UNIVERSITY OF TORONTO

THE GOVERNING COUNCIL

REPORT NUMBER 104 OF THE AUDIT COMMITTEE

October 10, 2012

To the Business Board,
University of Toronto.

Your Committee reports that it met on Wednesday, October 10, 2012 at 4:00 p.m. in the Board Room, Simcoe Hall, with the following members present:

Ms Paulette L. Kennedy (In the Chair)
Mr. Jeff Collins
Ms. Kathryn A. Jenkins
Mr. Peter Robinson
Ms Penny Somerville
Mr. Chris Thatcher

Mr. Mark Britt, Director, Internal Audit Department *
Ms Sheila Brown, Chief Financial Officer **
Mr. Louis R. Charpentier, Secretary of the Governing Council **
Prof. Scott Mabury, Vice-President, University Operations **

Ms. Sheree Drummond, Secretary

Regrets:
Mr. Howard Shearer

In Attendance:

Mr. William Ballios, Executive Director, Research Compliance & Risk Management, Office of the Vice-President, Research & Innovation +
Ms. Stephanie Chung, Ernst & Young **
Mr. Robert Cook, Chief Information Officer ++
Mr. Martin Loeffler, Director, Information Security ++
Mr. Michael Moore, Audit, Manager, Internal Audit **
Ms. Titi Oridota, Audit, Supervisor, Internal Audit **
Mr. Daniel Ottini, Audit Manager, Internal Audit **
Mr. Pierre G. Piché, Controller and Director of Financial Services**
Ms. Martha J. Tory, Ernst & Young **
Ms. Gosia Urbanski, Senior Auditor, Internal Audit **
Mr. Peter Wong, Assistant Auditor, Internal Audit **
Prof. Paul Young, Vice-President, Research and Innovation +

\+ Present for items 1 - 5 (a.)
++ Present for items 1 - 5 (b.)
* Absented himself for item 8 (a)
** Absented themselves for items 8 (a) 9

ALL ITEMS ARE REPORTED TO THE BUSINESS BOARD FOR INFORMATION.

1. Introductions and Chair's Remarks

The Chair welcomed members and guests to the meeting and asked members to briefly introduce themselves.

The Chair noted that the Committee meets in closed session and that meeting materials are confidential.

2. Report of the Previous Meeting

Report Number 103 (June 13, 2012) was approved.

3. Business Arising from the Minutes

The Chair reported that at the June 13, 2012 meeting it was decided that at the Committee's first meeting for 2012-13 the Committee would deal with three matters that had arisen at the previous meeting in the discussion of the Risk-Assessment Profile. The Committee would receive:

- A further risk assessment in the area of information technology on: risk identification, measurement and mitigation with reference to a risk control framework such as COBIT [originally an acronym for Control Objectives for Information and Related Technologies]; a discussion of the nature of information-technology spending (central versus distributed); and differences in control and oversight between those two levels;
- A review of risk identification and mitigation with respect to research activities; and
- A report from Internal Audit on its activities in relation to the risk-mitigation factors identified in management's Risk-Assessment Profile.

She noted that these three items were on the agenda - items 5 (a.), (b.) and (c.).

4. Audit Committee

a. Terms of Reference: Annual Review

The Chair reminded members that the terms of reference of Executive Committee have been revised to provide for "a comprehensive annual report on enterprise risk management following initial review by the Audit Committee." She noted that this will be taking place for the first time at the October 19, 2012 Executive Committee meeting.

b. Overview of the academic and administrative structure of the University (Professor Scott Mabury, Vice-President, University Operations and Mr. Mark Britt, Director, Internal Audit)

Professor Mabury provided an overview of the academic and administrative structure of the University. He began by noting that at the top of the organizational structure is a faculty member

and a student. In his view this is where the mission of the institution plays out. He pointed out that all faculty and students exist within a department. Referring to Part A of *Facts and Figures 2011*, he briefly outlined the faculty and departmental structure of the University, noting that at the University of Toronto Faculties are also known as divisions and that there are multi-department faculties (e.g., Arts & Science) as well as single department faculties (e.g., Social Work). He explained that all faculty members have an affiliation to a department or to an extra-departmental unit: A (EDU:A). While there is a great diversity among departments in terms of their organizational structures, all departments have human resources functions, business functions, teaching at the undergraduate and/or graduate level, and research activity. Some departments also have separate self-funded sub-units (e.g., machine shops). Under the University's budget model revenues and expenses are attributed at the Faculty level. Where possible, Deans download the principles of the budget model to their respective departments.

Professor Mabury also briefly outlined the structure of the senior administration highlighting the following:

- The six Vice-Presidents and the Chief Financial Officer report to the President.
- The Vice-President and Provost is the chief academic officer as well as the chief budget officer. The Vice-President, University Operations has a dotted reporting line to the Provost with regard to the budget.

Professor Mabury closed by commenting that this whole structure is meant to support the primary function of the institution, namely teaching and research.

Mr. Mark Britt then spoke to the role of Internal Audit (IA) within this highly decentralized environment. He noted that as a department of seven auditors it was critical that its limited resources were invested appropriately. IA identifies auditable units (defined as budgetary areas that have autonomy and authority to make budget decisions). These units can be academic, shared services or ancillary services. IA then identifies manageable pieces within these areas and looks into the nature of the risks and accountabilities within the respective unit with the goal of developing a risk profile. IA also meets with each of the senior executives to discuss areas that might benefit from an audit. On occasion, requests for an audit are received from a division.

Mr. Britt also spoke to continuous audit, noting that it is high impact but resource intensive. This looks at transactional activities, building awareness of central monitoring. He noted that this is one of the value-added services. He pointed out that IA does not do extensive auditing of local systems.

Mr. Britt noted that IA also provides assistance to Ernst & Young which saves the University some money and brings efficiencies to the audit. He concluded by observing that IA has a broad mandate and that when items are on the audit plan this reflects a strategic and tactical approach.

The Chair asked about the process for deciding where an audit will take place and whether it is accurate to say that IA is not in any one place frequently. Mr. Britt replied that once IA has

identified areas they validate that they are focusing on the areas of significant risk. He noted that some areas are considered more or less risky, pointing out that segregation of duties become far more important in areas with few people but broad suite of activities.

c. Calendar of Business, 2012-13

The Chair invited members to make any suggestions for items of business for the Committee. No suggestions were made. She noted that the calendar is publicly available on the web and that it is updated on a weekly basis.

5. Risk Assessment

a. Research Activities

The Chair invited Professor Paul Young, Vice-President, Research and Innovation to speak to efforts at risk mitigation in the portfolio. Professor Young introduced Mr. William (Bill) Ballios who had recently joined the University in the role of Executive Director, Research Oversight and Compliance in the Office of the Vice-President, Research and Innovation.

Professor Young addressed the following matters:

- Key risk areas – financial and reputational risk of funding suspension or application disqualification; financial risk of decrease in research funding; procurement activities; financial and reputational risk associated with Research Misconduct; decentralized research structure.
- Mitigating Controls and Risk Management Practices – Update
    - Project "RAISE":
        - Has delivered on (a.) risk management/compliance to third party agreements through automation of human and animal ethics protocols, and (b.) redirecting posting from closed/frozen restricted research funds. The impact of this has been the protection of Tri-Council Funding by reducing the risk of non-compliant activities.
        - Has improved accuracy/completeness/timelines of financial transactions through the (a.) monitoring controls and automation of close-out activities; (b.) automation of indirect cost revenue calculations and postings; and (c.) automation of revenue postings. The impact of this has been an increase in resource capacity through productivity; reduced risk of negative financial exposure through greater transparency and timely corrective action; and reduced risk of project deficits.
        - Work in process regarding transparency/auditability/efficiency: online research application submissions; online human protocol submissions and review; and online protocol submissions and review. The impact of these will be improved workflow efficiency as well as more transparent and auditable processes.

        - Work also in process regarding enhanced system embedded controls resulting in improved accountability.
- Mitigating Controls and Risk Management Practices going forward:
    - New Executive Director Research Oversight and Compliance, reporting to the Vice-President, Research and Innovation, joined the Office in September. His mandate is to move to build an integrated foundation in Enterprise Risk Management process elements in the research areas. Specifically this will involve: establishing context for managing risk; identifying risk; assessing risk; monitoring and reporting of risk; and consulting and communicating with stakeholders.
    - 2013-14 Budget scaling exercise is underway to identify resource gaps for effective centralized support.
    - Plans for revisions to Research Administration policies.

Mr. Ballios also spoke briefly to Project RAISE. He commented on the problem of managing the sheer volume of transactions and indicated that they are now giving those involved with research the tools to start to effectively manage the data in a more transparent and meaningful way. In addition, controls will be embedded in the online application processes. His view is that with the deployment of these tools the Faculties/Depts will see the biggest impact in terms of minimizing institutional risk and improved service.

The Chair thanked Professor Young and Mr. Ballios for their presentation to the Committee. She indicated that it would be helpful if they would come back and update the Committee on their progress on the portfolio's ERM initiatives.

b. Information Technology

The Chair invited Mr. Robert Cook, Chief Information Officer to provide the Committee with an update on efforts at risk mitigation in the portfolio. Mr. Cook introduced Mr. Martin Loeffler, Director, Information Security & Enterprise Architecture.

Mr. Cook thanked the Committee for the opportunity to continue the conversation on IT risk and risk management.

The presentation addressed five areas: I+TS Service Catalog; Governance, Risk and Compliance; Alignment of I+TS with Mission; COBIT; and IT Spend.

- I+TS Service Catalog: A comprehensive project across I+TS was underway to provide an on-line resource that would list the services and systems available through central IT services. These include: Blackboard; E-mail (Microsoft Live@EDU); Student Information Systems (ROSI and NGSIS); Student Services systems; Human Resources Information Services (HRIS) including UTORecruit; Development Information System (DIS) Infrastructure; Backup and Recovery; Voice services; Information Security services; Sign-in and identity services; IT services planning and assessment; IT Project Management Office; Enterprise Architecture services. Each comprises a number of

specific systems and services, and therefore it is necessary to identify common and unique risks and engage in solution-specific risk management. When the resource becomes available it will be possible to access information concerning risk.
    - Example of UTmail+ service: Success is largely attributed to the preparatory work done to identify common risks (id and authentication) and unique risks (e.g., outsourced nature, institutionally related data hosted externally). I+TS addressed these in the contract and in the service level agreement, as well as with internal security arrangements. In addition, there was a lot of communication with, and education of, the community.
- Governance, Risk, and Compliance: I+TS takes a holistic approach to articulating risk. Assets are identified as physical, logical, virtual or personnel. Contexts are identified as storage, transport, use, administration and deletion. Within each context, strategies are deployed to achieve the goals of confidentiality, integrity, availability, and accountability. These strategies are identification, authentication, authorization (IAA), isolation, continuity and reporting (ICR), which are each tied to a specific technology or group of technologies.
    - Threat Risk Assessment (TRA) and the Privacy Impact Assessment (PIA) process: TRA involves looking at threats to assets and identifying vulnerabilities and mitigation strategies. A recent example was UTMail+ and the issue of how to maintain a level of control in light of the fact that the service was being outsourced. In the end it was decided that the University would retain the identification and authentication component. PIA is a more targeted evaluation and requires drilling down to how the information is used, with a focus on Personally Identifiable Information (PII). These processes bring in an understanding of our governance regulations and processes – it is not just the risk of a hack but also the risk of failure in compliance.
    - IT Middle Tables: Process and Technology Committee, made up of managers (half from the technology side and half from the business side) from across the divisions, identifies opportunities and reviews proposals for their business and technical viability. Priorities and Accountability Committee confirms institutional alignment, recommends priorities and monitors performance of centralized initiatives.
- Alignment of I+TS with Mission: Importance of reporting to an academic leader. Academic oversight is closely aligned with the Vice-President and Provost. Participates in the university budgeting process that puts all initiatives, academic and administrative, in competition for funds. IT is not apart from but is subject to the same considerations that are brought to bear on the academic initiatives. Some examples of major business-aligned projects completed: new Data Centre; UTMail+; Learning Portal (Blackboard) upgrade; physical network renewal. Some examples of major business-aligned projects in progress: UShop; wireless network renewal; DIS renewal; Security Event Information Management (SEIM).
- COBIT: I+TS does not use COBIT, however, by virtue of the way I+TS is situated within the organization, and by the activities I+TS undertakes to engage the business, I+TS

empowers the business process owners to have full control over the business processes within I+TS.

- I+TS Risk Management Partnership: I+TS created the conditions for successful Risk Management at the periphery of the divisions.
- Total IT Spend: In 2011 $85.6 million (587 FTE staff, salaries $56.9 million) - $26.2 million in CIO, $54.2 million in divisions, and $19.6 million in other shared services divisions. This has implications for risk management.

The following comments were made by members:

The Chair remarked that a major challenge of the Committee was to understand whether the risk in the distributed environment largely exists unmitigated.

In relation to risk management in the divisions, a member asked whether a division understands that the accountability is fully theirs. Mr. Cook replied that it was difficult to know and that the Office of the CIO does not have visibility into all the projects as there is no formal requirement to bring them to the attention of the centre.

The Chair thanked Mr. Cook and Mr. Loeffler for their presentation.

c. Internal Audit

The Chair invited Mr. Mark Britt, Director, Internal Audit, to review the *Special Report: Internal Audit Effort and Risk Management*. Mr. Britt indicated that the objective of the *Report* is to identify the alignment of the internal audit effort with the risks and risk mitigation activities noted in the University's Risk Assessment Profile Report for 2012. Specifically, the Report provides the requested information to assist the Audit Committee with:

1. Evaluating the internal audit allocation of resources to the risks noted in the Profile Report and gain assurance that it is aligned with the identified significant risks;
2. Gaining an understanding of those risk management activities and audit areas that internal audit selects for inclusion in internal audit plans;
3. Identifying gaps in internal audit assessment or governance oversight of significant risks or risks not otherwise identified as assessed;
4. Providing input into future audit plans and update to the University's Risk Assessment Profile Report update.

He explained that Internal Audit activities identified in the Report have been classified into three levels: Level 1 – Recurring as part of the annual Audit Plan; Level 2 – periodic or infrequent audits; Level 3 – no audit activities to date.

As an example, he noted that past reports issued by Internal Audit have confirmed a number of the risk and internal control issues that Professor Young addressed in his presentation and that consequently a number of Audit Plans have been directed at these risks over a period of time

now. He indicated that audits of the research financial reporting processes fed into the creation of ROCCO as well as the subsequent RAISE project.

Mr. Britt contrasted internal audit's focus on audits of research services against the lower frequency of audits of the Human Resources risk mitigation activities noted in the Risk Profile Report. He indicated that there is no extensive involvement of Internal Audit in this area as other bodies have oversight. The Chair noted that the Vice-President, Human Resources & Equity reports to the Business Board on a wide variety of these matters and that this is not an area of oversight of the Audit Committee.

Mr. Britt closed by saying that the Report serves a number of purposes as previously stated and will be updated and provided to the Committee periodically for continuous assessment of the alignment of internal audit activities with significant risks; identification of any gaps in risk mitigation of significant risks and assisting with developing future audit plans. He noted that it would likely assist the Committee in deciding what information it requires to gain assurance about the effectiveness of the University's risk management activities and processes

6. Report of the Administrative Assessors

Professor Mabury spoke briefly to some examples of risk that the University faced and how the administration was dealing with them.

7. Date of Next Meeting

The Chair advised that the date of the next meeting is Tuesday, December 4, 2012.

8. Other Business

a. Discussion of External Audit Services

With the unanimous consent of members the Committee moved *in camera* to discuss this item. Members of the administration, the Secretariat (with the exception of the Committee Secretary) and the external auditors absented themselves.

THE COMMITTEE MOVED IN CAMERA.

9. Internal Auditor

Members of the administration, the Secretariat (with the exception of the Committee Secretary) and the external auditors absented themselves. The Committee met privately with the Director of the Internal Audit Department. Mr. Britt was invited, as provided in the terms of reference, to report on "any problems encountered, any failure to provide appropriate information or any restrictions on internal audit work, the general cooperation received in the performance of internal audit duties, and any matters requiring discussion arising from the auditor's findings".

Following his report, Mr. Britt absented himself from the meeting. Members discussed the matter of external audit services.

THE COMMITTEE CONCLUDED ITS *IN CAMERA* SESSION.

The meeting adjourned at 7:48 p.m.

Secretary Chair

November 1, 2012