Business Case Study - Akurana University

I hereby welcome you to present your proposal for solving how we should manage information security at Akurana University directly to our top management. In planning for this meeting, here is a little background information on our current situation in terms of managing the university in general and managing information security. The picture I give below is far from complete, but please use it as the basis for your solution. As I mentioned on the phone, Akurana University is a medium sized public university located in Akuran. The institution is situated on a beautiful one square kilometer large campus, not far away from the major city.

History

The University of Akurana (UA) was established on 1st September 2002 by merging the Institute of Computer Technology (ICT) and the Department of Computer Science (DCS), by an Order made under Section 24 A (1) of the Universities Act No. 16 of 1978 as last amended by Universities (Amendment) Act No.1 of 1995, as a Centre of Higher Learning for the purpose of providing, promoting and developing higher education in Computer Science, Information and Communication Technology.

Background

(a) Ungraduated studies

As a center of Higher Learning in Computing the UA has continued to train students at undergraduate and postgraduate levels as well as those in the IT industry with the latest developments in this field. Seven hundred and sixty-nine internal undergraduates have enrolled for the four degree programs offered. UA offers Computer Science and Software Engineering education under the Bachelor of Computer Science and Information Systems under Bachelor of Information Systems intakes. Beside 1,275 science graduates were trained in the use of IT in respective scientific domains and 2,034 students were provided the opportunity to do the BIT degree as external students. Taking into consideration the job opportunities that exist for ICT graduates, the UA took the initiative to launch the three-year External Degree Program leading to the award of Degree of Bachelor of Information Technology (External) in 2000. External candidates can learn for BIT online with optional assistance from private training institutions.

(b) Postgraduate studies

University of Akurana offers postgraduate and research degrees across disciplines in Computer Science, Information Technology and Information Security enabling candidates to uncover new knowledge either by the discovery of new facts, the formulation of theories or the innovative reinterpretation of known data and established ideas.

(c) Research

The UA operates on a devolved research basis, based upon a Research Group structure. Each Research Group has its own culture and strategy matched to the cutting edge of contemporary science in that area.

Departments and centers

The UA has three academic departments and the academic staff is allocated to these departments based on their specialization and teaching expertise. Three department heads are assigned to look after the undergraduate, postgraduate and external & extension programs respectively as none of them offer programs of its own. The three departments are,

1. Computation & Intelligent Systems (CIS)

2. Communication & Media Technologies (CMT)

3. Information Systems Engineering (ISE)

UA also performs many secondary activities. These activities are organized under six separate centers. Each center has a head who manages the day-to-day operations of the center. The six centers are as follows:

1. Network Operating Center (NOC)

2. Students and Staff Welfare Center (SSW)

3. External Degrees Centre (EDC)

4. e-Leaning Centre (ELC)

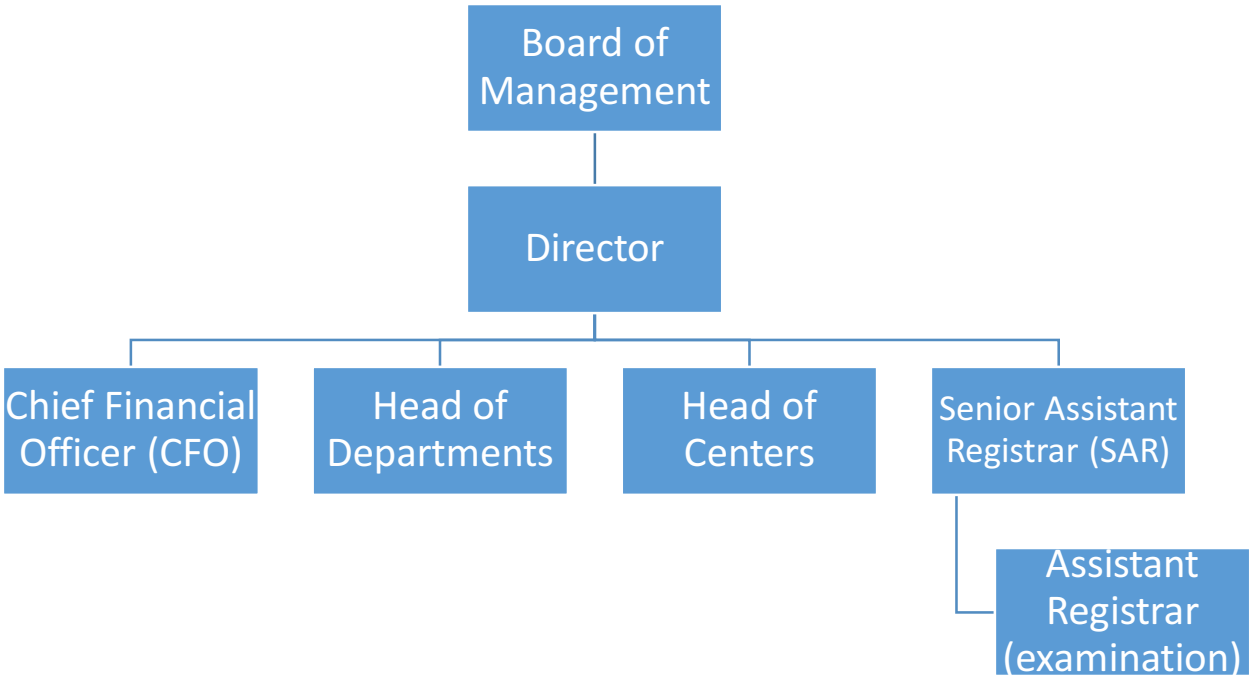
5. Professional Development Centre (PDC)

6. Centre for Digital Forensics (CDF)

Governance and Management

The UA is governed by a board of directors, who also form the top management team. We use the terms board, board of directors and top management interchangeably. There are 12 members in the Board of Management. Management of the UA is handled by the Director of UA with Chief Financial Officer (CFO) and Senior Assistant Registrar (SAR) of Administration. The director is also assisted by head of departments and centers. Information Security related incidents are reported to the director through the head of Network Operating Centre (NOC). The SAR handles facilities, buildings, recruitments, employees' issues, contracts with external parties including that private security firm that provides security guards.

The CFO is the head of the Finance Division. He is responsible for managing and reporting the financial state of the University. The division was made up of six departments: Financial Affairs, the Budget Office, Internal Audit, Accounts Receivable, Accounts Payable, and Student Services. All financial information reporting was overseen by the Financial Affairs department. Overall, the Finance Division employed 30 permanent employees and several part-time members on a need basis. The CFO is also responsible for operational risk. The chief internal auditor directly reports to the board of management.



Finance

Recurrent and capital expenditure of the UA is USD 300 Million. Part of that amount is funded by the government and the institute receives the balance amount from conducting external courses, external consultancy, and research work. Furthermore, a substantial amount is received as the interest income from the fixed deposits held in banks. Total assets of the institute is over USD 2 Billion.

Online services

The UA has a web portal where students can pay various fees using their credit cards. The payment gateway has been obtained from Asmpath Bank.

Data and information

Information collected and stored include but not limited to:

- Names
- Date of birth
- Credit Card information
- Social Security Number
- Examination results.
- Financial status of the students and their parents.
- Medical records. (Students who are absent for some classes or examinations have to provide medical certification, if a student wants to retake the missed class or examination.)

Departments and centers

All IT services are provided by the Network Operating Center (NOC). All server functions in the NOC. In addition to twelve (12) permanent and contract staff, NOC hires temporary employees including interns. Interns are internal students of the university who are placed in the various places to obtain industrial exposure. Interns are assigned by the head of the departments. In addition to providing and maintaining the IT infrastructure, the network center (NOC) provides application software and related services to all departments and centers. The employees of the NOC have access to every databases in the system. Actually, they have passwords to every system. However, as a practice, they do not access them without the permission of the head of the department or center. All information security issues are currently handled by the network operating center. This center is responsible for network security, database security, and application security. There is no formally qualified information security professional attached to the network operating center (NOC). Thus, presently the management of information security can be characterized as *ad hoc* and without any policies or guidelines.

Examinations department is responsible for matters related to conducting examinations. Once the lecturers have submitted the marked answer sheets, one staff members in the examinations department feeds the final marks given in the marked answer sheets into the examination database. Then, the system calculates grades and GPA of students from the data stored in the database. In addition to this normal duty, the department provides an online service through which external parties can verify the authenticity of certificates and transcripts issued by the university. This main server is located at the NOC and remotely accessed by the Assistant Registrar (examinations) from the examinations department.

The financial system creates system logs whenever an event occurs. This feature is very useful for showing what happened within a system. The logging feature shows the time, the user group, and the event that occurred. While the logs are useful, the primary drawback is that they only shows what group created an event. As a result, events could only be seen at the group level. This means if a user logged into the system and made a change and is a member of the administrator group, the log would only show that someone in that group made a change. It does not show which user made the change.

Administrative department hands all recruitments except for interns. After assuming duties, newly recruited individuals have to request an email account from the NOC. This request should be submitted through the respective head of department or center. Employees working under the SAR or CFO have to submit the request through the SAR or CFO. The administrative department has no formal relationship with the NOC. When a request is received, the system administrator working at the NOC would assign a *username*. The user name is the first three letters of the first name of the employee. If the name is already obtained, the user is asked to provide the first three letters of the surname. Once a user has a *username*, the system administrator places the user in the appropriate user group, which determines what functions the user could perform. When an account is set up, the policy is for the system administrator to provide the same generic password. Once a user logs into the system, they are advised to change the default password. The system does not require users to have strong passwords. Passwords could be as short as three characters long and does not need to

include numbers or special characters. The passwords could be kept forever and most have never been changed.

One of the duties of the Welfare Center (SSW) is to reimburse medical expenses of the staff. In order to make the reimbursement, the relevant staff member has to provide the prescription given by a medical officer, the bill given by a health care provider, and the request form. These information are fed into the computer system. This department is looked after by the Senior Assistant Registrar (SAR).

IT infrastructure

This university has a backup power generator and several uninterrupted power (UPS) units. Main servers can run 10 hours with these UPSs. The Internet connection is provided by the leading telecom service provider in the country and additional link from another service provider has been obtained.

The network is divided into four zones (A, B, C, D). All Internet traffic traversing the Zone A security perimeter that a physical server with a data center within the same location. All external parties and external students access the learning management system and other systems placed in Zone A. Zone B is only for academic staff. The remote access facility is not provided for academic staff. This prevents academic staff from accessing the library and other IT services online. Zone C is further divided to financial division and administrative division. Financial data is backed up and kept in the same place during the weekdays. The backup is taken in every Friday evening and is kept in the bank which is 2 km from the organization. Zone D is for students.

In addition to computers provided by the university, students are free to use their own devices. In order to access the Wi-Fi network, students have to obtain permission by giving the MAC address of the device. The devices with the registered MAC address is allowed to access the Wi-Fi network. Except for 4th year computer lab, students are not given the administrative (root access) privileges.

There is no central path-management policy. When someone raises an issue with a machine, vulnerability scan is conducted and that machine is patched, if necessary.

Recent incidents

There have been several incidents took place in the recent past. Appendix A gives the original message received by every staff member. It is reported that 5 academic members and 25 non- academic staff members have positively responded to this message. Only 2 members have reported it as a spam message.

One academic staff member lost his laptop in a public bus. Fortunately, there was no confidential information stored at that time. Usually, that academic staff member prepares examination papers on his laptop. He never uses encryption algorithms.

One intern discovered that several machines were infected with bots. However, the head of NOC has not taken it seriously since no formal complaint was logged.

Your task (Requirements)

This university plans to obtain ISO/IEC 27001 compliance OR certification against ISO/IEC 27001 for information security. You are hired to develop an information security program which is one of the requirements to obtain the ISO certification. You are required to make a presentation to the board of directors / top management to get the support needed so that they buy your service. In your presentation, you have to stress the importance of building an information security function and obtaining ISO/IEC 27001 compliance or certification. Based on your presentation, the board of directors / top management will decide if they want to buy your service or a competitor's.

After hearing several data breaches at many international universities, the board of directors have made risk management a priority. Furthermore, the board has decided to *try* to *align* with the *central aspects* of the new European general data protection regulation GDPR.

Additional information for the presentation

Two board members are technical savvy. Another one is an expert in the banking sector. In making your presentation, you got to know that the board members are interested to get to know additional information. Therefore, you have decided to mention these points also in your presentation. These points are:

- The potential need to be compliant with the PCI/DSS standards
- The potential need to obtain business interruption / cyber insurance
- Risk tolerance and appetite

Some ideas on what to cover

The following points would help you make your presentation. However, addressing every point or following the given order is not necessary.

- The values that this organization is going to create
- Stakeholders, major resources, and other resources
- Risks in general and information security risk
- Necessary processes needed to meet organizational objectives.
- A full description of the process (owners, inputs, output, outcomes) and process environment (regulations and laws)
- Risk involved in the process
- Security requirement for the process (for the information and information systems)
- Identified security requirement and the ISO standards
- Identify the cost of implementing the controls
- A cost benefit analysis
- Frameworks, standards, regulations to be adopted and/or followed.
- Risks to be mitigated and accepted and justification for the residual risk.

- The need for support from the senior executives and other staff members.
- Identify the emergence and possible reactions. (culture/behavior)
- Emerging technologies to mitigate the identified risks.
- Importance of the monitoring process and correcting process.
- Assurance controls for the access to sensitive information
- Access control matrix, RACI chart,

Compulsory presentation content

See grading sheet for compulsory content.

Appendix A

Delivered-To: rnd@UA.cmb.ac.lk

Received: by 10.140.34.38 with HTTP; Mon, 25 Jan 2016 20:29:24 -0800 (PST)

Date: Tue, 26 Jan 2016 09:59:24 +0530

Subject: WELCOME TO UNIVERSITY OF COLOMBO - ONLINE SERVICES

From: Help desk <drsksingh.phy@dcrustm.org>

To: allusers@cmb.ac.lk

Content-Type: multipart/alternative; boundary=001a114710925d5ffa052a352198

Bcc: rnd@UA.cmb.ac.lk

Content-Type: text/plain; charset=UTF-8

General Notice,

We are upgrading from 10GB to 20BG as well as deleting

of inactive Email Accounts. We request you to click on the

upgrading link below or copy the link to your device browser

to update your mailbox account.

http://universityofcolombo-onlineservice.weebly.com

*We will process **your request once we receive your information.*

Admin..