Chapter 32
Advanced Education—Managing Risks to Post-Secondary Services from its Unsupported Critical IT System

1.0 Main Points

The Ministry of Advanced Education (Ministry) is responsible for the post-secondary education system, including coordinating, developing, implementing, and promoting the Government's programs related to post-secondary education.[1] The Ministry uses its One Client Service Model (OCSM) system to support the delivery of the programs.

The OCSM system resides on information technology (IT) infrastructure that is past its recommended life and for which it can no longer receive technical support or updates to fix known security problems or vulnerabilities (i.e., unsupported). Systems running on unsupported infrastructure are at greater risk of availability and security issues that could impact operations.

For the 12-month period ended August 31, 2015, the Ministry had, other than the following, effective processes to manage the risks to service delivery from its unsupported information technology system, the OCSM system. The Ministry needs to:

- Clarify roles and responsibilities for upgrading and patching the IT infrastructure on which the OCSM system resides
- Periodically obtain information to support decisions related to the IT infrastructure
- Implement long-term plans for upgrading and patching the IT infrastructure

Other ministries and agencies with IT systems that are unsupported may find the criteria in this chapter helpful in self-assessing their processes for managing risks related to their unsupported IT systems. See **Section 6.0 Glossary** for definition of IT terms.

2.0 Introduction

The Ministry works with other key stakeholders, including the Ministry of the Economy (Economy) and post-secondary education institutions to carry out its mandate. It provides operating and capital funding to post-secondary institutions, as well as financial support to post-secondary students (e.g., student loan programs, bursaries). For 2015-16, it expects to provide $707.8 million[2] (2014-15: $716.1 million)[3] to post-secondary institutions and $56.6 million[4] (2014-15: 90.1 million)[5] to support students.

[1] *The Ministry of Advanced Education Regulations,* s. 3.
[2] Ministry of Advanced Education, *Plan 2015-16*, p. 10.
[3] Ministry of Advanced Education, *2014-15 Annual Report*, p. 22.
[4] Ministry of Advanced Education, *Plan 2015-16*, p. 10.
[5] Ministry of Advanced Education, *2014-15 Annual Report*, p. 22.

The OCSM system is the primary IT system used to deliver key post-secondary services of the Ministry, certain post-secondary institutions,[6] and Economy. Key post-secondary services include student financial assistance, training programs, registration services, and employment-related counselling.

The OCSM system resides on certain IT infrastructure (i.e., application server hardware, application server operating system, and application and database operating software [i.e., Oracle]) that is past its recommended life and unsupported (i.e., vendors no longer provide technical support or updates to fix known security problems or vulnerabilities). This unsupported state may impact the availability and efficiency of the system over the long term.

2.1 Overview of OCSM System

The OCSM system is the key IT system of the Ministry. The Ministry is the steward of the OCSM system, and jointly manages it with Economy.

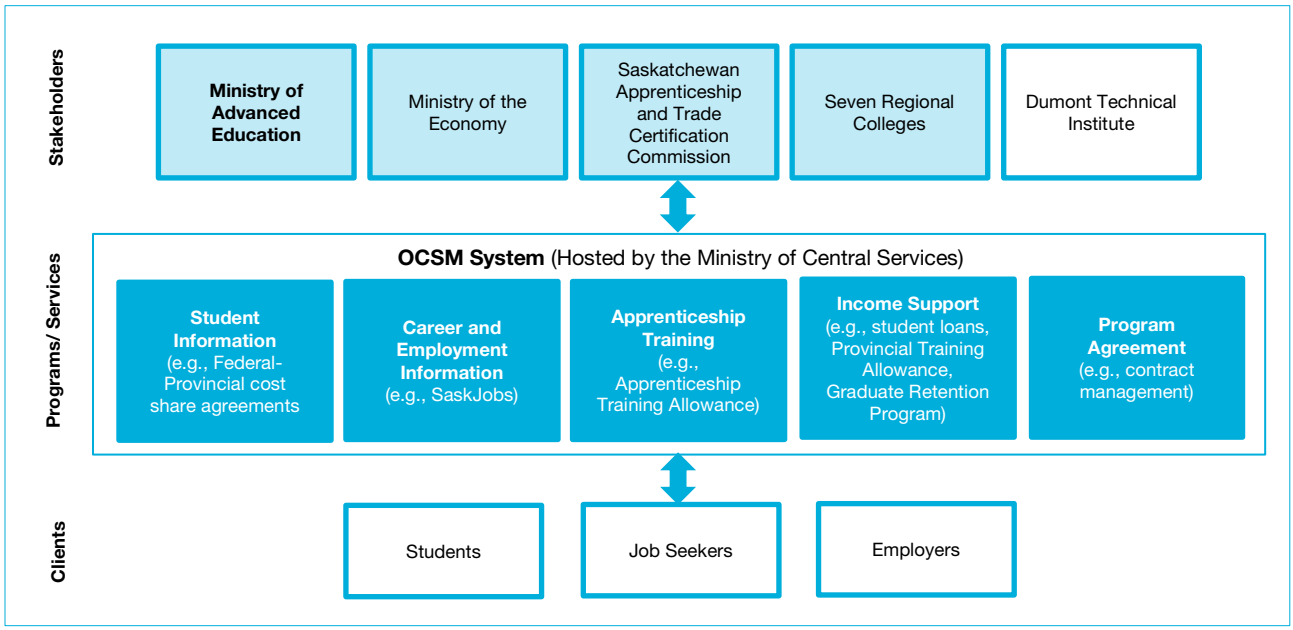
Some post-secondary institutions, the Ministry, and Economy rely significantly on the OCSM system to carry out their operations. The ministries use information in the OCSM system to apply for various federal-provincial cost-sharing programs, provide student loans, and make decisions about training programs (e.g., adult basic education, technical training to meet needs of employers). For example, in 2014-15, the Ministry provided over $53 million in student loans to about 12,000 full-time students[7] and Economy provided about $140 million for training programs,[8] some of which are reimbursed by the federal government. Post-secondary institutions use the OCSM system to manage student registrations and make operational decisions (e.g., budget, human resources). Student enrollments total about 20,000 in Saskatchewan's seven regional colleges.[9]

The Ministry pays the Ministry of Central Services to host and support the OCSM system. Hosting services provided by Central Services include certain security controls (e.g., firewalls, intrusion detection systems) that can help to reduce the risk of unauthorized access to hosted systems.

Figure 1 illustrates the various stakeholders and programs related to the OCSM system.

[6] Post-secondary institutions that use the OCSM system include the seven regional colleges, the Association of Regional Colleges, Saskatchewan Apprenticeship and Trade Certification Commission, and Gabriel Dumont Institute.
[7] Ministry of Advanced Education, *Annual Report for 2014-15*, p. 9.
[8] Ministry of the Economy, *Annual Report for 2014-15*, p. 35.
[9] Ministry of Advanced Education, *Annual Report for 2014-15*, p. 10.

Figure 1—OCSM System Stakeholders and Programs



Shaded Stakeholders are government entities; Ministry of Advanced Education (in bold) is the focus of this audit.
Source: Adapted from information provided by Ministry of Advanced Education.

2.2 A Brief History of the OCSM System

The OCSM system (an Oracle application and database) was developed in modules between 1999 and 2005.

Since 2005, significant changes to the OCSM system have been limited. In 2009 and again in 2013, the Ministry, through Central Services, upgraded OCSM database servers that were experiencing significant performance issues. However, the remaining IT infrastructure the OCSM system uses is past its end of life and unsupported as of August 31, 2015. For example, the Ministry and Central Services have not upgraded the underlying application and database operating software (i.e., Oracle) since vendor support ended in July 2008; this means no vendor security updates or other fixes have been possible for the past seven years. See **Figure 2** for a timeline of key events since the OCSM system's inception.

Figure 2—Timeline of Key Events for the OCSM System

1997: Adoption of a client-centred service model for common identity management (concept).

1999: First module, Career and Employment Information System, goes live.

2005: Last module, Integrated Income Support System (for student loans, provincial training allowance, and apprenticeship training allowance), goes live. The OCSM system infrastructure is upgraded.

2007: Student loan online application goes live.

2008: Vendor support ends for the underlying application and database operating software (Oracle).

2009: OCSM system's database server hardware and operating system upgraded.

2010: Provincial Training Allowance online application goes live.

2011: OCSM system experiences efficiency problems. Development of plan for the OCSM system mitigation and stabilization.

2013: OCSM system mitigation phase completed (i.e., database server hardware and operating system upgraded). Validation and initial planning for stabilization phase completed.

2015: Work begins on the stabilization phase.

Source: Adapted from information provided by Ministry of Advanced Education.

2.3 Risks of Running an Unsupported IT System

The lifespan of IT systems varies, with many public and private sector organizations choosing to use many IT systems for more than 10 years. While older IT systems may meet current needs, they may pose certain risks if the infrastructure on which they reside is not properly maintained. These risks include:

- **Disruption to service continuity** – system instability due to failing components or lack of people with the necessary skills to service these systems
- **Access to data** – information becomes increasingly cumbersome to extract and analyze as systems age
- **Security** – the system may not be able to be modified to meet changing security requirements (e.g., password complexity) or to respond to cyber threats[10] (e.g., bug fixes or patches no longer available to address security weaknesses)
- **Limited adaptability** – new business requirements (e.g., regulatory compliance, changing client expectations such as wanting online services) may be more difficult, time-consuming, and costly to implement
- **Rising maintenance costs** – costs increase due to complexity and difficulty carrying out maintenance activities, few service providers, and parts are scarce and costly
- **Manual workarounds** – manual processes required due to the lack of functionality within the system or inability to interface with other systems (e.g., performing detailed calculations on spreadsheets, re-entering data into other systems) as a result of being unable to use new software features only available in an updated version
- **Hidden costs** – the cost of workarounds and manual processes may not be identified, which could lead to poor decision-making[11]

Without sufficient and timely investment (e.g., financial, human resource), the risk of the OCSM system failing increases. Loss of the availability of the OCSM system prevents users from efficiently delivering key services to post-secondary students (e.g., not registering students for courses causing training delays and loss of revenues) and results in additional expenses (e.g., manual workarounds).

In addition, the OCSM system includes sensitive data about post-secondary students and some of their family members. Sensitive and confidential data include social insurance numbers, health numbers, birth dates, banking data, and income data.

[10] Cyber threats lead to risk of attackers hacking systems using electronic means such as the internet.
[11] Office of the Auditor General of Canada. (2010). *Report of the Auditor General of Canada – Spring 2010, Chapter 1, Aging Information Technology Systems*, p. 6; United Kingdom National Audit Office (2013). Managing the risks of legacy ICT to public service delivery, p. 19.

Unsupported infrastructure of the OCSM system increases the risk of unauthorized access to sensitive information.

3.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess the effectiveness of the Ministry of Advanced Education's processes to manage the risks to service delivery from its unsupported information technology system, the One Client Service Model (OCSM) system, for the 12-month period from September 1, 2014 to August 31, 2015. Unsupported IT systems are those for which vendors no longer provide technical support or updates to fix known security problems or vulnerabilities.

We examined the Ministry's policies, summaries of risks, risk management plans, and progress reports related to managing risks to service delivery from the OCSM system's unsupported state. We interviewed the Ministry's staff involved in management of the OCSM system and its related risks. We examined minutes from IT committees and other communications with stakeholders about risks posed by the OCSM system's unsupported state.

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate the Ministry's processes, we used criteria based on our related work, reviews of literature including reports of other auditors, and consultations with management. The Ministry's management agreed with the criteria (see **Figure 3**).

Figure 3—Audit Criteria

1. Analyze risks using a risk management framework
1.1 Identify significant risks
1.2 Determine impact and likelihood of risks occurring (e.g., collect data about incremental costs and adverse events caused by the system)
1.3 Evaluate if risks exceed acceptable risk levels
1.4 Confirm evaluation of risks with key stakeholders that use the system
2. Implement a risk management plan
2.1 Analyze options with key partners (e.g., Ministry of Central Services) to address unacceptable risks (e.g., consider cross-agency solutions)
2.2 Allocate resources
2.3 Implement cost-effective, long-term strategies for addressing risks
3. Monitor risk responses
3.1 Analyze actions and results compared to plan
3.2 Recommend changes to plan based on results
3.3 Report results to senior management and key stakeholders that use the system

We concluded that for the 12-month period from September 1, 2014 to August 31, 2015, the Ministry of Advanced Education had, other than the following, effective processes to manage the risks to service delivery from its unsupported information technology system, the One Client Service Model (OCSM) system. The Ministry of Advanced Education needs to:

- **Clarify roles and responsibilities for upgrading and patching the information technology infrastructure on which the OCSM system resides**
- **Periodically obtain information to support decisions related to the information technology infrastructure**

- **Implement long-term plans for upgrading and patching the information technology infrastructure**

4.0 Key Findings and Recommendations

4.1 Complete Information for Risk Analysis Needed

We expected the Ministry to determine the impact and likelihood of significant IT risks associated with the OCSM system, and use this information to evaluate if those risks exceed acceptable risk levels. Confirmation of risks with key stakeholders that use the OCSM system would help ensure the analysis appropriately evaluated all relevant risks.

The Ministry had an enterprise risk management policy and framework. It used this framework to consider the risks and lost opportunities (e.g., availability, security, limited adaptability) posed by the unsupported state of the OCSM system infrastructure. It included these risks in its list of enterprise risks.[12] It also considered possible causes leading to the OCSM system infrastructure's unsupported state (e.g., lack of upgrade and patching schedule, difficulties resolving funding sources, lack of collaboration/co-operation with key stakeholders). It also conducted surveys to assess stakeholder and client satisfaction with the OCSM system.

To help with its assessment of risk for the OCSM system, the Ministry requested from Central Services information about maintenance costs incurred, unavailability (downtime) statistics, and system weaknesses. Because Central Services could not provide all information requested, the Ministry carried out additional processes to increase the data available for the risk assessment. These processes included implementing monitoring tools to gather additional availability statistics and conducting security assessments[13] to identify system weaknesses. For example, using information from Central Services and its own tool, the Ministry identified about 47 hours of system unavailability (i.e., outages) where users could not access the OCSM system during April 1, 2013 to March 31, 2015. In May 2015, the OCSM system experienced its largest availability issue with a 66 hour outage.[14] The Ministry acknowledged these performance issues impacted its ability to provide services using the OCSM system.

The Ministry could not gather sufficient information about indirect costs such as manual workarounds or "break-fix"[15] costs. Also, the Ministry found that regular reports it received from Central Services did not provide complete information about the OCSM's system infrastructure, such as end of life/support dates and expected costs to upgrade to vendor supported infrastructure.

Information about indirect costs, end of life or support dates, and estimated costs to upgrade infrastructure is needed from Central Services to determine which options are the most cost effective to provide the required risk reduction. The Ministry requires this

[12] Enterprise risks are financial, strategic, and operational risks faced by an organization.
[13] Security assessments test an IT system to find vulnerabilities that an attacker could exploit (e.g., vulnerability assessment, penetration testing).
[14] Obtained from Ministry of Advanced Education availability monitoring tool.
[15] "Break-fix" is the reactionary repair of an IT system due to issues with computer equipment, the network, or software programs.

information to develop effective long-term plans for maintaining its OCSM system infrastructure over its expected remaining life.

Without sufficient, appropriate information about the risks, the Ministry may not correctly assess risks to make effective decisions.

1. **We recommend that, to analyze risks and make decisions about its One Client Service Model system, the Ministry of Advanced Education periodically obtain information about its One Client Service Model system's:**
   - **Indirect costs**
   - **Information technology infrastructure end of life or end of support dates**
   - **Estimated information technology infrastructure upgrade costs to maintain vendor support**

The Ministry's enterprise risk assessment process used information available to assess the impact and likelihood of risks occurring. The Ministry used an overall scoring method called a "heat map" to evaluate if the risks exceeded acceptable risk levels and to identify the top priorities for risk treatment. In the 2015 risk information, the OCSM system's unsupported IT infrastructure ranked as one of the top risk mitigation priorities for the Ministry.

While the Ministry's risk management processes reflected a Ministry-specific view, the risks related to the OCSM system's unsupported infrastructure are also applicable to other key stakeholders that use the OCSM system (e.g., Economy, regional colleges). The Ministry discussed risks to the OCSM system at its regular IT committee meetings with these stakeholders. The meetings provided stakeholders an opportunity to provide feedback so that the Ministry would be able to confirm its evaluation of risks or make necessary adjustments. For example, consistent with the Ministry's concerns, the biggest concern for stakeholders with regards to the OCSM system related to its limited adaptability and the lack of long-term planning for the system.

4.2 Implementation of Risk Management Plan Ongoing

4.2.1 Planning Options over Expected Remaining Life Needed

We expected the Ministry to work with its key partners to identify and analyze options to address unacceptable IT risks related to the OCSM system. The analysis would include assessment of the cost and suitability of options. The Ministry would use the analysis to select cost-effective risk management strategies for the short-, mid-, and long-term. We expected the Ministry to develop operational plans (e.g., multi-year action plans, deadlines, detailed financial and human resource budgets) to implement its IT risk management strategies and communicate the plans to its stakeholders.

The Ministry and Economy worked with Central Services to identify options for addressing risks related to the OCSM system including upgrades to the OCSM system

infrastructure to a vendor-supported state. The analysis provided information about detailed actions and requirements, allocation of human resources, budget, and deadlines.

The Ministry has a strategy to make changes to the OCSM system infrastructure to enable it to have vendor support. In 2011, Central Services recommended a three-phase plan for the OCSM system:

- Mitigate immediate performance issues (mitigation phase)
- Move the OCSM system infrastructure to a supported state (stabilization phase)
- Meet additional business requirements of the sector (modernization phase)

The Ministry accepted this recommendation. The Ministry's *Information Management Strategic Plan – 2012-2016* included risks and plans related to the OCSM system's unsupported IT infrastructure. It completed the initial mitigation phase in 2012-13; this project included the replacement of database server hardware related to OCSM.

In 2013, Central Services provided the Ministry with two options for the stabilization phase: complete the work within one year or spread over two years. For each option, Central Services estimated the costs, deadlines, and business impacts such as human resources required. The Ministry worked with Central Services to validate the feasibility of plans for the stabilization phase. The Ministry selected the option to complete the work within one year, but funding was not identified to complete the work in that year.

Regional colleges communicated concerns in 2013 about delays in completing the stabilization phase and the impact on their ability to deliver services to students. They expressed declining confidence in the Ministry's ability to address the OCSM system's performance risks. In response, the Ministry has kept the regional colleges up to date about ongoing developments. Also, the Ministry initiated business capability planning to document gaps in the system's functionality and opportunities for improvements, and completed additional assessments of the system to refine its risk analysis.

In 2014, the Ministry revisited its plans for the stabilization phase to determine what work could be done with existing resources (e.g., divide work into manageable pieces that can be completed and afforded over a longer timeframe). The Ministry worked with stakeholders to prioritize other sector IT initiatives to reallocate funding to the stabilization phase. Following this, the Ministry and Economy worked with Central Services to update the work plan to complete the work over two years and included a revised budget. Work on the stabilization phase began in summer 2015.

The Ministry received regular progress reports, including information about contractual requirements and approved changes. Detailed plans were not yet developed for the second year of the stabilization phase; however, a detailed plan is expected before work begins for the 2016-17 year.

The 2011 three-phase plan identified the need for a strategy to maintain vendor support for OCSM system's infrastructure over the long-term (i.e., to keep supported after the stabilization phase is complete and considering decisions made in the modernization phase). As of August 31, 2015, given lack of key information, the Ministry had not determined the expected remaining life of the OCSM system infrastructure and how best

to maintain it over its remaining life – that is, the Ministry had not developed a plan for upgrading and patching the OCSM system infrastructure over its expected remaining life. Such a plan is necessary to facilitate a schedule and budget for upgrading and patching the system over its expected remaining life.

Without a plan to upgrade and patch the OCSM system infrastructure over its expected remaining life, the Ministry and other stakeholders that use the OCSM system will continue to be at risk of the infrastructure remaining unsupported. Systems running on unsupported infrastructure are at greater risk of availability issues that could impact the ability to apply for federal-provincial cost-sharing programs or the ability of students to register for classes, apply for student loans, or apply for training programs. It also increases the risk of security breaches that could expose confidential information maintained in the OCSM system.

2. We recommend that the Ministry of Advanced Education develop and implement a plan, over the One Client Service Model system's expected remaining life, for upgrading and patching the information technology infrastructure on which the system resides.

The Ministry and Economy pay Central Services about $620,000 each year for hosting the OCSM system and about $190,000 each year for Oracle licensing costs. According to Central Services' IT service catalogue, the hosting service includes software and server upgrades, patches, and maintenance.[16] The Ministry and Central Services were not clear about who was responsible for determining when to upgrade and patch the OCSM system infrastructure. As a result, the OCSM system infrastructure was not regularly upgraded and patched.

At August 2015, the Ministry's service agreement with Central Services remains incomplete; it does not clearly state who is responsible for upgrading and patching the OCSM system infrastructure and paying for the associated costs. We initially reported this matter in our *2008 Report – Volume 3,* Chapter 2. At August 2015, the Ministry continues to negotiate its service agreement with Central Services.

Sound service agreements should reflect long-term strategies to maintain systems over their expected lives, including clarifying roles and responsibilities and funding processes (i.e., clearly indicate if system upgrades and patches are included in monthly fees or how these will be billed). If roles and responsibilities are unclear, the system's infrastructure may not be maintained and supported as required, which has occurred with the OCSM system.

3. We recommend that the service level agreement between the Ministry of Advanced Education and the Ministry of Central Services clearly outline responsibility for upgrading and patching the information technology infrastructure on which the One Client Service Model system resides and the associated costs.

[16] *ITD Service Catalogue, Version 5.1*. p. 8.

4.2.2 Allocating Resources to Risk Management Plans

We expected the Ministry to assign responsibility and allocate financial and human resources for its IT risk management strategies.

The Ministry assigned responsibility for the risks related to the OCSM system to a member of its executive team. In 2015, the Ministry, Economy, and Central Services developed a detailed plan for completion of 2015-16 work of the OCSM system stabilization phase. This plan assigned roles and responsibilities to members of a project team and established a budget of $1.1 million. The Ministry and Economy agreed how to share the costs for the project. The Ministry, Economy, and Central Services expect to agree on a detailed 2016-17 work plan and budget in early 2016.

4.3 Risk Strategies Monitored

We expected the Ministry to analyze actions and results compared to the plan to inform changes to the risk management plan. Processes would include review of outcomes and recording of residual risk. Results and changes to the plan would be reported to senior management and key stakeholders that use the OCSM system.

The Ministry received regular progress reports from Central Services regarding the status of the OCSM system stabilization project. These included updates about project risks and explanations about any differences from budget or deadlines. The Ministry met regularly with Central Services to discuss the reports. The Ministry also discussed progress regularly at meetings of its executive.

The Ministry's policy required its executive to monitor its plan to manage risks during the year and to annually approve changes to the risk listing. The executive reviewed its listing of enterprise risks several times during 2014-15, including the risks related to the OCSM system unsupported infrastructure status. The review considered whether strategies were effective or if changes were required. The Ministry revised its strategies to address the risks to the OCSM system during the year as evidenced by its decision to internally fund the stabilization project over a two-year period when it could not find new funding sources. In summer 2015, the Ministry's executive approved a revised risk listing, including updated risk priorities.

Throughout the year, the Ministry met regularly with key stakeholders through its IT management committees. IT risks, including the risks related to the OCSM system's unsupported infrastructure, were discussed regularly at the meetings. The Ministry provided updates about the plans to address the risks.

5.0 Selected References

Office of the Auditor General of Canada. (2010). *Report of the Auditor General of Canada – Spring 2010, Chapter 1, Aging Information Technology Systems.* Ottawa: Author.

Provincial Auditor of Saskatchewan. (2014). *2014 – Report Volume 2, Chapter 37, Saskatchewan Rivers School Division No. 119 – Processes to Maintain Facilities*. Regina: Author.

Provincial Auditor of Saskatchewan. (2012). *2012 Report – Volume 2, Chapter 35, Saskatchewan Indian Gaming Authority Inc. – Information Technology Threat and Risk Assessment Processes*. Regina: Author.

Provincial Auditor of Saskatchewan (2011). *2011 Report – Volume 1, Chapter 2, Advanced Education, Employment and Immigration*. Regina: Author.

Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment (TRA) Methodology*. Ottawa: Author.

United Kingdom, National Audit Office. (2013). *Managing the Risks of Legacy ICT to Public Service Delivery*. London: Author.

6.0 Glossary

Application – A software program. This includes programs such as word processors, spreadsheets, accounting programs, etc.

Database – A comprehensive collection of related data organized for convenient access in a computer.

Hardware – The physical device (e.g., server) used to share data on a network.

Information Technology (IT) Infrastructure – For the purpose of this audit, IT infrastructure is application server hardware, application server operating systems, and application and database operating software.

Network – A group of computers that communicate with each other.

Operating System – A computer program that runs other programs and applications.

Patch – An update to a computer program or system designed to fix a known problem or vulnerability.

Server – A computer that hosts systems or data for use by other computers on a network.

Software – A set of machine-readable instructions that directs a computer to perform specific operations.

Unsupported Systems – Systems where venders no longer provide technical support or updates to fix known security problems or vulnerabilities.