and Information Security Governance.

Based upon the findings about vulnerabilities, available technologies, present state of awareness, preventive measures, security policies, applicable laws, technologies deployed, lessons learnt and practices being followed at various academic institutions, ISG assessment plan shall be developed. In order to assess effectiveness of the existing ISG implementation the proposed assessment strategies shall be designed. The assessment will provide:

- A fair idea about information security posture of organization before and after implementing the ISG;
- Evidence about the effectiveness of the security controls in the organizational information security system;
- An indication of the quality of the risk management processes employed within the organization; and
- Information about the strengths and weaknesses of an organization's information system which is supporting critical business functions.
- A comprehensive view of the organization's overall security status.

Design Considerations, Principles and Challenges

The survey of Indian Universities [12], shows that there are institutions having some basic ISG structure, but there are many still struggling to make a beginning.

The IT Act 2008 states that organizations handling sensitive personal data need to follow "Reasonable Security Practices" (RSP), under section 43A, failing which they will be liable for paying compensation to any person who suffers a loss. Similarly, under Section 79, there is a need for "Intermediaries" to follow "Due Diligence". Though "Due Diligence" cannot be prescribed and has to be left to be decided on a case to case basis, in case there exists a standard security practice, it could be a starting point to bench mark the requirements under due diligence. IT Act 2008, also provides data retention norms under section 67C, which should be considered part of the "Reasonable Security Practices".

While designing the assessment strategy the documents listed below were referred along with the research papers mentioned in the related work:

- Corporate Task Force Recommendation, Information Security Governance a call to action, April 2004 [13].
- Information Security Governance**:** Toward a Framework for Action, business software alliance, 2005 [14].
- Guide for Developing Performance Metrics for Information Security, NIST Special Publication 800-80 [15].
- Prioritizing IT Controls for Effective, Measurable Security. DHS, October 2006 [16].
- Introduction to Security Governance, August 22, 2006 [17].
- Aligning CobiT, ITIL and ISO 17799 for Business Benefit: Management and Summary
- Governing for Enterprise Security (GES) Implementation Guide Carnegie Mellon University, Software Engineering Institute, CERT, August 2007
- **National Institute of Standards and Technology** Key Standards and Guidelines

The proposed strategy allows quick assessment of the key elements in quantitative terms and takes less time to evaluate. The quick assessment may be done more frequently, preferably on monthly basis. Like quality, Information Security is also a continual improvement process where perfection is desired but rarely achieved. By making incremental improvements over time, periodic cycles of assessment, remediation and reporting significant and measurable progress can be achieved. The major target is to keep the process as simple as possible. One must start the process

with the activities having major impact first. While proposing the assessment plan, efforts are made to ensure that the plan:

- Enables consistent, comparable, and repeatable assessments of security controls;
- Facilitates cost-effective assessment of effectiveness of security controls;
- Promotes a better understanding of the risks to organizational operations, organizational assets, individuals, and other organizations; and
- Generates comprehensive and reliable information to support security assurance decisions.

Based on the guidelines published by various standards agencies NIST (800-53)[18], ISO 27001, Policy documents of various universities [19],[20],[21], Indian IT Act 2000 [22], UGC/AICTE guidelines and the requirements of academic environment as discussed above, the following plan is proposed.

The assessment plan is divided into five groups: Institute Profile, Information Security Risk Management, People, Process, and Technology. The following resources were referred while designing and building the quick assessment plan.

- Corporate Governance Task Force, 'Information Security Governance: Call to Action', USA, [13]
- Information Security Governance Assessment Tool, Educause [23]
- Program Review for Information Security Management Assistance (PRISMA) NISTIR 7358 [24]

The details of the proposed assessment strategy

The survey conducted during the research for the Indian Universities shows that, only nine percent institutes have periodic review procedure in place. According to the CSI 2008 survey results, respondents with IT security plans in place, have more satisfied users compared to the others.

The proposed assessment strategy helps institutions in quickly assessing the extent to which ISG has been implemented and its effectiveness. This would supplement the role based assessment metric described earlier. It will not provide detail list of controls and best practices. Rather, it is intended to help a Vice-Chancellor or Application Owner, identify general areas of concern as they relate to the ISG framework. If a particular question can't be answered affirmatively, then that question indicates an area the institution needs to examine, to determine what risks may be associated with it and how the institution will address those risks.

The first section of this assessment plan will help an institution understand its profile and dependency on Information Technology. The remaining sections are intended to help IHE, determine the maturity of the information security governance at a strategic level. The overall rating (good, needs improvement, poor) will depend on the score obtained and dependency on IT. The purpose of this metric is to address two issues: First, quickly assess institutes security posture, as the other metric is lengthy and time consuming. Second, allow monthly assessment and see improvements with immediate past performance.

Assessment parameters are grouped in five logical units: Institute Profile, Information Security Risk Management, People, Process, and Security Technology used. Each group is described below:

Group I (Institute Profile):

This group assists in assessing overall dependence of the institution on IT and availability of resources. Based upon size and resources available, grading scale is also increased. (See Table 7).

Table 1: Institute Profile

Grading Scheme(0 to 4 Points): Very Low = 0; Low = 1; Medium = 2; High = 3; Very High = 4

S.No.	Parameter	Points
1	Impact of major system downtime on normal functioning	
2	Impact of Internet failure on normal business functioning	
3	Percentage of students registered in the distance education program Above 35 % very high 25-35 % High 15-25 % Average 05-15 % Low 0-5 % Very Low	
4	Level of foreign collaboration in research and teaching	
5	Compliance with IT ACT 2000 and 2008 amendment	
6	Impact of security incident on future revenue	
7	Extent of outsourcing of the operations	
8	Stakeholders' sensitivity to security	
9	Value of institutions research outcomes and other intellectual property stored	
10	Impact of security incident on stake holders (Student, Faculty etc)	
	Total Points	40

Group II (Information Security Risk Management):

These group of parameters help in assessing level of Information Security Risk Management activities.

Table 2: Information Security Risk Management

Grading Scheme (0 to 4 Points): Not Implemented = 0; Being Planned = 1; Implementation Initiated = 2; Partially Implemented = 3; Fully Implemented = 4

S.No.	**Parameter**	**Points**
1	Identification of critical assets, functions and associated threats & vulnerabilities?	
2	Has a cost been assigned to each critical asset or function?	
3	Do you have written IS plan?	
4	Does your institution has an IS assessment plan?	
5	Does your institution have a Disaster Recovery Plan?	
6	Does your institution have a Business Continuity Plan?	
7	Is there any annual review to verify compliance with government laws?	
8	Is there any periodic review of the present IS practices?	
	Total Points	32

Group III (People):

This group helps in assessing people element of the overall programme.

Table 3: People

S.No.	Parameter	Points
1	Resources are enough to successfully implement the IS program ?	
2	Do the CISO & his staff has the necessary experience and qualifications?	
3	Does the responsible IS personnel's have necessary authority?	
4	Does Executive- Council and Vice-Chancellors are getting periodic report on effectiveness of IS program	
5	Is responsibility and authorities clearly described as who will do what, when and how?	
6	Do you have a continuous skill up gradation and new technology absorption program for IT technical team	
7	Every department dean and department head knows what is his role and responsibilities	
8	Have persons accountable for BCP and DRP are clearly identified?	
9	Does all the departments are participating in the IS initiative and complying with the IS procedures.	
10	Have you implemented an IS training program for faculty, student and staff	
	Total Points	40

Group IV (Process):

This group helps in assessing process of Information Security Governance.

Table 4: Process

S.No.	Parameter	Points
1	Do you have a process to assess information assets and functions, which communicates level of security?	
2	Do you have an IS specialist who architects the institutional security requirements into an implementable program?	
3	Do you have a configuration management, patch management strategy, policy, and procedures in place along with responsibilities?	
4	Do you involve the security personnel during new H/W or S/W acquisition or in-house development of applications?	
5	Do your security policies effectively address the risks identified in your risk analysis/risk assessments?	
6	Are relevant security policies included in all of your third-party contracts?	
7	Are there documented procedures for granting exceptions to policy?	
8	Do you have written institutional IS policies available to all the stake holders?	
	Based on your information security risk management strategy, do you have official written information security policies or procedures that address each of the following areas?	

9	Acceptable use of computers, e-mail, Internet, and intranet	
10	Protection of organizational assets, including intellectual property	
11	Access control, authentication, and authorization practices and requirements	
12	Data classification, retention, and destruction	
13	Vulnerability management (patch management, antivirus software)	
14	Disaster recovery contingency planning (business continuity planning)	
15	Security Compliance & Incident reporting and response	
16	Do you maintain a current inventory of both the physical network elements (routers/switches, subnets, DNS, DHCP servers) and also the logical network assets (domain names, network addresses, access control lists, and present configuration files)?	
17	Does your organization periodically test and evaluate or audit your information security program, practices, controls, and techniques to ensure they are effectively implemented?	
18	Reporting security events to affected stake holders	
19	Is your critical hardware and wiring protected from power loss, tampering, failure, and environmental threats?	
20	Are multiple physical security measures in place to restrict forced or unauthorized entry?	
21	Do you carry out background check before giving access to insider or outsider?	
	Total Points	84

Group V (Security Technology Used)

This group helps in identifying technologies being used and its impact on other security functions.

Table 5: Security Technology Used

Grading Scheme (0 to 4 Points): Not Implemented = 0; Being Planned = 1; Implementation Initiated = 2; Partially Implemented = 3; Fully Implemented = 4

S.No.	Parameter	Points
1	Anti-virus, Anti-spyware software	
2	Application-level firewalls	
3	Biometrics	
4	Data loss prevention / content monitoring	
5	Forensics tools	
6	Encryption of data in transit	
7	Encryption of data at rest (in storage)	
8	Endpoint security client software / NAC	
9	Firewalls	
10	IDS/IPS	
11	Log management software	
12	Configuration Management	
13	AV Definition upgradation	
14	Patch Management	
15	Public Key Infrastructure systems	

16	Server-based access control lists	
17	Smart cards and other one-time tokens	
18	Specialized wireless security systems	
19	Static account / login passwords	
20	Virtualization-specific tools	
21	Virtual Private Network (VPN)	
22	Vulnerability / patch management tools	
23	Web / URL filtering	
24	centralized data backup & recovery system	
	Total Points	96

Assessment Summary

The following table gives group wise summary of the scores obtained, total score and the grade awarded.

Table 6: Group Wise Assessment Summary

Sub-Group No.	Sub Group	Max. Score	Cut-off Score	Monthly Score
1	Institute Profile	40	16	
2	IS Risk Management	32	13	
3	People	40	16	
4	Process	84	34	
5	Technology	96	39	
	Total Score	292	118	
	Final Grade			

Final Grading Criteria:

The final grades are given on the basis of the profile score and corresponding assessment range, as shown in the table 7. For example, if a medium sized institute (Profile Score in the range 10 to 30), earns 191 points, i.e. total of four categories (IS Risk Management, People, Process, and Technology), out of 252, then as per the table the institution would be graded as "good".

Table 7: Table Showing Final Grading Scheme based upon institute profile

S.No.	Institution Profile	Total Score Out of 256	Assessment
1	Small (0 – 10 Points)	0-97 98-137 138-170 171-252	Poor Average Good Very Good
2	Medium (11 – 30 Points)	0-121 122-162 163-194 195-252	Poor Average Good Very Good
3	Large (31 – 40 Points)	0-145 146-178 179-210 211-252	Poor Average Good Very Good

Experimental Results

In this case study, one year's data for the Devi Ahilya University is collected and the results are shown below. The progressive results of the quick assessment plan II, are shown in the group wise tables. The frequency of the assessment was bi-monthly. The changes and impact of the ISG over the period are analyzed and presented using graphs and tables. Bi-monthly, detailed score for each group/parameter is given in the appendix "B".

As explained earlier, assessment is divided into five groups. Bi-monthly data was collected for the groups: Institute Profile, IS Risk Management, Process, People, and Technology used. Group wise analysis of the collected data is presented below:

Institute Profile

The total score for November 2009, for this group is approximately fifty percent, which indicates that the Devi Ahilya University is not fully dependent on IT, but there is substantial jump in the score compared to initial months. The jump is due to the fact that the some modules of the University Automation Project, became operational during this period. It is expected that in near future reliance on IT would increase from fifty percent, when the remaining module also become operational So, it is the right time to have ISG in place.

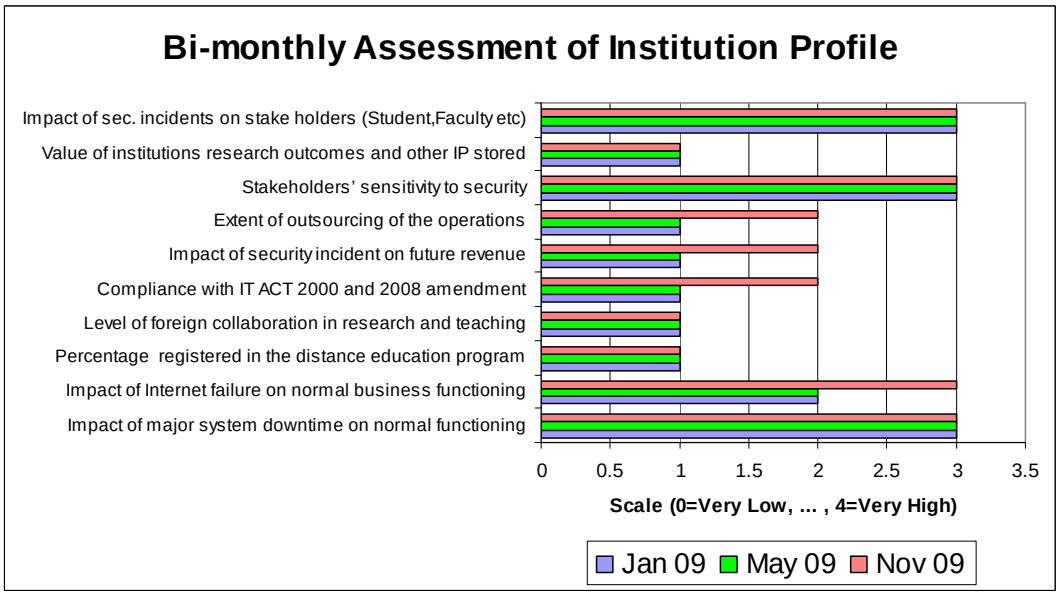

Figure 1: Bi-monthly Assessment of Institute Profile

Information Security Risk Management (ISRM)

Parameters of this group, focuses on assessment of the risk management process, as it relates to creating an information security strategy and program. In this group DAVV has scored twenty one points out of thirty two i.e. around 66 percent, which is an acceptable steady improvement, compared to the modest beginning of fourteen points. As none of the parameter is implemented fully, there is enough room for improvement, which may be achieved with continuous assessment and follow up.

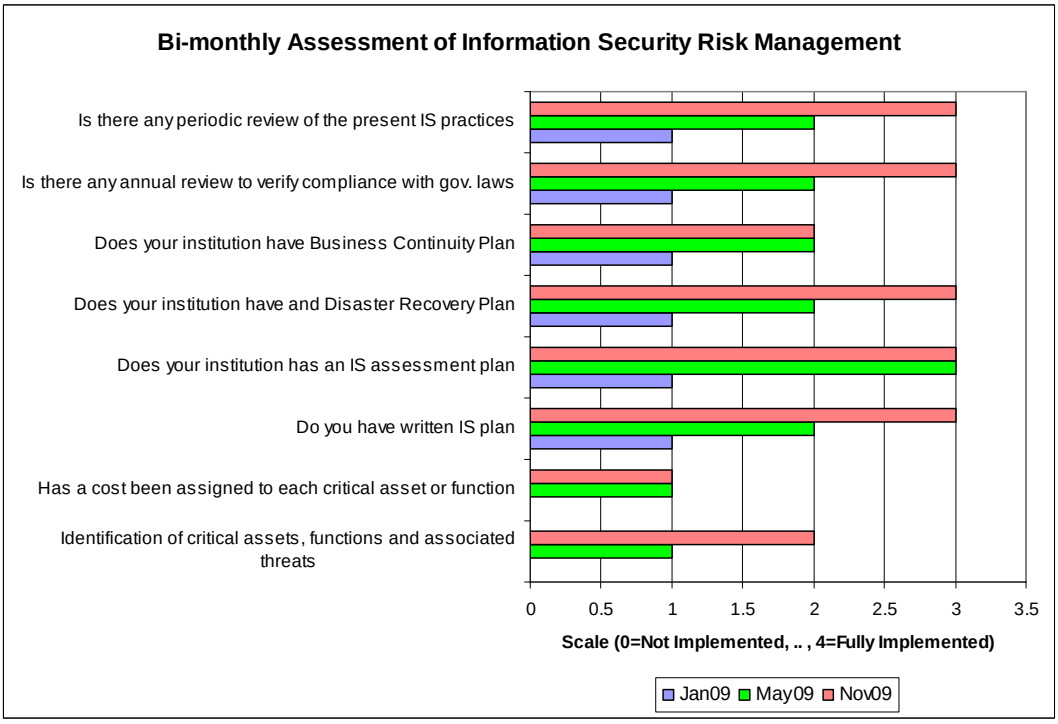

Figure 2: Bi-monthly assessment of Information Security Risk Management

People

In this group, organizational aspects necessary to implement the Information Security Governance are evaluated. The total score for November 2009, is approximately 70%, which indicates satisfactory performance. There are some gray areas like less involvement of top management in the process. It is encouraging to see that even in this period of economic slow down, university is not facing any resource crunch. Second, important finding is that enough authority has been delegated, as far as IS management is concerned. Some of the activities are in the initiation stage, which also indicate that, there is a management consent, and full implementation is matter of time.

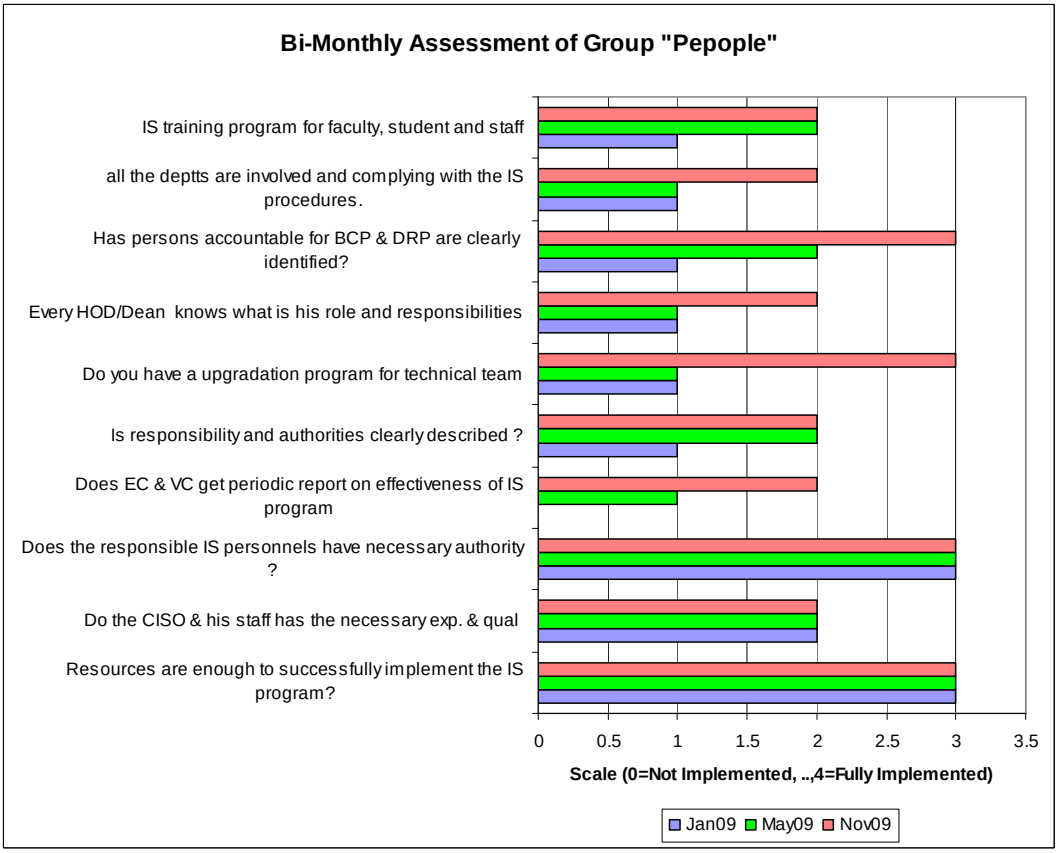

Figure 3: Bi-monthly assessment of group "people"

Process

In this group, processes necessary for implementation of the Information Security Program, are assessed. Overall score of this group is 46 out of 84, i.e. 54 percent, which is on lower side. Therefore, there is a scope of improvement in this group. There are three parameters which could not score any point, are given below:

- Is there an IS specialist who architects the security requirements?
- Are there procedures for granting exceptions to policy?
- Background check before giving access to insider or outsider?

The University has got highest score in deployment of anti virus software, definition updation and patch management. Another weak area is third party contracts, where university security policies are not reflecting in the terms and conditions. There is a scope of improvement in Business Continuity Planning, Disaster Recovery, Incident Reporting, Data Retention, and Data Destruction procedures. An inventory of Hardware Configuration and Server Configuration files is being maintained. There is a satisfactory arrangement of power backup devices for required capacity and for reasonable amount of time. Almost all the critical devices have access to the uninterrupted power supply, which can sustain at least 12 Hours.

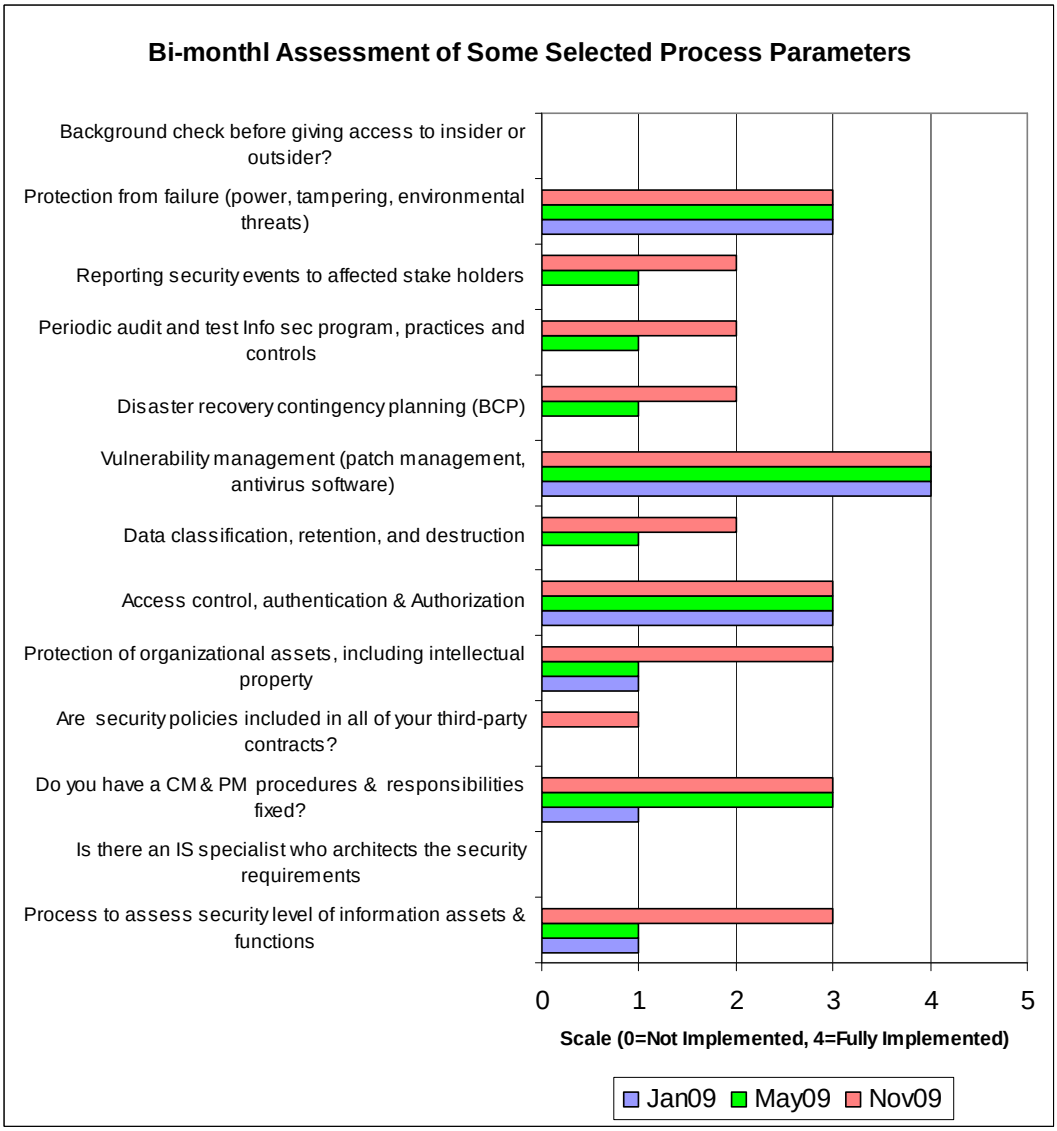

Figure 4: Bi-monthly assessment of group "Process"

Technology Used

In this group, type of technologies being used in the institution, are assessed. Overall score of this group is 56 out of 92 i.e. 61 percent, which is not very poor, but still it can be further improved., shows that the following are the strong points of the University Information Security Management, as minimum points received are not less than four:

- Anti-virus, Anti-spyware software
- Application-level firewalls
- Firewalls
- AV Definition upgradation
- Server-based access control lists
- Web / URL filtering

The following are the weakest areas where points received are not more than one:

- Use of Biometrics
- Forensics tools
- Encryption of data at rest (in storage)
- Public Key Infrastructure systems
- Smart cards and other one-time tokens
- Specialized wireless security systems
- Virtualization-specific tools
- Virtual Private Network (VPN)
- centralized data backup & recovery system

Technology is an area, which can be adopted and implemented; in lesser time compared to the people dependent areas. Therefore, there is a scope of achieving better results in short time.

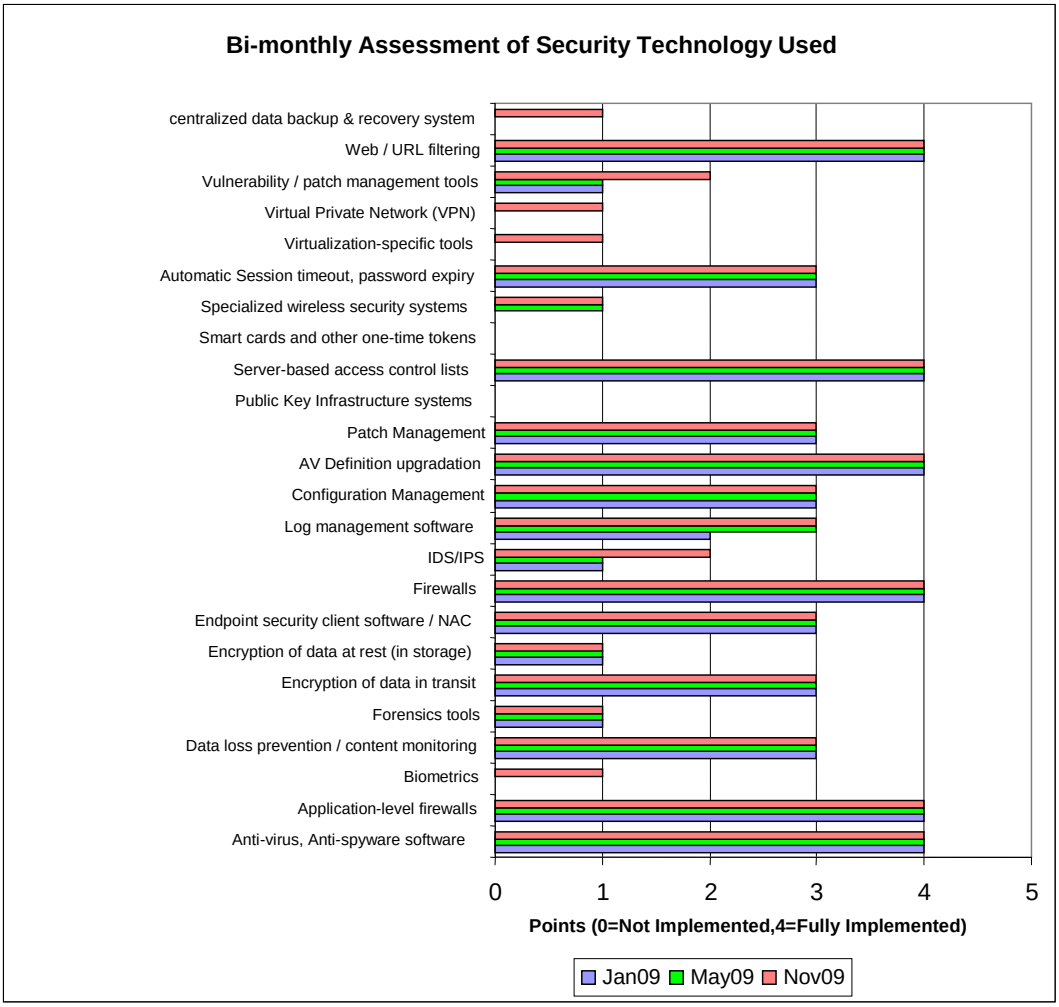

Figure 5: Assessment of group "Security Technologies" being used

Overall Assessment Summary

The following table gives group wise bi-monthly statistics for the period 2009. The table also shows group-wise maximum possible marks and minimum cut-off marks. Final grading is not done, if group-wise minimum cut-off marks are not obtained.

In the initial assessment, three groups: ISRM, People and Process, failed to get minimum cut-off points. However, there is a progressive improvement, which can be noticed in all the groups. At present University rating, for the month of November, 2009 is "Average", as score obtained for four major groups is 146, which lies in the range 122-162 (Table 7). With little efforts, present grading may improve upwards, as these are the early stages of the Information Security Management in the Indian Universities.

Table 8: bi-monthly group wise Summary of scores for the period 2009
Devi Ahilya University

Sub Group	Max	Min	Jan 2009	Mar 2009	May 2009	Jul 2009	Sep 2009	Nov 2009
Institution Profile	40	16	17	17	17	19	21	21
Information Security Risk Management (ISRM)	32	13	6	14	15	17	19	20
People	40	16	14	17	18	20	22	24
Process	84	34	18	24	29	35	42	46
Security Technology	96	39	48	48	50	51	55	56
Total	**292**	**118**	**103**	**120**	**129**	**142**	**159**	**167**
Total (People+Process+ Technology+ISRM)	**252**	**102**	86	103	112	123	138	146

Final Grade (Result): "**Average**" **(Based upon the criteria shown in the Table 7)**

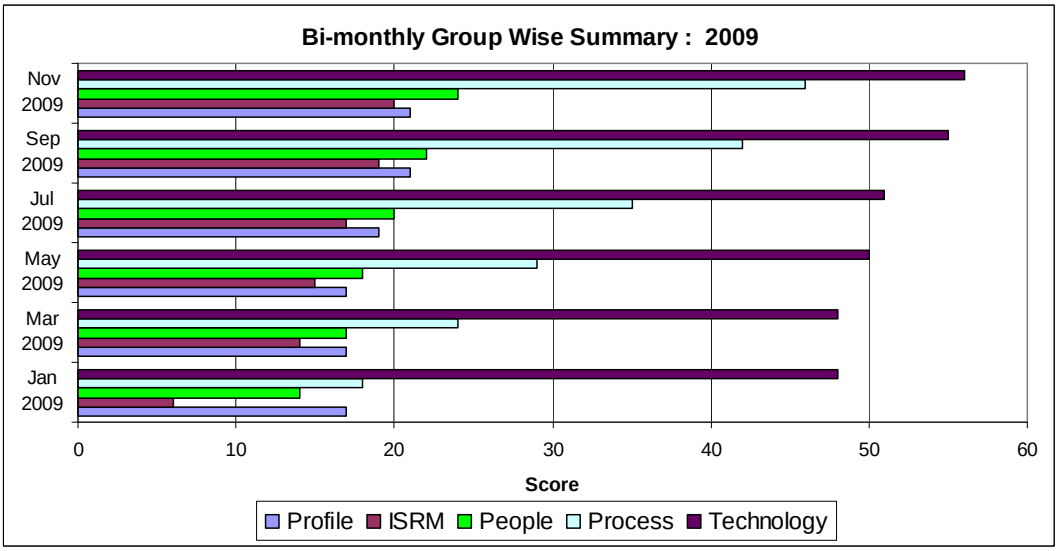

Figure 6: Group Wise Assessment Summary (Bi-monthly)

The overall results and data analysis outcome are encouraging and the top management believes that, over the period of time 95% score is achievable. Thus, if this exercise is conducted continuously and in right spirit, then it may prove an

effective catalyst towards implementation of the ISG in the Institutes of Higher Education.

The proposed assessment framework, enables institutes of higher education to implement a formal framework, which is adaptable, easy to deploy, and based upon industry best practices and standards.

CONCLUSION

The proposed assessment plan enables institutes of higher education to implement a formal mechanism, which is adaptable, easy to deploy, and based upon industry best practices and standards. The framework, by virtue of its design, enforces integration with the existing ISG framework. The assessment plan of ISG is developed as per the specific needs of the academic environment. The proposed assessment plan shall improve overall security governance and ensure more secure campuses. The proposed assessment plan allows a quick deployment and assessment, which provides a broad view of the institutes present state of information security. The quick assessment allows assessment of key elements in quantitative terms and takes less time to evaluate.

Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting, and accountability. In order to secure information assets, information security must be treated as an integral part of the institutions overall governance. Thus, it is concluded that the work presented here shall help IHE in building more secure campuses; where confidentiality, integrity, and availability of the information is assured.

Future Research: An automated assessment system may be developed to increase the frequency of the assessment. Further, there should be mechanism to estimate potential loss in financial terms due to security breaches as well money saved due to proactive actions.

REFERENCES

[1]The CIS Security Metrics Service, The Center for Internet Security (CIS), http://securitymetrics.org/content/attach/Metricon3.0/metricon3-kreitner%20handout.pdf, July 2008.

[2] Caulkins, J., Hough, E. D., Mead, N. R., & Osman, H. "Optimizing Investments in Security Countermeasures: A Practical Tool for Fixed Budgets." *IEEE Security & Privacy 5*, 5 , October 2007

[3] Kaufman, Second Edition, 2007, “Network Security, private communication in a public world”, Pearson Education, 2007.

[4] Allen, Julia. “Security Is Not Just a Technical Issue.” Build Security In web site, Department of Homeland Security, https://buildsecurityin.us-cert.gov/daisy/bsi/chapters/best-practices/management/563.html , October 2006.

[5] Judith B. Karuso, “Information Technology Security: Governance, Strategy, and Practice in Higher Education”, ECAR, http://net.educause.edu/ir/library/pdf/EKF/ekf0305.pdf, 2006.

[6]Shon Harris, “Information Security Governance Guide”, http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1211236,00.html, August 2006.

[7] Lianying Zhou,Fengyu Liu, "Research on Cooperative Computer Network Security Technologies", IEEE international conference on man, machine and cybernatics, 2004.
[8] Jody R. Westby, "Governing for Enterprise Security (GES) Implementation Guide", Carnegie Mellon University, Software Engineering Institute, CERT, August 2007.
[9] Gamma , *Corporate Governance.* http://www.gammassl.co.uk/bs7799/corporate%20governance/index.html, 2004
[10] Acuff, Jr., A. Marshall. "Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business," Institute of Internal Auditors.
http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=143, 2000.
[11] Indian Information Security Framework, IISF-309, www.naavi.org, March 2009.
[12] D.S. Bhilare et al., **"**An investigation of information security issues in the Indian institutes of higher education: current security state and practices"**,** Accepted by International Journal of Computer and Network Security, ISSN: 2076-2739, January (Vol.2 No.1), 2010.
[13] Corporate Governance Task Force, 'Information Security Governance: Call to Action', USA, 2005
[14] Information Security Governance: Toward a Framework for Action, business software alliance, http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx, 2005
[15] Elizabeth, Chew, et al. Guide for Developing Performance Metrics for Information Security, Initial Public Draft (NIST Special Publication 800-80). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/index.html, May 2006.
[16] Kim, Gene, et al. "Prioritizing IT Controls for Effective, Measurable Security." Department of Homeland Security, Build Security In web site, https://buildsecurityin.uscert. gov/daisy/bsi/articles/best-practices/deployment/577.html, October 2006.
[17] Harris, Shon. "Introduction to Security Governance." SearchSecurity.com,
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210565,00.html, August 2006.
[18] Nist Publications: computer security resource centre, SP800-53, src.nist.gov/publications/nistpubs/,
[19] University of Houston, Information Security Manual, http://www.uh.edu/infotech, referred 2008
[20] University of Washington policy document, http://www.wustl.edu/policies/compolcy.html, October 2006.
[21]University of Auckland Newzeland, Security policy and organization http://www.auckland.ac.nz/security/SecurityOrganisationPolicy.htm#1.1, Jan 2008
[22] Information Technology ACT 2000, www.eprocurement.gov.in/news/act2000mod.pdf
[23] Educasue, "Information Security Assessment Tool in Higher Education", net.educause.edu/ir/library/pdf/SEC0421.pdf, 2005
[24] Pauline Bowen, Richard Kissel, Program Review for Information Security Management Assistance (PRISMA) NISTIR 7358, 2007