Faculty of Medicine and Dentistry, UofA

Information Technology

Final v2.0

Prepared by: Yuen Ip, Director of Information Technology
Prepared for: FoMD Faculty Management Committee
Date: Nov 16, 2009
## Table of Contents

Executive Summary ................................................................. 3
What is IT Governance? ............................................................. 5
Proposed IT Governance Model ............................................... 10
Appendix A – References ......................................................... 14
Appendix B – Proposed IT Governing Bodies .............................. 15
Appendix C – Sample Questions Related IT Governance ............. 16
Executive Summary

Over the past couple of decades, the collection and accessibility of information has grown exponentially. No longer are organizations putting their focus solely on physical assets to gain competitive advantage. For organizations to stay competitive in a dynamic business environment where information is power, they have to determine and understand how to manage Information Technology (IT) strategically just like any parts of the organizations (Marketing, HR, Finance, etc).

In early September 2009, Vivien Wulff, Executive Director, and Yuen Ip, Chief Information Officer, discussed the need for the Faculty of Medicine and Dentistry (FoMD) to have the proper IT Governance Model to facilitate a clearer, more effective, and efficient decision process in the IT domain. This document describes the need and key areas of IT governance model, and proposes areas where improvements can be made.

The right IT Governance specifies “the framework for decision rights and accountabilities to encourage desirable behaviour in the use of IT” specifically in the following area:

- Business/IT Alignment
- Value Delivery & Performance Measurement
- Exploit Business Opportunities with IT
- Responsible Usage of IT
- IT Risk Management

The above IT governance areas can be achieved through tools/processes such as an annual IT strategic planning process, the oversight of various IT task force or committees, business cases, balanced scorecards, project portfolio management, project charters, value management, risk management plan, annual security audits, etc.

This proposal also includes recommendations to the establishment of the following IT governing bodies to ensure adequate IT Governance:

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Authority</th>
<th>Membership</th>
</tr>
</thead>
</table>
| IT Executive Council | • Provides oversight on behalf of the DEC on topics such as:  
  — The relevance of developments in IT from a business perspective  
  — The alignment of IT with the business direction  
  — The achievement of strategic IT objectives  
  — Risk, return and competitive aspects of IT investments  
  — Progress on major IT projects  
  — The contribution of IT to the business (i.e., delivering the promised business value)  
| • Decides the overall level of IT spending and how costs will be allocated  
  • Approves business cases, IT priorities and milestones  
  • Acquires and assigns appropriate resources  
  • Ensures projects meet business requirements  
  • Reports to the DEC | • Exec Director (Chair)  
  • CIO  
  • Vice Dean Reps (2x)  
  • Chairs from each of IM Steering Committee (4x)  
  • VPIT  
  • Freq of Meeting: Semi-annual |
<table>
<thead>
<tr>
<th></th>
<th>— Exposure to IT risks, including compliance risks</th>
<th>— Containment of IT risks</th>
<th></th>
</tr>
</thead>
</table>
| IM Steering Committee (Education) | • Advises the IT Executive Council on IT strategy  
  • Provides input to the IT strategy in preparation its approval  
  • Focuses on current and future strategic IT issues  
  • Reviews IT Business Cases brought forward to ensure alignment of business strategies  
  • Provides prioritization of IT initiatives within the area  
  • Reviews and proposes IT policies and procedures | • Assists the IT Executive Council in the delivery of the IT strategy  
  • Oversees IT service delivery and IT projects  
  • Reports to the IT Executive Council | IMSC (Education)  
  • CIO, Faculty Learning Committee Reps (2x), Office of Education Reps (2x), CADE (2x), Student Reps (2x) |  |
| IM Steering Committee (Research) |  |  | IMSC (Research)  
  • CIO, Faculty Research Committee Reps (2x) and Office of Research Reps (2x) |  |
| IM Steering Committee (Clinical) |  |  | IMSC (Clinical)  
  • CIO, Clinical Reps TBD, AHS Rep (1)  
  • CIO, Faculty Administrator Committee Reps (3x), Office of the Dean Reps (3x) |  |
| IM Steering Committee (Administration) |  |  |  |
| Technology Council | • Provide technology guidelines  
  • Provide architecture guidelines  
  Consult/advise on the selection of technology within standards  
  • Assist in variance review | • Assists the IT Executive Council in the determination, provision, and review of IT Standards  
  • Reports to the IT Executive Council | IMSC (Administration)  
  • CIO, Faculty Administrator Committee Reps (3x), Office of the Dean Reps (3x)  
  • Chairs (Other than CIO. To be elected by the IMSC)  
  • Term: 2 years as per Faculty Committees terms  
  • Freq: Semi-annual |  |
|  |  |  | CIO (Chair)  
  • IT Manager  
  • Key advisors as required (IT, audit, legal, finance)  
  • Freq: Semi-annual |
What is IT Governance?

According to Peter Weill, Center for Information System Research, MIT Sloan School of Management, IT Governance is defined as:

“… Specifying the framework for decision rights and accountabilities to encourage desirable behaviour in the use of IT”

It is driven by the need for closer interaction and involvement with stakeholders by integrating the three “C’s”: Cooperation, Consensus and Community. In other words, these foundations are also based on the principles of effectiveness, transparency, and accountability.

IT Governance is not about the specific decisions made, but rather about determining who makes each type of decision, who has input into the decision, how one is held accountable for their role. It also defines the structure of the composition of the bodies that make or execute on joint decisions, while providing information about how the different parties work together (Figure 1).

![The Governance and Organization’s Relationship](image)

Figure 1 – The Governance and Organization’s Relationship.
Source: Treasury Board of Canada – IT Governance Overview

Failure to have proper IT governance usually results in one or more of the following risks:
• Wrong IT strategy precludes growth and operational sustainability
• False starts and wasted resources (i.e. money, time and productivity)
• Short-sighted planning
• Fragmented IT planning
• High project implementation failure rates
• Lack of business resumption and disaster recovery planning
• Increased information risks (confidentiality, integrity, accessibility)

The purpose of IT governance is to direct IT endeavours, to ensure that IT’s performance meets the following objectives:

Alignment of IT with the Enterprise
The alignment of IT with the rest of the enterprise is considered to be a very important area of IT Governance for the enterprise to maximize its benefits and leverage future opportunities from IT. Historically, business and IT operated in silos where IT did not fully understand business and vice-versa. Many IT departments were happy to stay in the “technical” world, while business departments experienced the frustrations of not getting the desired end-product. Over the past five years, organizations are increasingly realizing the need to bridge and align IT investments to support enterprise initiatives at a strategic level. Whereas in the past IT acted in a mechanical “back office” role and provided basic infrastructure services such as computer/printer support, emailing services, the best IT departments are now partnering with business by adopting a more “strategic” role with the potential not only to support chosen business strategies, but also to shape new business strategies.

Alignment of IT with the enterprise simply means that the enterprise’s IT investment is in harmony with its strategic vision and objectives. This has to be based on full understanding of the business context while applying a set of processes to translate the organization’s direction into IT strategies and tactics. The following diagram (Figure 2) shows such translation:

![Figure 2 – Business/IT Alignment Flow](image)

Value Delivery & Performance Measurement
The optimization of IT costs while proving the value of IT is an important component of IT governance. Projects or initiatives whose marginal benefits are greater than their marginal costs can be classified as a gain. Where IT projects can be delivered on-time and within-budget delivery of appropriate quality matching the business needs, this often translates to improved operational efficiencies, improved data quality and accuracy, increased customer
satisfaction, etc. In FoMD’s terms, these result in the increased ability for the faculty to more effectively "promote health through innovative leadership in research, education, and service".

According to the IT Governance Institute, in order to achieve the realization of the promised benefits, both IT and business need to define the following relative to IT deliverables:

- Fit for purpose, meeting business requirements
- Flexibility to adopt future requirements
- Throughput and response times
- Ease of use, resiliency and security
- Integrity, accuracy and currency of information
- Time-to-market
- Cost and time management
- Partnering success
- Skill set of IT staff

Exploiting Business Opportunities with IT
Over the past four decades, IT has reinvented itself at an amazing pace by creating new technologies. Examples include faster, more powerful, and cheaper computers, the creation of enterprise-wide applications to manage the organization’s data and processes, fast and efficient supply-chain management systems, and the exploitation of the internet. The latter has significantly created a new paradigm shift in the business world helping early on adopters to put others off the race. Health care providers have benefited from IT systems which enable access to health records anywhere in the world. Whereas before, physicians needed to read through piles of hand written documentation to find little details for diagnosis purposes, IT systems now can alert physicians immediately to any dangerous drug interactions and allergies. In the first half of the 20th century, companies focused on mass production to reduce costs, today's consumers expect services to be adapted to meet their individual needs.

Responsible Use of IT Resources
According to industry sources, the industry IT operational spending, as a percentage of revenue, has averaged to about 1.7% over the last six years (see Figure 1-6). For the fiscal year of 2009 (ending March 31, 2009), FoMD's IT group's expenditures came in at $970K. All funds expenditures (net of recoveries) came in at $311,741K. Assuming total revenue inflows of $400,000K, this equates to an IT spending of 0.31% of the total expenditure or 0.24% of total revenue.
FoMD must balance its IT operational and capital spending to ensure the right portfolio mix between sustaining operational excellence and position itself for future strategic growth. Not only is the FoMD required to maximize the value of future investments, but also that the current assets are put to the right usage such as annual software licenses matches the demand and applications functionalities are fully leveraged. The following are the major IT resourcing areas:

- Human Resources
- Server Infrastructures
- Desktop Infrastructures
- Software Applications

Appropriate Management of IT-Related Risks
The need to safeguard IT assets and disaster recovery lies at the center of IT governance. Just as organizations need to demonstrate appropriate risk management and control as its finances, because of the increased dependence on computer automation and information, technology risk and information security risks have become prominent in today’s environment. Although the University is not a publicly traded company, and therefore not bound to such public securities legislation such as the Sarbanes-Oxley Act in the US or the Canadian Securities Administrators (CSA) rules, it is still bound to the requirements of the Personal Information Protection Act c.P-6.5 [PIPA], and the Province’s Auditor General. The leakage and tampering of private information due to insufficient reasonable practices would result in direct violation of these
Acts and severe negative impact to the branding of the Faculty, University, and relationship with other close partners such as Alberta Health Services.

According to the IT Governance Institute, enterprise risks should be managed by:
- Ascertaining that there is transparency about the significant risks to the enterprise
- Being aware that the final responsibility for risk management rests with the Dean
- Being conscious that risk mitigation can generate cost-efficiencies
- Considering that a proactive risk management approach can create competitive advantage
- Insisting that risk management be embedded in the operation of the enterprise
- Ascertaining that management has put processes, technology and assurance in place for information security to ensure that:
  - Business transactions can be trusted
  - IT services are usable, can appropriately resist attacks and recover from failures
  - Critical information is withheld from those who should not have access to it

The following diagram (Figure 3) illustrates the key components of information security: Confidentiality, Integrity, and Availability.

![Figure 3 – Information Security Components](http://en.wikipedia.org/wiki/Information_security)
Proposed IT Governance Model

An effective IT Governance Model has to follow the following principles:

- **Simple**
  - Simple to understand and explain
  - Easy to maintain

- **Participative and inclusive**
  - Stakeholders must be part of the decision process
  - All parties concerned should be given the opportunity to provide input and feedback

- **Formal**
  - Roles and responsibilities of the various stakeholders are defined, recognized, and supported
  - Process is transparent

- **Flexible**
  - Accommodate new directions and decision areas

- **Acting as One**
  - Support the alignment with Faculty-wide decisions and directions

**Business/IT alignment**

This is addressed through annual interviews by the CIO with the Dean, Vice Deans, Executive Director, Department Chairs, and other key stakeholders. During the interview, an environmental scan (both business and technology) is performed to recognize any changes to the business using tools such as the SWOT and PEST analysis, Key Performance Indicators (KPI) analysis, etc. Once all of the interviews are conducted, the CIO reviews the information gathered, looks for common themes or patterns across departments, and produces a draft IT Strategic Plan. The IT Strategic Plan has a three year outlook and is updated on an annual basis. The different Information Management Steering Committees (IMSC) then reviews each business case brought forward and the proposed draft IT Strategic Plan, makes any recommendations, and decides on the prioritization of the project portfolio. Once the IT Strategic Plan has been endorsed by the IMSC, it then goes for review and feedback by the corresponding committee/council (i.e. the Faculty Learning Council, Faculty Research Council, or the Faculty’s Research Council). The final draft document is then presented to the IT Executive Council for final executive review and approval. Please refer to Appendix B for a high level Terms of Reference for the different Information Management Steering Committees and their reporting structure.

The Faculty should implement a formal process for project selection and prioritization by using balance scorecards (BSC). The basics idea of a BSC is that the evaluation of an initiative should not be restricted to a traditional financial evaluation or any single evaluation metric, but should be supplemented with
measures concerning a more holistic approach. The following is a sample IT BSC:

<table>
<thead>
<tr>
<th>Business Perspective</th>
<th>Financial Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Promotes community best interest</td>
<td>• Increases business value</td>
</tr>
<tr>
<td>• Promotes student/research growth</td>
<td>• Generates a positive ROI</td>
</tr>
<tr>
<td>• Supports strategic initiatives</td>
<td>• Achieve financial sustainability</td>
</tr>
<tr>
<td>• …</td>
<td>• …</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal Satisfaction</th>
<th>Future Orientation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improves business practices and efficiencies</td>
<td>• Promotes new business capabilities</td>
</tr>
<tr>
<td>• Promotes staff skill set growth</td>
<td>• Positions organizations to maximize opportunities while minimizing threats</td>
</tr>
<tr>
<td>• Promotes staff satisfaction</td>
<td>• …</td>
</tr>
<tr>
<td>• …</td>
<td>• …</td>
</tr>
</tbody>
</table>

Figure 4: Sample Standard IT Balanced Scorecard

**Value Delivery & Performance Measurement**

In order to ensure that proposed projects are justified, the business sponsor is required to put together a business case which describes the Strategic Drivers, Objectives, Risk Assessment, Return-On-Investment (ROI), etc, to be reviewed by the IMSC and executive. Once a project is approved, there are various controls within the project management best practices to ensure that the project has the highest chances of meeting its objectives on budget and on schedule. Some of these controls include the approval of the project charter, business sign-off of the detail requirements specifications, iterations reviews, user acceptance testing, etc. The project also completes with a formal review where the project team evaluates areas where the project went well and where future improvements need to be made. The project team also completes a Project Review Satisfaction Survey with numerical ratings. The survey aggregated result gets incorporated into the final Project Review document.

Furthermore, the Faculty could improve by ensuring that benefits, goals, and objectives, as stated in the business case are harvested, measured, and reported by the business sponsor. This practice falls under the area of Value Management and stewards all investments towards greater success and accountability by ensuring that everything that is invested and done inside the scope of the project will result in the achievement of the desired business benefits. From a Governance perspective, harvesting and measuring benefits form the very core practices of any governance structure.

**Exploit Business Opportunities with IT**

The exploitation of business opportunities with IT are done in partnership between the IT and business departments. The CIO and Manager of IT should review IT publications, attend IT workshops/conferences, and maintain a regular
communication with Central University IT to stay in tune with any technological trends or opportunities for collaboration. The CIO and Manager of IT also meet with partners (AHS, Government Ministries) and key vendor account managers to inform them of the University’s strategic and operational needs and seek inputs.

In partnership, both IT and business needs to continue to scan the environment from a business and technical perspective to spot for new innovative opportunities on a more formal basis through annual reviews and discussion between IT and the Information Management Steering Committees. All brainstormed opportunities could be rated for business and technical feasibility, and the top rated ones could then evaluated further by going through Research & Development pilot project stage. This is where the business sponsor in collaboration with IT could “safely” experiment the concept to determine whether it is prudent to proceed to the business case stage.

Response Use of IT
The CIO will meet with the Executive Director on a biweekly basis to discuss the statuses of key IT initiatives, IT staffs allocations, IT risks, etc. The various IMSCs will meet on a semi-annual basis to review the status of major IT initiatives in its domain. Regular meetings will also occur with the University’s Vice Provost, Information Technology to ensure collaboration with central services is optimized. At the infrastructure level, IT could potentially install special monitoring software for measuring the consumption level of applications and internet. Where software applications are deemed under-used, they can be decommissioned to save licensing cost.

IT Risk Management
Within IT projects, risk management should be conducted as part of the project management best practices. Risks are to be identified and monitored for the duration of the entire projects. Risks are rated based on their level of impact of severance and their probability of occurrence. In the operational contexts, the Faculty’s IT infrastructure is protected from the external Internet by using firewalls which prevents outside penetration into the internal network. Antivirus is updated on an hourly basis, scans and removes all computers (servers, desktops, laptops) for hardware malware which are harmful to the Faculty. Laptops computers and USB keys should be encrypted for added protection to ensure that penetrators cannot access to information stored within laptops in the event that it is lost or stolen. The Faculty should formalize the security risk management plan including an annual external audit process and follow-up to ensure that its information maintain the highest possible confidentiality, integrity, and availability, and meets the requirements of the Auditor General.

The following figure summarizes the proposed IT Governance model for FoMD:
Figure 5 – FoMD Governance Areas
Appendix A – References


“Board Briefing on IT Governance”, IT Governance Institute, 2nd Edition

Blank, Gale, and Henry, Chuck, “IT Governance Overview”, Treasury Board of Canada Secretariat, October 14, 2007

Computer Economics 2009 -

Grembergen, Wim Van, “The Balanced Scorecard and IT Governance”, IT Governance Institute


IT Governance Institute – http://www.itgi.org

IT Audit – http://www.theiia.org/itaudit

“Value Management at the City of Edmonton”, PMI-NAC Dinner Meeting, September 12, 2007
Appendix B – Proposed IT Governing Bodies

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Authority</th>
<th>Membership</th>
</tr>
</thead>
</table>
| **IT Executive Council** | • Provides oversight on behalf of the DEC on topics such as:  
  — The relevance of developments in IT from a business perspective  
  — The alignment of IT with the business direction  
  — The achievement of strategic IT objectives  
  — Risk, return and competitive aspects of IT investments  
  — Progress on major IT projects  
  — The contribution of IT to the business (i.e., delivering the promised business value)  
  — Exposure to IT risks, including compliance risks  
  — Containment of IT risks  
| • Decides the overall level of IT spending and how costs will be allocated  
  • Approves business cases, IT priorities and milestones  
  • Acquires and assigns appropriate resources  
  • Ensures projects meet business requirements  
  • Reports to the DEC | • Exec Director (Chair)  
  • CIO  
  • Vice Dean Reps (2x)  
  • Chairs from each of IM Steering Committee (4x)  
  • VPIT  
  • Freq of Meeting: Semi-annual |
| **IM Steering Committee (Education)** | • Advises the IT Executive Council on IT strategy  
  • Provides input to the IT strategy in preparation its approval  
  • Focuses on current and future strategic IT issues | IMSC (Education)  
  • CIO, Faculty Learning Committee Reps (2x), Office of Education Reps (2x), CADE (2x), Student Reps (2x) |
| **IM Steering Committee** | • Assists the IT Executive Council in the delivery of the IT strategy  
  • Oversees IT service delivery and IT projects | IMSC (Education)  
  • CIO, Faculty Learning Committee Reps (2x), Office of Education Reps (2x), CADE (2x), Student Reps (2x) |
IMSC (Research)  
- CIO, Faculty Research Committee Reps (2x) and Office of Research Reps (2x)
- IMSC (Clinical)  
- CIO, Clinical Reps TBD, AHS Rep (1)
- IMSC (Administration)  
- CIO, Faculty Administrator Committee Reps (3x), Office of the Dean Reps (3x)
- Chairs (Other than CIO. To be elected by the IMSC)  
- Term: 2 years as per Faculty Committees terms
- Freq: Semi-annual

IMSC (Research)  
- CIO, Faculty Research Committee Reps (2x) and Office of Research Reps (2x)
- IMSC (Clinical)  
- CIO, Clinical Reps TBD, AHS Rep (1)
- IMSC (Administration)  
- CIO, Faculty Administrator Committee Reps (3x), Office of the Dean Reps (3x)
- Chairs (Other than CIO. To be elected by the IMSC)  
- Term: 2 years as per Faculty Committees terms
- Freq: Semi-annual

Appendix C – Sample Questions Related IT Governance

- Is it clear what IT is doing?
- How often do IT projects fail to deliver what they promised?
- Are end users satisfied with the quality of the IT service?
- Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?
- Is IT core competencies maintained at a sufficient level to meet required enterprise strategic objectives?
- How well is IT outsourcing agreements being managed?
- What has been the average overrun of IT operational budgets?
- How often and how much do IT projects go over budget?
- How long does it take to make major IT decisions?
- Are the total IT effort and investments transparent?
- How much of the IT effort goes to firefighting rather than enabling business improvements?
- Is the enterprise’s internal IT skill set decreasing? How successfully are skilled IT resources attracted to the organisation?
- What is the percentage of revenue (revenue can be replaced by budget for the public sector) spent on IT compared to the industry average?
• How has IT evolved over the years?
• What is the amount spent on IT compared to the enterprise’s entire profit (profit can be replaced by budget for the public sector)?
• Does IT support the enterprise in complying with regulations and service levels?
• How well do the enterprise and IT align their objectives?
• How critical is IT to sustaining the enterprise? How critical is IT to growing the enterprise?
• What strategic initiatives has executive management taken to manage IT’s criticality relative to maintenance and growth of the enterprise, and are they appropriate?
• What is the organization doing about leveraging its knowledge to increase stakeholder value?
• What IT assets are there and how are they managed?
• Are suitable IT resources, infrastructures and skills available to meet the required enterprise strategic objectives?
• Is the enterprise clear on its position relative to technology: pioneer, early adopter, follower or laggard?
• Is IT participating in overall corporate change-setting and strategic direction? Do IT practices and IT culture support and encourage change within the enterprise?
• Does the enterprise research technology, process and business prospects to set direction for future growth?
• Are enterprise and IT objectives linked and synchronised?
• Is the enterprise clear on its position relative to risks: risk-avoiding or risk-taking?
• Is there an up-to-date inventory of risks relevant to the enterprise?
• What has been done to address these risks?
• Is the board regularly briefed on risks to which the enterprise is exposed?
• Based on these questions, can the enterprise be said to be taking "reasonable" precautions relative to technology risks?