UNIVERSITY OF TORONTO

THE GOVERNING COUNCIL

**REPORT NUMBER 102 OF THE AUDIT COMMITTEE**

**May 9, 2012**

To the Business Board,
University of Toronto.

Your Committee reports that it met on Wednesday, May 9, 2012 at 4:00 p.m. in the Board Room, Simcoe Hall, with the following members present:

Ms Paulette L. Kennedy (In the Chair)
Ms Penny Somerville
Mr. Chris Thatcher

Professor , Scott Mabury
Vice-President, University Operations

Mr. Mark Britt, Director, Internal Audit
Mr. Louis R. Charpentier, Secretary of the Governing Council

Mr. Neil Dobbs, Secretary

Regrets:

Ms Sheila Brown
Mr. J. Mark Gardhouse
Mr. Steve (Suresh) K. Gupta
Mr. W. John Switzer

In Attendance:

Ms Stephanie Chung, Ernst & Young
Mr. Robert Cook, Chief Information Officer
Mr. Martin Loeffler, Director, Information Security and Enterprise Architecture, Information + Technology Services
Mr. Daniel Ottini, Audit Manager, Internal Audit Department
Mr. Pierre Piché, Controller and Director of Financial Services
Ms Martha Tory, Ernst & Young

ALL ITEMS ARE REPORTED TO THE BUSINESS BOARD FOR INFORMATION.

## 1. Report of the Previous Meeting

Report Number 101 (March 21, 2012) was approved.

## 2. Audited Financial Statements for the Year ended April 30, 2012: Draft Notes

The Chair reminded members that the full audited financial statements would come before the Committee at the June 13th meeting, at which time the Committee would consider a motion to recommend approval. Ms Brown and Mr. Piché would, at that meeting, report specifically on any changes to the wording of the notes made between now and June 13th. Therefore, the presentation of the notes at this time was for information, and while no formal action was required, the Committee should tender any advice. Any advice provided at this time could be considered for incorporation into the statements presented on June 13th.

Mr. Piché reported that the changes to the notes from the previous year were relatively few in number, but they were important.

- **Note 5, Investments** included information about the new structure adopted by the University of Toronto Asset Management Corporation (UTAM) for managing investments in publicly traded securities. UTAM had, in order to save trading costs, established unitized pooled funds for all investments in five categories of publicly traded assets: two fixed-income funds and three funds to hold investments in Canadian, U.S. and international equities respectively. All investments in each of those asset classes, whether made for the pension fund master trust or the Long-Term Capital Appreciation Pool (primarily the endowment funds) would be made in one of those pools, with the pension fund and the L.T.CAP holding units in the pools.

- **Note 11, Series E senior unsecured debenture**. The note reported the new debenture issue amounting to $200-million to be used primarily to fund capital projects, at an interest rate of 4.251%.

- **Note 23, First Generation Pilot Project Initiatives**. The note reported expenditure on a pilot project "to increase the awareness of the benefits of post-secondary education of first-generation students thereby increasing their participation, retention and graduation rates." A member observed that the reason for this note was unclear. Mr. Piché replied that, like the notes concerning the Ontario Student Opportunity Trust Fund and the Ontario Trust for Student Support, the funder for this initiative had insisted on the separate note disclosure or on a separate audit of the fund. The former, less expensive option had been selected. In response to a question, Mr. Piché said that the fund would be included as being subject to the general audit of the University's financial statements. The fund was, however, small relative to the materiality threshold for the overall audit.

In response to the Chair's suggestion, Mr. Piché commented on note 2(n), Future Accounting Policy Changes. He recalled that, as reported to the Committee at the previous meeting, the University had decided to apply the new Part III of the Canadian Institute of Chartered Accountants' (C.I.C.A.) Handbook for the 2013-14 financial statements. That decision would mean recognizing immediately the full cost of employee future benefits (reducing net assets by about $926-million) and at the same time valuing the University's land at its fair market value

**2. Audited Financial Statements for the Year ended April 30, 2012: Draft Notes**

(leading to an increase in net assets of about $2.05-billion). It appeared that that approach had been or would be adopted by other Ontario universities. Mr. Piché had, however, just learned that the Canadian Association of University Business Officers (CAUBO) staff had prepared a draft response to the C.I.C.A. supporting the deferred amortization method of accounting for employee future benefits. Mr. Piché had advised the CAUBO staff of the views of the Ontario university finance officers with respect to the matter and had urged further discussions.

**3. Risk Assessment: Information Technology: Follow-Up Report**

The Chair recalled at the December meeting, the Committee had received a detailed report on information-technology risk and risk management. A significant part of the report had dealt with the improved security arrangements at the University's new data centre. At that time, it was suggested that it would be useful to hear again from the Chief Information Officer with "a framework for understanding the overall risks in the information-technology environment. What did the Information-Technology Services group see as the priorities the University should adopt for dealing with risk? What were the major needs and opportunities?"

Mr. Cook said that he and Mr. Loeffler were pleased to provide a report to follow up on that presented to the Committee in December. The objectives of the current presentation would be: to describe the University's risk-identification process; to describe the key areas of risk; to discuss the challenges involved in managing those risks; and to describe the strategies for managing risk.

Mr. Loeffler presented the report.

- **Risk identification**. Information security encompassed the need for the confidentiality of data, its integrity, its availability to appropriate users, and accountability for its use. The security of information had to be assured throughout the five parts of its life-cycle: its creation and use; its transport; its storage; its administration; and its deletion and destruction. There were two types of strategies available to ensure the security of information. The first was the identification, authentication and authorization of appropriate creators and users of the information. That strategy involved the requirement for appropriate users to log into the system to which they had access, identifying themselves by an assigned user name, authenticating their access by entry of a password, and then being granted authorization to have access to the system. The second strategy involved isolation, continuity and reporting. Isolation of systems behind network firewalls reduced risk of intrusion. Redundancy of system components, and backup practices, enhanced continuity of service provision. System reporting supported optimization of performance and problem identification.

- **Key areas of risk**. Risk tended to be greatest where the value of the information was greatest, and that tended to be in the core enterprise systems: the student Portal and its

**3. Risk Assessment: Information Technology: Follow-Up Report** (Cont'd)

"Blackboard" system; the Human Resources Information System (H.R.I.S.); the Financial Information System (F.I.S.); the Student Information System (called ROSI or the Repository of Student Information); and the e-mail system. Research data resided on local systems within each Faculty or Department. While the central Information + Technology Services group shared ideas and expertise with the divisions, the security of the research information was wholly within the control of the divisions. Mr. Loeffler found that risk to information was frequently high where there was an uneven application of information-security practices. The strength of security measures in some areas tended to give a false sense of confidence concerning overall security.

- **Challenges in managing risk**. The University-wide systems were large and complex. They were in most cases developed within the University and were of a kind used only within the academic world. It was, therefore, difficult to replicate risk-control systems from outside the University's environment, and it was costly to develop customized risk-management systems. The University was proceeding with the development of business-continuity arrangements at the technical level. Data was being backed up outside the Data Centre, and redundant capacity was being introduced within the Centre. Other challenges arose from the use of the University-wide systems. Data was downloaded to the divisions, where it was less secure than it would be in a central environment. However, downloading data was essential in order to enable the divisions to do their work. The Information + Technology Services group was working with the Internal Audit Department to do the best possible job to meet information-security standards.

- **Strategies for managing risk: Information Security Guidelines**, approved by the Vice-President and Provost had been developed to advise users of the University's expectations. Those Guidelines began with high-level general statements of expectations, which were followed by progressively more detailed and more technical guidelines. The Guidelines defined data that should be regarded as confidential, set out measures to protect data, discussed retention and disposal of data, and set standards for security, discussing, for example, requirements for passwords and virus protection.

- **Strategies for managing risk: New Data Centre**. Actions to reduce risk had been taken in the establishment of the new data centre, which provided a robust, modern environment to host its virtual services. The Centre, as reported at the previous meeting, had back-up power supplies, fire suppression, and environmental monitoring, all to a very high standard.

- **Strategies for managing risk: Off-site backups and redundant systems**. The Information + Technology Services Group had taken advantage of the University's geographical diversification to establish off-site data backup in the Faculty of Dentistry building on Edward Street and in the Health Sciences Centre on the south side of College Street. The back-up arrangements included a "warm back-up" capability for the Blackboard system

**3. Risk Assessment: Information Technology: Follow-Up Report** (Cont'd)

within the student Portal, which backup was located in the Health Sciences Building. The arrangement would result in the ability to provide the back-up service very quickly in the event of a problem. To provide appropriate capacity and redundancy to divisions, it was of key importance that they articulate their expectations clearly. The student e-mail system was based on Microsoft architecture. With that firm's having its reputation on the line, it had invested heavily in redundant capacity.

- **Strategies for managing risk: services renewed on virtualized servers.** The use of virtualized servers enabled the provision of more than one backup server for each item of hardware. The model of one server for each service had ended. The result was considerable flexibility and ease of reloading of programs and data after a failure, and virtualized servers provided considerable ease of migration from old to new hardware.

- **Strategies for managing risk: protection for sensitive systems**. Firewalls and two-factor authentication were in place for all enterprise systems containing sensitive information.

- **Strategies for managing risk: prevention of intrusion**. Talented staff worked at detecting and observing efforts by hackers to enter the University's systems. The staff probed systems as might hackers in an effort to determine weaknesses. They made efforts to detect compromised accounts, for example ones in which efforts were made to log into systems from two widely separated locations. In such cases, they locked down the accounts and notified the users.

- **Strategies for managing risk: New initiatives**. The Information + Technology Services group was introducing an identity management system, enabling each user to employ a single user name and password for all systems. The group was looking into taking advantage of the University's tri-campus location for purposes of disaster-recovery and business-continuity plans. The main obstacle at present was limited bandwidth available, but the matter was under review with an aim to expanding the bandwidth. The group was working on encryption of administrative access and authentication traffic to core systems. Finally, it was planning to implement Security Information Event Monitoring. A dashboard would show suspicious events taking place in different systems, and potential infections would be tracked moving through those systems. That would trigger a lock-down of the system until the matter was cleared up.

Mr. Cook said, in conclusion, that the distributed nature of the institution posed a challenge. That challenge would be met by working on achieving compliance with the Information Security Guidelines and spreading the benefits of the good work of the Information + Technology Services group throughout the University. Mr. Cook was, happily, finding that there was considerable interest in the divisions in observing the Guidelines and in taking advantage of the expertise available.

**3. Risk Assessment: Information Technology: Follow-Up Report** (Cont'd)

The Chair thanked Mr. Cook and Mr. Loeffler for their report, and she instructed that the slides for the report be made available on the Audit Committee Resources section of the BoardBooks governance portal.

Discussion focussed on the following topics.

**(a) Information-security risk and information-technology risk**. Two members commented that information-security risk and information-technology risk could be seen as two separate risks. The report had dealt primarily with information-security risk and had dealt less with information-technology risk. For example, was the University managing change well – was it keeping up to date with new developments and investing in new systems? Was the University spending wisely in keeping up? Were the divisions opting into new arrangements? Was the University keeping up with COBIT guidelines with respect to information-technology governance, management, control and assurance?

Mr. Cook replied that he had interpreted the Committee's request to be for a report that dealt primarily with information-security risk. There were mechanisms in place to assess the improvements arising from upgrades and the consequences of decisions to make or not to make upgrades. He would be pleased to provide further information about information-technology risk, but he would be grateful for guidance with respect to the additional information required. The Chair suggested that a report based on the University's achievement of the COBIT criteria would be helpful. Mr. Cook said that the University was not yet at the point of adopting those industry standards, especially in view of the environment that distributed responsibility partly to the central Information + Technology Services group and partly to the divisions. However, the group was beginning to discuss the matter and it was working with the Internal Auditor to seek opportunities to establish institutional standards requiring compliance.

**(b) Central and divisional responsibilities**. A member said that the assessment of risk that had emerged was an uneven one, with considerable confidence about central risk management but uncertainty about risk-management in the divisions. That was a matter of concern in view of the fact that about two-thirds of spending on information technology took place in the divisions. Mr. Cook said that he and members of the Information + Technology Services group did not have the capacity to assess the security of research data, which was maintained in the divisions. While he did not know of the specific steps being taken to ensure security of research and other data maintained in the divisions, he did not lack confidence that the matter was being handled well by the divisions. There were University policies and procedures in place that governed the conduct of research. Grantors and sponsors had requirements in place as conditions of their grants and as terms of their research contracts, which requirements called for adherence to certain externally articulated standards of information security and (where appropriate) privacy.

**3. Risk Assessment: Information Technology: Follow-Up Report** (Cont'd)

Professor Mabury said that while two thirds of spending on information technology did take place in the divisions, much of that spending was for staff. A great deal of the work done by the divisions in using information-technology involved using the central administrative systems and divisional staff spend a substantial proportion of their time advising divisional staff on the use of those central systems. Divisions and departments did use certain systems independently, but most research data was maintained by individual faculty members whose systems were often limited to the basic operating system for their personal computers plus Microsoft Office.

**(c) Overview of information systems**. A member commented that committee members, who were from outside of the University, did not have a good overview of the central systems. It would be important to supply an overview of the key systems in place as well as the secondary ones. It would also be useful to know controls in place for each and to have an assessment of the gaps in those controls – gaps that occurred in any organization's systems. Such a high-level picture and assessment of gaps would enable the Committee to assist the Chief Information Officer and his colleagues in dealing with the gaps.

Professor Mabury suggested the preparation of a single-page overview with the requested information about the key University-wide systems and the controls in place with respect to them.

Mr. Cook thanked the Committee for its interest in information-technology services and risk. It had not always been the case that his portfolio received high-level attention. He would be very pleased to provide the requested overview of systems and the breakdown of spending between the centre and the divisions.

The Chair said that the additional information would be very helpful. While the first meeting of the Committee for the academic year was usually scheduled for December, it might well be valuable to hold a meeting earlier in the fall that would (among other things) permit additional consideration of information-security and information-technology risk, with the aid of the additional information that Mr. Cook had kindly agreed to supply.

**4. Risk Assessment Profile, 2012**

The Chair said that the Audit Committee terms of reference called upon the Committee to review "an annual management report on significant business, financial and regulatory risks and [to] monitor the University's processes for identifying and controlling those risks. In carrying out this responsibility, the Committee focuses primarily on the adequacy of key controls over, and mitigations of, those vital risks considered to be, currently or in the future, more significant and likely to occur, [and] meets with management and the internal or external auditors to come to a fuller understanding and better assessment of management's response to controlling important risk situations. . . " The Committee would report any concerns to Professor Mabury, to the President, or to the Executive Committee of the Governing Council, as appropriate.

**4. Risk Assessment Profile, 2012** (Cont'd)

Professor Mabury said that Ms Riggall had, before her retirement, drafted the report now before the Committee. Professor Mabury had sent the draft report to the vice-Presidents or other senior officers responsible for managing each area in risk with the request that they review and update the draft as appropriate.

Professor Mabury reviewed each area of risk along with the mitigating controls and risk-management practices in place, and he responded to questions. In the course of discussion, the Committee agreed to request: (a) a presentation on risk and risk-management in the area of research; and (b) a report from the Internal Department on its activities in relation to the risk-mitigating factors identified in the risk-assessment report.

The Chair stressed that the risk-assessment document was particularly sensitive, and it was especially important that members ensure that the report, and the discussion at the Committee's meeting, remain confidential.

**5. Reports of the Administrative Assessors**

Mr. Piché reported on the discovery of a financial fraud that had taken place in the University and on the steps taken to deal with it. The University would be bringing the matter to the attention of the Police with the recommendation that a criminal charge be laid.

Mr. Piché reported that the Moody's credit rating agency had, in a recent credit opinion, downgraded the credit rating of the Province of Ontario and of three Ontario universities, including the University of Toronto. The University's credit rating was changed from Aa1 with a negative outlook to Aa2 with a stable outlook.

**6. Date of Next Meeting**

The Chair reminded members that the next regular meeting of the Committee was scheduled for Wednesday, June 13, 2012 at 4:00 p.m. The major item of business would be the review of the audited financial statements. The Committee would also, among other things, receive the annual report on insurance and risk management and the annual report of the Internal Audit Department.

**8. Internal Auditor: *In Camera* Meeting**

(a) The administrative assessors other than Mr. Britt, and(b) the Secretary absented themselves.

**8. Internal Auditor: *In Camera* Meeting**

THE COMMITTEE MOVED IN CAMERA.

The Chair invited Mr. Britt to comment on any matters that should be drawn to the attention of the Audit Committee, or to respond to any questions. A substantial discussion ensued.

THE COMMITTEE COMPLETED *ITS IN CAMERA* SESSION.

The meeting adjourned at 6:25 p.m.

Secretary Chair

June 8, 2012