UNIVERSITY OF ALBERTA
FACULTY OF MEDICINE & DENTISTRY

IT GOVERNANCE MODEL - FOMD

DEFINING THE GOVERNANCE STRUCTURE FOR TECHNOLOGY RELATED PROJECTS AND OPERATIONAL ITEMS

Created: November, 2009
Approved: by Dean's Executive Committee
November 16, 2009
Edited: September 2018

IT GOVERNANCE MODEL - FOMD

In September 2009, the Chief Operating Officer and Director of MedIT discussed the need for the Faculty of Medicine & Dentistry (FoMD) to have a proper information technology governance model (IT Governance Model) to facilitate a clearer, more effective and efficient decision process in the IT domain.

This initial document was reviewed and approved by the Dean's Executive Committee (DEC) or equivalent body in 2009 and has become the adopted model adhered to for IT governance within the FoMD.

In the spring of 2015, the FoMD embarked on a strategic planning process which saw the creation of seven core strategic processes:

- **Education** – "The FoMD will be a nationally leading academic entity that provides flexible, innovative and socially accountable programs that are adaptive to learners, clinical prevalence, societal needs and professional mandates."
- **People** – "The FoMD will attract and retain a diverse and talented workforce by proactively supporting and engaging the development of its people throughout their career path."
- **Governance** – "The FoMD will have clear and purposeful structures, mechanisms and processes by which our organization is directed; evaluated and regulated. The organization will allocate resources in a way that ensures alignment with the mission and strategy of both the Faculty and the University of Alberta."
- **Funding** – "The FoMD will develop and ensure a robust, sustainable and transparent funding formula that guarantees long-term viability and success of its research, education and clinical platforms."
- **Partnerships** – "The FoMD aims to strengthen and develop partnerships that are mutually beneficial and value-added, while fulfilling the mission of the Faculty. We also aim to build capacity through our relationships and improve our outreach and community impact."
- **Research** – "The FoMD will create an enriched and collaborative research environment, allowing to shorten the timeline from concept to funding, with the aims of increasing our community impact and globally competitive research for the improvement of health outcomes."
- **Innovation** – "The FoMD will be consolidated as an internationally recognized Faculty, by fostering a culture of innovation that will generate transformational change in research and education in health and wellness."

An IT Governance process supports FoMD's strategic plan by ensuring clear structures are defined and articulated consistently to the FoMD as a whole. Collaboration with internal programs as well as external stakeholders is critically important to help ensure technology is used to its advantage. Funding and fiscal responsibility is also a key component within the IT Governance structure to help ensure the FoMD is funding projects efficiently and effectively, making the best use of public funds. This helps ensure our people also have access to the "right tool at the right time". Technology-driven initiatives governed appropriately will also create a pool of knowledgeable resources that can appropriately be leveraged across the Faculty.

EXECUTIVE SUMMARY

Innovation in technology has become a rapidly evolving reality that can see the deployment of many on-premise and cloud-based tools broadly available for consumer consumption. With this rapid growth, it is more important than ever to ensure there is a clear governance process followed by the FoMD to ensure that strategic goals are met and privacy and security risks are assessed and mitigated.

The FoMD's IT Governance process compliments the FoMD's Information Governance Framework. This framework describes the roles, responsibilities, policies, procedures and standards to support good information management practices. It further supports the administrative, technical and physical safeguards required to protect the FoMD's information assets.

Operating units' purchases and deployment of technical solutions outside of the IT Governance process will erode the benefits of the Information Governance Framework and increase the risk to Faculty data and its information assets. Public reputation and the ongoing ability of FoMD to manage its IT needs will also be impaired.

It is important to ensure that both operating units and technical staff within the FoMD work together to find a solution that supports the needs while maintaining a secure, compliant and productive environment. Duplication of efforts, non-compliance with privacy legislation and sustainability of technical support are also key considerations.

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 they have to determine and understand how to manage Information Technology (IT) strategically.

The right IT Governance Model specifies "*the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT"*, specifically in the following areas:

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

Committee	Responsibility	Authority
Information Management Steering Committee (IMSC)	• Provides oversight on behalf of the DEC on topics such as: — The relevance of developments in IT from an operational perspective — The alignment of IT with the operational 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 operational area (i.e., delivering the promised value) — Exposure to IT risks, including compliance — Containment of IT risks	• Decides the overall level of IT spending and how costs will be allocated • Approves business cases, setting priorities and milestones • Acquires and assigns appropriate resources • Ensures projects continuously meet operational requirements • Faculty-wide policies are sent to DEC for review and approval
IM Steering Committee (Education) IM Steering Committee (Research) IM Steering Committee (Clinical) IM Steering Committee (Administration)	• Advises the IMSC on IT strategy • Provides input to the IT strategy • Focuses on current and future strategic IT issues • Reviews IT business cases brought forward to ensure alignment of operational strategies • Provides prioritization of IT initiatives within the area • Reviews and proposes IT policies and procedures for discussion at IMSC	• Assists the IMSC in the delivery of the IT strategy • Oversees IT service delivery and IT projects • Reports to IMSC
Technology Working Group	• Provides technology guidelines • Provides architecture guidelines • Consults/advises on the selection of technology within standards • Assists in variance review	• Assists the IMSC in the determination, provision and review of IT Standards • Reports to IMSC

Note: IMSC Steering Committee (Administration) has been folded into the Faculty Administrators Committee (FAdC). IMSC Steering Committee (Education) has been folded into the Faculty Learning Committee (FLD). Membership and additional details are found in Appendix B of this document.

WHAT IS IT GOVERNANCE?

According to Peter Weill and Jeanne W. Ross, IT governance is defined as:

"… specifying the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT."[1]

It is driven by the need for closer interaction and involvement with stakeholders by integrating the three "Cs": Cooperation, Consensus and Community. These foundations are in turn based on 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 and how one is held accountable for his or her role. It also defines the structure of the composition of the bodies that make or execute joint decisions, while providing information about how the different parties work together (see Figure 1, below).

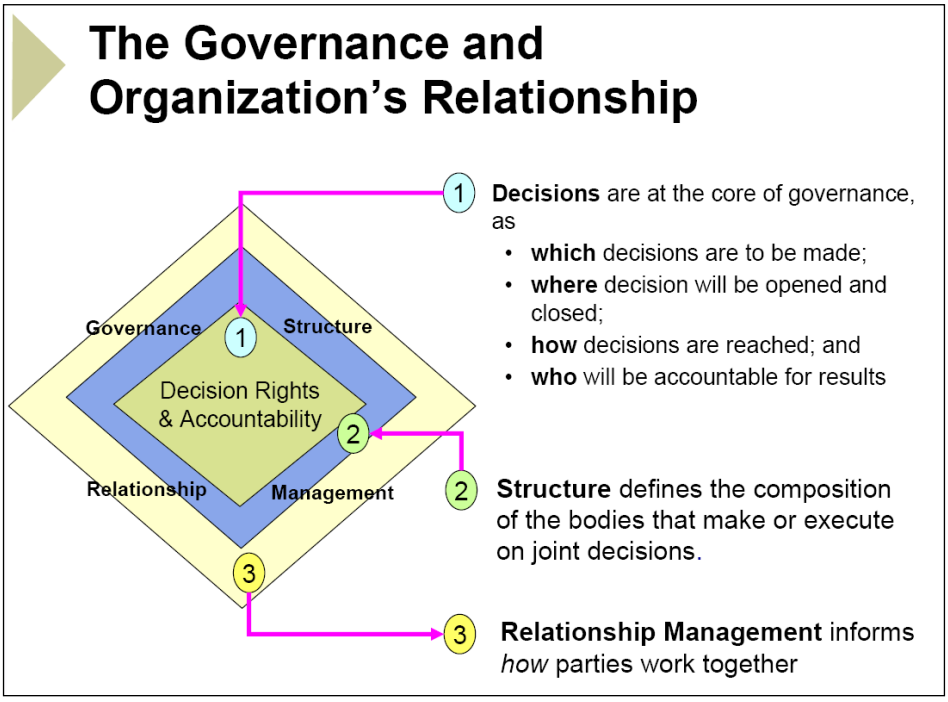


Figure 1 – The Governance and Organization's Relationship.
Source: Treasury Board of Canada – IT Governance Overview

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 operational resumption and disaster recovery planning
- Increased information risks (confidentiality, integrity, accessibility)

[1] Weill, P. and Ross, J.W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA: Harvard Business School Press.

The purpose of IT governance is to direct IT endeavors, 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, operational areas and IT operated in silos where IT did not fully understand operating requirements and vice-versa. Many IT departments were happy to stay in the "technical" world, while departments/units experienced the frustrations of not getting the desired end-product. 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 and emailing services, the best IT departments are now partnering with operational areas by *adopting a more "strategic" role with the potential not only to support chosen strategies, but also to shape new 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 operational areas 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:

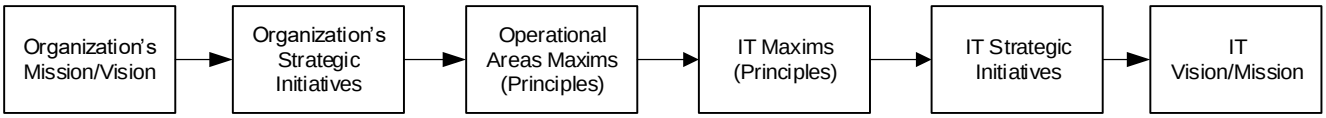


Figure 2

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, within-budget and at an appropriate quality matching the operational 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 meet the mission statement of serving the public through excellence in medical and health professions' education, research and patient care.

According to the IT Governance Institute (ITGI), in order to achieve the realization of the promised benefits, both IT and the operational area's need to define the following relative to IT deliverables:

- Fit for purpose, meeting 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 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 internet has most significantly contributed to a paradigm, whereby organizations must either adapt quickly to online advances, or be left behind.

RESPONSIBLE USE OF IT RESOURCES

FoMD must balance its IT operational and capital spending to ensure the right portfolio mix between sustaining operational excellence and positioning itself for future strategic growth. Not only is the FoMD required to maximize the value of future investments, but also to ensure that its current assets are put to the right usage (e.g. ensuring annual software licenses match the demand, and that application functionalities are fully leveraged). Ensuring IT dollars are spent in a way that provides the best value to the organization is an important aspect of ensuring technology is used appropriately and in a cost-efficient manner. Following the FoMD IT Governance Model will ensure that dollars are not spent purchasing similar services from multiple vendors with multiple support models. Aligning IT budget dollars to have them efficiently spent across the faculty as a whole will see a decrease in cost per user, as well as ensuring alignment with the strategic plans of the faculty. 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. Due to the increased dependence of organizations on computer automation and information, technology risk and information security risks have become prominent in today's environment. Although the University is not bound by such public securities legislation such as the *Sarbanes-Oxley Act* in the United States or the Canadian Securities Administrators (CSA) rules, it is still bound to the requirements of the Alberta *Freedom of Information and Protection of Privacy Act* and *Health Information Act*, and Alberta's Auditor General. These statutes impose a requirement on public bodies or individuals in the custody or control of personal information to establish reasonable safeguards against the inappropriate collection, use or disclosure of that personal information. Proper IT governance is critical to establishing such safeguards, and a proper IT Governance Model must ensure that these safeguards are developed, implemented and integrated across the enterprise and are considered in each IT decision-making process. Failure of the FoMD to establish these safeguards can result in the authorized access to or loss of personal information, which may then put the organization in contravention of provincial privacy statutes and cause direct, severe harm to the reputation and public trust in the University of Alberta (University) as a whole, and damage existing relationships with close partners such as Alberta Health Services and Alberta Health.

Current news cycles highlight the significant risk to organizations with respect to privacy and security breaches. This includes network breaches, malware attacks, and widespread infections of ransomware. As a result, security and privacy spending in the industry at large has seen a significant increase in dollars spent to combat the heightened risk in these areas.

New processes have been identified within the University and the FoMD in order to address privacy and security risks. The University has both privacy and security checklists and processes in place to ensure that any project or initiative is reviewed by experts in these fields to identify and address any potential risks to the organization. Specifically, the FoMD has an IT Privacy and Compliance team that reviews FoMD IT business cases or briefs in order to provide analyses and recommendations. These recommendations are then shared with the University's Central Information Services and Technology (IST) group in an effort to help clarify the analysis, and help alleviate the waiting time of these initiatives.

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:
  - Operational 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.

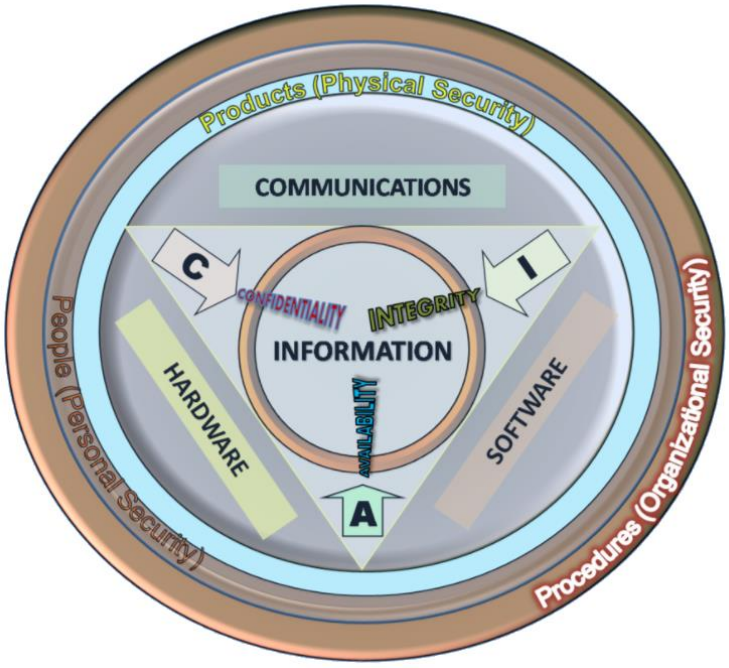


Figure 3 – Information Security Components
Source: http://en.wikipedia.org/wiki/Information_security

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

ORGANIZATIONAL AREAS/IT ALIGNMENT

This is addressed through annual interviews by the Director of MedIT with the Dean, Vice Deans, Chief Operating Officer, Department Chairs, and other key stakeholders. During the interview, an environmental scan (both operational and technology focused) is performed to recognize any changes to the operations using tools such as the Strength Weakness Opportunity and Threats (SWOT) and Political Economic Social and Technological (PEST) analyses, Key Performance Indicators (KPI) analysis, etc. Once all of the interviews are conducted, the Director 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 IMSC subcommittees then review each business case brought forward and the proposed draft IT Strategic Plan, makes any recommendations, and decides on the prioritization of the project portfolio.

This process can also be initiated by operational areas identifying a proposed need, and moving the briefing note or business case through the appropriate IMSC subcommittee.

Once the IT Strategic Plan has been endorsed by the IMSC, it then goes for review and feedback by the corresponding committee (i.e. the Faculty Learning Committee, Faculty Research Committee, Faculty Affairs Committee, or the Faculty Administrators Committee). The final draft document is then presented to the Dean's Executive Committee (DEC) for final executive review and approval. Please refer to Appendix B for a high level Terms of Reference for the different IMSC subcommittees and their reporting structure.

The faculty should implement a formal process for project selection and prioritization by using balance scorecards (BSCs). 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:

Operational Area Perspective	**Financial Perspective**
• Promotes community best interest • Promotes student/research growth • Supports strategic initiatives • …	• Increases value • Generates a positive ROI • Achieve financial sustainability • …
Internal Satisfaction	**Future Orientation**
• Improves practices and efficiencies • Promotes staff skill set growth • Promotes staff satisfaction • …	• Promotes new capabilities • Positions organizations to maximize opportunities while minimizing threats • …

Figure 4: Sample Standard IT Balanced Scorecard

VALUE DELIVERY AND PERFORMANCE MEASUREMENT

In order to ensure that proposed projects are justified, the operational area sponsor is required to put together a briefing note or 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, appropriate sign-off of the detailed 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, our process could be improved by ensuring that benefits, goals, and objectives, as stated in each business case are leveraged, measured, and reported by the operational area sponsor at the project's close. 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 benefits.

EXPLOIT OPPORTUNITIES WITH IT

The exploitation of opportunities with IT are done in partnership between the IT and operational areas. The Director of MedIT and Manager of MedIT should remain current with industry best practices and maintain regular contact with University's Central IST group to identify opportunities for collaboration. The Director and Manager of MedIT should also meet with partners (e.g. AHS, Government Ministries) and key vendor account managers to inform them of the University's strategic and operational needs and seek their inputs.

In partnership, both IT and operational areas need to continue to scan the environment from an operational and technical perspective to identify new innovative opportunities on a more formal basis, through annual operating reviews and discussions between IT and the IMSC subcommittees. All brainstormed opportunities should be rated for operational and technical feasibility, and the top rated ones could then be evaluated further by going through a development pilot project stage. The operating area sponsor in collaboration with IT could "safely" pilot the concept to determine feasibility and a fully costed business case and implementation plan.

RESPONSIBLE USE OF IT

The Director of MedIT will meet with the Chief Operating Officer on a biweekly basis to discuss the status of key IT initiatives, IT staff allocations, IT risks, etc. The various IMSC subcommittees will meet on a monthly basis to review the status of major IT initiatives in their respective domains. Regular meetings will also occur with the University's Vice-Provost & AVP Information Technology, to ensure collaboration with the University's Central IST group is optimized. At the infrastructure level, IT could measure application consumption levels to feed into licensing renewal decisions.

There should be consistent and transparent governance processes across the Faculty with respect to IT initiatives and oversight. An inventory of technical resources and their compliance with the University and Faculty governance model is required.

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 project. Risks are rated based on their level of impact of severance and their probability of occurrence. In the operational context, the faculty's IT infrastructure is protected from the external Internet by using firewalls antivirus, encryption, etc. The security risk management plan would include an annual external audit process and follow-up to ensure that its information maintains the highest possible confidentiality, integrity and availability, and meets the requirements of the Alberta Auditor General.

The following figure (Figure 5) summarizes the IT Governance model for FoMD:

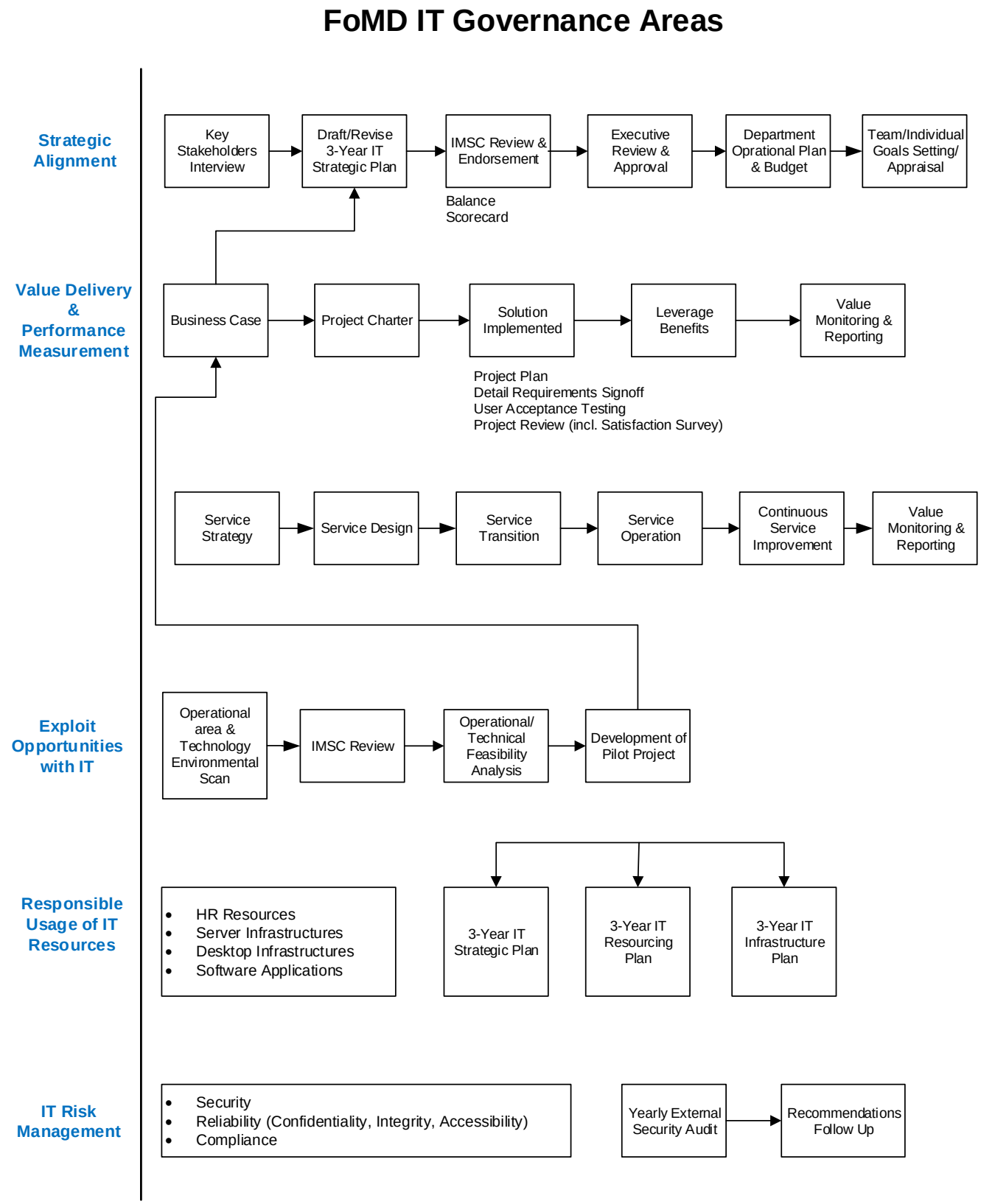


Figure 5: FoMD IT Governance Areas

APPENDIX A – REFERENCES

"20 Questions Directors Should Ask about IT", CICA, April 2004.

"20 Questions Directors should Ask About IT, Second Edition", CPA Canada, 2012.

"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 - http://www.computereconomics.com/temp/ISS2009ch01execsum418392.pdf

Grembergen, Wim Van, "The Balanced Scorecard and IT Governance", IT Governance Institute

"Information Security Governance: Guidance for Boards of Directors and Executive Management", 2nd Edition

IT Governance Institute (ITGI) – http://www.itgi.org

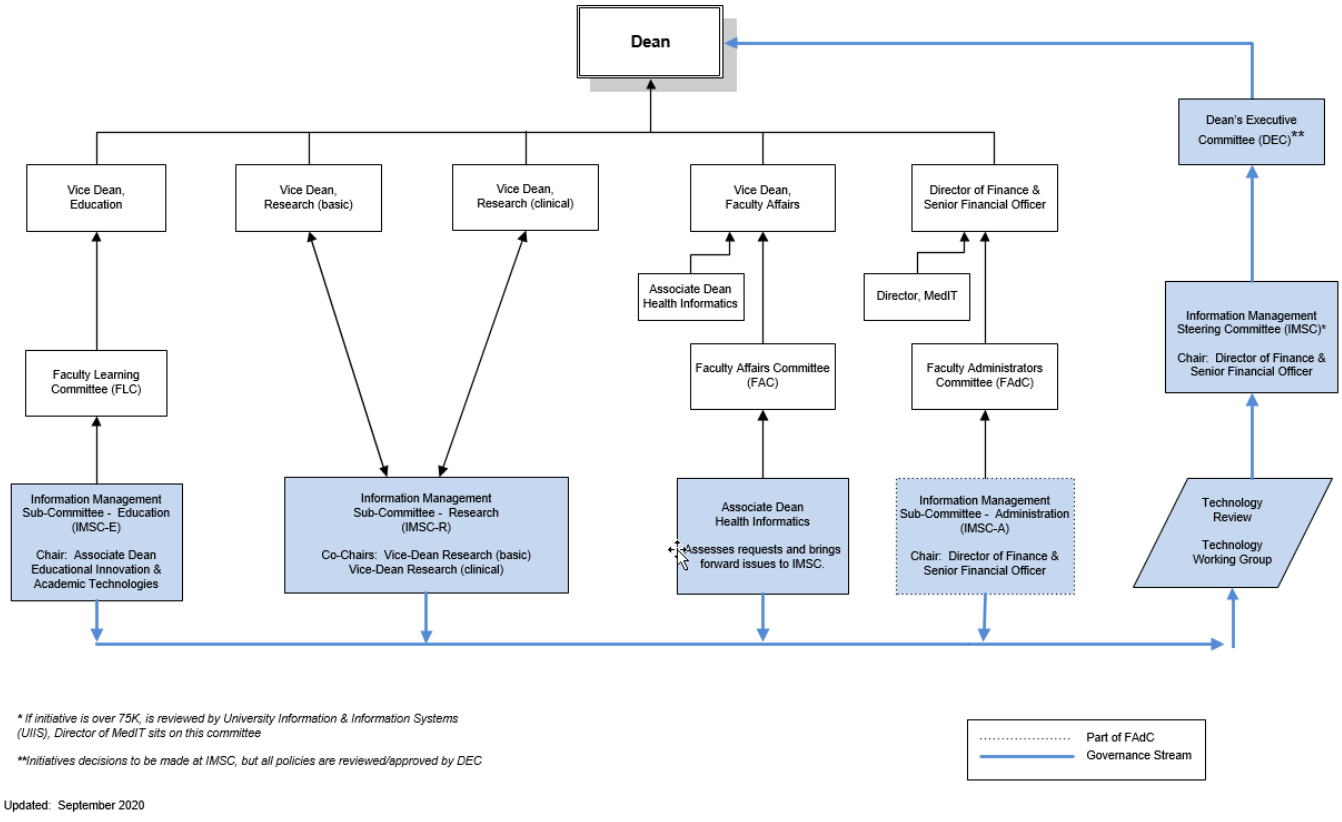
IT Audit – http://www.theiia.org/itaudit

"Value Management at the City of Edmonton", PMI-NAC Dinner Meeting, September 12, 2007

"IT Governance: How Top Performers Manage IT Decision Rights for Superior Results", Weill, P. and Ross, J.W. (2004).

"Be Afraid Of Your Shadow: What is 'Shadow IT' and How to Reduce it", GlobalSCAPE Whitepaper (https://www.globalscape.com/resources/whitepapers/shadow-it-guide)

APPENDIX B – IT GOVERNING BODIES



Committee	Responsibility	Authority	Membership
Information Management Steering Committee (IMSC)	• Provides oversight on behalf of the DEC on topics such as: — The relevance of developments in IT from an operational perspective — The alignment of IT with the operational area's 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 operational area (i.e., delivering the promised value) — Exposure to IT risks, including compliance — Containment of IT risks	• Decides the overall level of IT spending and how costs will be allocated • Approves business cases, setting priorities and milestones • Acquires and assigns appropriate resources • Ensures projects continuously meet requirements • Faculty-wide policies are sent to DEC for review and approval	• Director of Finance & Senior Financial Officer (Chair) • Director MedIT • Vice Dean Reps (4x) • Chairs from each of IM Steering Committee (2x) <u>*Guests:</u> • VPIT • CISO • Manager, MedIT *Central Guests invited to attend External IMSC meetings.*
IM Steering Committee (Education) IM Steering Committee (Research) IM Steering Committee (Clinical) IM Steering Committee (Administration)	• Advises the IMSC 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 operational strategies • Provides prioritization of IT initiatives within the area • Reviews and proposes IT policies and procedures	• Assists the IMSC in the delivery of the IT strategy • Oversees IT service delivery and IT projects • Reports to IMSC	<u>IMSC (Education)</u> • Academic Lead/Chair, Director MedIT, Folded into Faculty Learning <u>IMSC (Research)</u> • Academic Lead/Chair, Director MedIT, Faculty Research Committee Reps (2x) and Office of Research Reps (2x) <u>IMSC (Clinical)</u> • Academic Lead/Chair, Director MedIT, Clinical Reps TBD, AHS

Committee	Responsibility	Authority	Membership
			Rep (1) <u>IMSC (Administration)*</u> • Director of Finance & Senior Financial Officer, Folded into FAdC • Frequency: Monthly
Technology Working Group	• Provide technology guidelines • Provide architecture guidelines Consult/advise on the selection of technology within standards • Assist in variance review	• Assists the IMSC in the determination, provision, and review of IT Standards • Reports to IMSC	• Director MedIT (Chair) • IT Manager • Key advisors as required (IT, audit, legal, finance) Technical staff as required (Systems Analyst, Health Information Privacy Advisor, Security Analysts, etc.) • Frequency: Initiative dependent

Note: IMSC Admin folded into FAdC.

- Chairs to be elected by the IMSC
- Term: 2 years as per Faculty Committees terms

APPENDIX C – IMSC TERMS OF REFERENCE

Chair(s)	Director of Finance & Senior Financial Officer, Office of the Dean
Accountability	The Information Management Steering Committee (IMSC) is directly accountable to Dean's Executive Committee. See organization structure below.
Purpose	The purpose of the Information Management Steering Committee (IMSC) is to provide leadership and oversight in the faculty's overall Information Technology/Information Management strategy. This includes ensuring the alignment of IT/IM investments with faculty's strategies, oversight of value delivery and performance measurement, exploit new opportunities using IT/IM, responsible usage of current IT/IM resources, and overall IT/IM risk management.
Function	<u>Strategic Alignment</u> • Provide strategy direction and the alignment of IT/IM initiatives within the faculty and the business. • Verify strategy compliance (e.g., achievement of strategic goals and objectives). • Provide high-level direction (e.g., policies) for funding, sourcing, partnering. • Oversee the aggregate funding of IT/IM at the enterprise level. • Align with central university initiatives whenever possible. • Seek collaborations, which align with faculty directions. • Reviewing proposals submitted by sub-committees and provide recommendations to Dean's Executive Committee. <u>Value Delivery</u> • Confirm that the IT/IM architecture is designed to drive maximum business value from IT/IM. • Review post project reviews and evaluations. <u>Delivery and Performance Measurement</u> • Benchmark against other medical schools and industry best practices. • Review the measurement of IT/IM performance and the contribution of IT/IM to the business (i.e. delivering the promised business value). <u>Exploit new opportunities using</u> IT/IM • Verify that the IT/IM portfolio has the right balance between innovations and operations. • Ensure that the Faculty has established key IT/IM strategic partnerships for new opportunities. <u>Risk Management</u> • Ascertain that management has resources in place to ensure proper management of IT/IM risks. • Take into account risk aspects of IT/IM investments. • Confirm that critical risks have been managed.

Membership	• Director of Finance & Senior Financial Officer, FOMD • Vice Dean, Education • Vice Dean, Faculty Affairs • Vice Dean Research (basic) • Vice Dean Research (clinical) • Director, MedIT • IMSC Education Chair • IMSC Clinical Chair Guests: • Vice-Provost and Associate Vice-President Information Technology • Chief Information Security Officer, UA • Manager, MedIT Recording Secretary: • Executive Assistant to the Director of Finance & Senior Financial Officer Membership Term: Leadership appointment or 2 years.
Subcommittees:	(see IM Governance Structure attached) 1. Information Management Sub-Committee (Education) 2. Information Management Sub-Committee (Research) 3. Information Management Sub-Committee (Clinical) 4. Information Management Sub-Committee (Administration; FAdC) (Steering Committees Terms of Reference attached)
Meeting Frequency	Quarterly or as deemed necessary by the chair.
Decision Making	A quorum will be the Chair (or a designated alternate) and 50% of members.
Agenda and Minutes	Agenda will be circulated to the IM Steering Committee in advance of the meeting. Minutes will be circulated no later than two weeks after the meeting.

APPENDIX D – SAMPLE QUESTIONS RELATED TO IT GOVERNANCE

- Is it clear what technology initiatives are being undertaken?
- 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?
- Are IT core competencies maintained at a sufficient level to meet required enterprise strategic objectives?
- How well are 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 operational improvements?
- Is the enterprise's internal IT skill set decreasing? How successfully are skilled IT resources attracted to the organization?
- What is the percentage of revenue (revenue can be replaced by budget for the public sector) spent on IT compared to the industry average?
- 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 operational prospects to set direction for future growth?
- Are enterprise and IT objectives linked and synchronized?
- 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?
- Is there appropriate accountability for identifying, acquiring and deploying information assets and capabilities to meet the needs of the organization?
- How is performance of the organization's information assets & capabilities measured, monitored and reported?
- What measures are being taken to enhance, preserve and safeguard the integrity and reliability of the organization's information assets, commensurate with their importance and value?
- Are there sufficient appropriate IT resource and competencies including succession plans for key IT personnel?
- Based on these questions, can the enterprise be said to be taking "reasonable" precautions relative to technology risks?

Asking these questions across the faculty to the technical teams will help ensure consistency and help manage and mitigate risk to the FoMD. A few examples of technical groups within the faculty currently are listed below: