Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Expanding OCTAVE to Facilitate SysTrust

by

DARI, Bashar

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Expanding OCTAVE to Facilitate SysTrust

by

DARI, Bashar

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

ISSM 571
Research Project

Concordia University College of Alberta
Master of Information Systems Security Management

Research Paper

Expanding OCTAVE to facilitate SysTrust

Prepared By:

Bashar Dari

Email: **bwdari@telus.net**

Student # **110429**

Research Advisors:

Dr. Pavol Zavarsky

Dr. Dale Lindskog

Table of Contents

KEYWORDS

AICPA/CICA SysTrust™ Principles and Criteria, control frameworks, availability, confidentiality, controls, control objectives, Information Security Framework (ISF), information security risk management, integrity, OCTAVE[SM] (Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM]) , risk assessment, risk profile, threat profile.

EXECUTIVE SUMMARY

Operationally Critical Threat Asset and Vulnerability Evaluation (OCTVAE) and SysTrust are two information security methodologies used to audit and review information security practices. OCTAVE is a comprehensive methodology to assess and analyze information security risks based on IT asset type. OCTAVE is ideal to be used by internal organization resources to perform Threat/Technology risk assessment (TRA). SysTrust on the other hand is set of criteria and controls acting as an audit checklist aimed at providing stakeholders with assurance that organization has adequate controls for its application. SysTrust is driven from a financial background and can only be performed by a licensed certified Public Accountant. Organizations might find themselves using both methodologies (e.g. using OCTVAE-S for their internal TRA and SysTrust to gain the seal of assurance from an independent 3rd party).

OCTAVE and SysTrust have several similarities and many differences. One main similarity is that both methodologies are considered an information security audit/review exercise based on the three famous security principles: confidentiality, integrity, and availability. The two most important differences are: OCTAVE is a methodology while SysTrust is a set of criteria and controls that act

as an audit checklist, and SysTrust can only be done by licensed CPA while OCTAVE can be used by internal or external resources.

Two main components of OCTAVE-S (which is a variation from OCTAVE for small organizations) has been mapped against SysTrust criteria and controls. These two components are: security practices questionnaires and threat profiles. Mapping OCTAVE-S security practices statement to SysTrust controls allow organization to better understand its readiness for a SysTrust certification audit by identifying which SysTrust controls are in place, which are missing, and which can be compensated by other controls.

Developed threat profiles for application, ORACLE database, and UNIX server provides a template or start point for organizations who need to conduct a TRA for IT assets with similar types. These threat profiles that are mapped to SysTrust controls can help organizations in identifying controls needed to mitigate unacceptable risks. They can also help prioritizing OCTAVE-S action items and mitigation plans based on their alignment with SysTrust.

INTRODUCTION

Information Technology (IT) is driving Business in all sectors. Security in IT field have gained special attention in recent years especially after 9/11 events in the US. Business executives are required to demonstrate accountability for their business more than ever before. Sarbanes-Oxley Act and other regulations are demanding such accountability.

In order to demonstrate accountability, executives need to assess and manage IT Risks. There are different approaches in the market to assess and manage IT risks. The most common ones are: conducting Vulnerability Assessment (VA), conducting Penetration Testing (PT), conducting a

Threat Risk Assessment “sometimes called technology risk assessment” (TRA), and compliance with an accepted trust/control framework like COBIT or SysTrust. Unfortunately, there is no one de facto or generally accepted standard to assess and manage IT risks. The main reason behind that is that IT risks are dependant on the business type and supporting IT infrastructure. Each organization has its own unique risk profile based on its IT assets: people, processes, and technology. Each approach has its strengths and weaknesses. Executives need to decide on what is the best approach for their organization, or do they need a combination of approaches. Some Organizations might need to use one or more of these approaches in the course of assessing their IT risks. One example is for an organization that is using both TRA and SysTrust: TRA is used as an internal process to analyze information security risks while a third party will conduct a SysTrust certification audit in preparation of awarding this organization/business the SysTrust seal of Assurance. This SysTrust seal of assurance indicates that organization’s IT processes have adequate controls as per internationally accepted best security practices.

Operationally Critical Threat Asset and Vulnerability Evaluation (OCTVAE) is a risk analysis methodology developed by the Software Engineering Institute (SEI) and it is a comprehensive self-directed approach to TRA.

This research links OCTVAE with SysTrust by extending OCTAVE to facilitate and incorporate SysTrust criteria and illustrative controls. This will help organizations leverage work done internally with OCTAVE to fulfill SysTrust audit requirements and hence saving organizations both time and money by removing duplication/overlap between these two audit/review activities.

LITERATURE REVIEW

TRAs are usually based on a standard or framework. The American Bankers Association recommends the following resources for TRAs: International Standards Organization (ISO) 17799, Control Objectives for Information Technology (COBIT), SysTrust, Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE), and NIST. Both Lanz (2002) and Campbell (2003) have described these approaches in detail. Lanz (2002) compared between ISO standards, COBIT, SysTrust, OCTAVE, and NIST.

American Institute of certified Public Accountants (AICPA) and the Canadian Institute of Charted Accountants (CICA) developed **SysTrust** which is a service to provide assurance on the reliability of systems. SysTrust principles are: availability, security, integrity or maintainability. Lanz (2003) states that" SysTrust principles could be adopted as an effective TRA tool since the principles provide a stakeholder's perspective on the impact of technology on business activities."

OCTAVE is developed by the Software Engineering Institute (SEI) and it is a comprehensive self-directed approach to TRA. OCTAVE is a focused approach in the sense that it assess risks on IT assets based on their criticality. OCTAVE has a comprehensive online documentation published on http://www.cert.org/octave/pubs.html. There are several variations of OCTAVE. The most important one is OCTAVE-S for small businesses. OCTVAE-S is the most ideal choice for small to medium organizations as such OCTAVE-S will be the subject of this research.

OCTAVE-S is a free methodology that can be used by an organization internally as the basis/framework for their information security risk management process. OCTAVE-S approach is to analyze security risks for critical IT assets first. OCTAVE-S identifies IT assets in terms of: systems,

information, software, hardware, and people. OCTVAE-S provides very generic threat profiles for human actors using network access, human actors using physical access, system problems, and other problems only. As such, OCTAVE-S does not provide any generic threat profile for any type of assets (e.g. ORACLE database threat profile). This is one area that can be expanded in OCTAVE-S; Creating generic threat profiles for some common types of IT assets while including illustrative controls listed in SysTrust.

Another potential area of linkage between OCTAVE-S and SysTrust is the step to "Capture Current Security Practices" in OCTAVE-S. OCTAVE-S's security practices have 15 areas which can be mapped to SysTrust criteria that are divided into four areas: policies, procedures, communication, and monitoring.

Literature review has revealed that there is no work in the field of mapping or linkinking OCTAVE-S with SysTrust.

RESEARCH STATEMENT

This research attempts to enhance OCTAVE-S to incorporate and facilitate SysTrust audit. The main objective of this research is mapping SysTrust controls in the areas of security, confidentiality, processing integrity and availability to OCTAVE-S. This mapping focuses on two OCTAVE-S materials: Security Practices questionnaire and Threat profiles.

RESEARCH METHODOLOGY/METHODS

The main objective of this research is to expand OCTAVE to facilitate SysTrust audit by 3rd party. Hence, the following need to be taken into consideration:

1. Many SysTrust criteria and illustrative controls can be mapped to many OCTAVE's security practices statements.

2. Care should be given not to transfer OCTAVE into a SysTrust audit. The main focus should be to leverage overlapped/duplicated efforts in both security review/audit activities.

3. OCTAVE can help prepare an organization for a SysTrust certification audit by:

    a. Making sure that IT processes, procedures, and practices are documented. Tacit knowledge needs to be documented as possible.

    b. Listing all related supporting documents beside identifying missing ones.

    c. Identifying IT processes owners and contact information.

This research was approached in the following order:

1. Both SysTrust and OCTAVE have been reviewed in depth resulting in a comprehensive comparison between OCTAVE and SysTrust identifying similarities and differences.

2. OCTAVE-S's security practices questionnaire statements have been mapped to SysTrsut controls.

3. Three threat profiles have been created for: Application/information-system, ORACLE Database, and UNIX server. Threats in these profiles have been mapped to SysTrust related controls.

DELIVERABLES

A comprehensive comparison between OCTAVE and SysTrust can be found in Appendix A. OCTAVE-S's security practices questionnaire statements mapping to SysTrust criteria and controls can be found in Appendix B.

A threat profile for an application/information system asset mapped to SysTrust controls can be found in Appendix C. Appendix D & Appendix E contains threat profiles for an Oracle Database and UNIX server respectively.

Findings and Discussion

OCTAVE and SysTrust have several similarities but many differences. The most important similarities are:

1. Both OCTAVE and SysTrust are considered information security review/audit activities. Furthermore, these two methodologies/approaches are based on the three famous information security domains: confidentiality, Integrity, and Availability.

2. Both methodologies have been recommended by American Bankers Association to be used for Technology Risk Assessments (TRAs).

The main differences between OCTAVE and SysTrust are:

1. SysTrust is a set of criteria and controls similar to a checklist. SysTrust does not tell you how to conduct a TRA. OCTAVE on the other hand is a comprehensive methodology/approach

that outlines how to conduct a TRA from start till finish. Though, OCTVAE can not be viewed as a checklist with the exception of its security practices questionnaire.

2. SysTrust can only be performed by Certified Public Accountant licensed by AICPA and CICA. OCTAVE can be performed by internal resources, 3rd party vendor, or both.

3. SysTrust certification audit is conducted for one IT asset type (namely application or information system). OCTAVE can apply to different types of IT assets: Hardware, System, Software, Information, and people.

The mapping of OCTAVE-S security practices questionnaire statements to SysTrust controls has revealed the following observations:

1. Many SysTrust Illustrative Controls are duplicated in Security, Availability, Processing Integrity, and Confidentiality but with focus on that area (e.g. SysTrust illustrative controls talking about “Physical Access Restriction” which includes Security 3.2, Availability 3.5, Processing Integrity 3.6, and Confidentiality 3.5 are identical in all four areas). This explains why a security practice statement might be mapped to many SysTrust criteria and controls.

2. Many SysTrust Illustrative controls are listed in more than one criteria in the same security domain (e.g. conduct periodic security reviews and vulnerability assessments are listed in Security 3.3, 3.8, and 4.1).

3. OCTAVE-S pays attention to outsourcing by adding a specific section in many security practices domains for "If staff from a third party is responsible for this area:" While SysTrust has very few number of illustrative controls for outsourcing and they are mainly in the confidentiality area.

4. SysTrust does not mention security strategy. This topic might be implied from the security policies section, though no specific mention of security strategy. SysTrust talks about a Backup and Restoration strategies only.

5. OCTAVE-S has some security practice statements that are difficult to measure. Some security indicators might provide relative information (e.g. “staff members follow good security practices” can be measured by number of security incidents with user as root cause).

6. SysTrust concentrates on Policies administrative controls; in the sense of policies needs to be reviewed periodically and updated. It does not mention same administrative controls to other types of documents: standards, processes, procedures, and guidelines. While OCTAVE-S security statements include these administrative controls for standards, procedures and processes beside policies.

7. OCTAVE-S Security practices statements are very specific or directly related to IT and Physical Security. The background of OCTAVE-S is IT/Physical Security while the background of SysTrust is Financial Systems/Transactions. This is why we find many OCTAVE-S statements with no match or exact match in the SysTrust criteria and controls. (e.g. Working with Law Enforcement is found in OCTAVE-S but not SysTrust).

One good example of a security practice statement mapped to SysTrust control is: “System and Network Management” area of OCTAVE-S security practices states that “*Only necessary services are running on systems - all unnecessary services have been removed*.” This can be mapped to the following SysTrust criteria: Security 3.3.4, Availability 3.6.4, Processing Integrity 3.7.4, and Confidentiality 3.6.4which states that “*Unneeded network services (e.g., telnet, ftp,*

and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions."

An application threat profile has been created in Appendix C. This threat profile contains a list of threats that might impact an application/information-system. The impact of this threat on confidentiality, integrity, and availability is flagged. Each threat is mapped with a set of SysTrust controls that can mitigate risk of that threat. For example, the threat of "**Computer viruses impact (Worms, Trojan Horses, Spyware, Adware)**" can be mitigated by two main controls:

1. Preventive/Proactive Control: Anti-Virus Software as identified in SysTrust criteria: Security 3.4, Availability 3.7, Processing Integrity 3.8, and Confidentiality 3.7.

2. Detective/Reactive Control: Incident Management as identified by SysTrust criteria: Security 3.6, Availability 3.9, Processing Integrity 3.10, and Confidentiality 3.9.

CONTRIBUTION TO KNOWLEDGE

The maximum benefit of mapping OCTAVE-S to SysTrust is achieved when the OCTAVE-S based TRA and the SysTrust certification audit is performed for the same application/information-system.

The ideal scenario is to conduct OCTAVE-S based TRA on critical application/information-system. Next, ask a licensed CPA to conduct the SysTrust audit. In this case, the mapping can be used in the OCTAVE-S based TRA in a way to prepare organization for the SysTrust audit. Hence,

OCTAVE-based TRA will act as a preliminary stage to address any SysTrust related weaknesses/gaps.

Mapping identified in this research can be used in the following way to leverage SysTrust certification audit:

1. **OCTAVE-S security practices questionnaires**: Part of OCTAVE-S based TRA, an organization needs to score/evaluate its alignment with stated security practice statements. Organization can then make use of the corresponding SysTrust mapping in the following way:

    a. The SysTrust mapping can help organizations understand specific controls that need to be in place to address the corresponding OCTAVE-S security statement. This can help organizations understand the security practice statement much better and hence provide better scoring/evaluation for this OCTAVE-S security practice statement.

    b. Organizations can identify which SysTrust controls are currently in place, which are not, and which can be replaced/mitigated by other controls. This analysis will help organization answer/respond to licensed CPA's SysTrust audit questions. For example, this analysis will help organizations identify missing processes or missing documentation that are needed for SysTrust certification audit.

2. **Threat profiles mapped to SysTrust controls:** The first advantage of these Threat profiles (for application, Oracle Database, and UNIX Server) is that they provide a good start point/template for any organization conducting an OCTAVE-S based TRA for similar type

assets. The second advantage is achieved when organization need to mitigate high-risk threats to an acceptable risk levels. Organizations can choose some or all of mapped SysTrust controls as mitigating controls. A third advantage of this mapping is to help in prioritizing action items and mitigation plans. Actions items and mitigations plans can be classified as directly related to SysTrust or not related to SysTrust. Organizations should give higher priority for those action items and mitigation plans that are directly related to SysTrust.

3. Lastly, the previous two mappings will help internal resources work first hand with many SysTrust criteria and controls. Hence, establishing SysTrust competency among them.

PRELIMINARY BIOGRAPHY

AICPA & CICA (2003). Trust Services Principles and Criteria.
Web Link: http://www.cica.ca/multimedia/Download_Library/Standards/WebTrust/English/e_TSPCriteria.pdf

Alberts, C., Dorofee, A., Stevens , J., Woody , W. (2005) OCTAVE-S Implementation Guide . Carnegie Mellon® Software Engineering Institute (SEI)
Web Link: http://www.cert.org/octave/

Campbell, P. (2003) An Introduction to Information Control Models. Sandia National Laboratories.
Web Link: http://www.sandia.gov/scada/documents/sand_2002_0131.pdf

Institute of Internal Auditors (IIA) (2005) GTAG Volume 1: IT Controls
Web Link: http://www.theiia.org/

Lanz, J. (2002). Prioritizing Aspects of Technology Risk Assessment and Mitigation. Bank Accounting And Finance Journal: Year 16; Part 1, pages 19-26
Web Link: http://www.joellanzcpa.com/downloads/articles/Dec%202002-%20BAF%20-%20Tech%20Risk%20Ass.pdf

Lanz, J. (2003) Conducting A Security Risk Assesment
Web Link: http://www.itriskmgt.com/speeches.html

Le Grand, G., Adar, E. (2006) White Cyber Knight – A Risk Assessment Tool for Network Resilience Evaluation
Web Link: http://www.whitecyberknight.com/Publications.aspx

APPENDIX A: COMPARISON BETWEEN OCTAVE AND SYSTRSUT

	SysTrust	OCTAVE
Definition	Trust Services (including SysTrust) are defined as a set of professional assurance and advisory services based on a common framework to address the risks and opportunities of IT. [AICPA]	OCTAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) is a risk-based strategic assessment and planning technique for security. [Cert.org]
Business Endorsement	The American Bankers Association recommends SysTrust as one of 5 methodologies for Technology Risk Assessment exercises.	The American Bankers Association recommends OCTAVE as one of 5 methodologies for Technology Risk Assessment exercises.
Publishing Entity	SysTrust was developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).	OCTAVE was developed by Christopher J. Alberts, Audrey J. Dorofee, and Julia H. Allen @ Carnegie Mellon University. Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.
Approach Variations	Trust Services include both SysTrust and WebTrust: **SysTrust** engagements are designed for the provision or advisory services or assurance on the reliability of a system. **WebTrust** engagements relate to assurance or advisory services on an organization's system related to e-commerce.	There are currently three recognized methods that meet the OCTAVE criteria, and other methods are under development by third parties. The recognized methods are: OCTAVE Method—for large organizations OCTAVE-S—for smaller organizations OCTAVE Allegro—for organizations focused on information assets and a streamlined approach
Target Audience	Target audience are management, customers and business partners. As SysTrust is designed to increase the comfort of management, customers, and business partners with systems that support a business or particular activity	Target Audience are mainly internal stakeholders. As Octave is related to Information Technology, hence it is target audience are mainly IT personnel. Protection plans and main mitigations plan recommendations are to be presented and actioned by IT senior management. Threat/Risk profiles and details of risk analysis are meant to be used by IT support analyst and IT security/risk personnel.
Risk Areas	There are five main: Security, Availability, Processing Integrity, Online Privacy, and Confidentiality. A SysTrust audit can be for any combination of the above five risk areas.	There are mainly three risk areas: Confidentiality, Integrity, and Availability. Ideally all of these risk areas should be taken into consideration.

Outcomes/ Deliverables	SysTrust Seal awarded along with an executive SysTrust seal letter (usually 2 pages). SysTrust seal ideally published on the main page of the web application/system site.	* For each IT asset: 1. Security Requirements. 2. Threat/Risk profiles. 3. Actions Items and Mitigation plans. * For overall Octave-based TRA: 1. Management/Executive report and presentation. 2. Detailed Risk Analysis report (and possibly a presentation).
Risk Analysis Approach	SysTrust audit is conducted for one IT asset (system) at a time.	OCTAVE is a focused approach in which critical IT assets are addressed first. Usually, first OCTAVE exercise will evaluate organization practices and analyze risks of several critical IT assets. Later Octave-based TRAs will analyze risks of other IT assets based on their criticality.
	Only applicable for IT systems/applications.	OCTAVE can apply to different types of IT assets: Hardware (e.g. a UNIX server), System, Software, Information, and people (e.g. individual or team).
	SysTrust audit is built around evaluating existence of IT controls in a manner similar to a checklist.	OCTAVE-based TRA is based around evaluating and analyzing risks, impacts, and probabilities.
	SysTrust can not be modified unless with revision from AICPA and CICA.	OCTAVE is flexible. It can be tailored for most organizations as well as IT assets.
	SysTrust audit is divided into five domains (security, availability, processing integrity, online privacy, and confidentiality). Each of these domains is divided into four areas: policies, communications, procedures, and monitoring. Each of these four areas has a list of criteria with each criteria has a list of illustrative controls. Hence a SysTrust audit is well defined and structured.	OCTAVE provides a high level approach of how to conduct risk analysis. As for controls: 1. OCTAVE contains a catalog of practices which is usually being completed for all IT assets. This catalog of practices is divided into strategic and operational practices. 2. OCTAVE provides a high-level generic threat profile template for an IT asset. These templates are: Human actors using network access, human actors using physical access, system problems, and other problems.
	SysTrust audit evaluates effectiveness of IT controls from a information security perspective.	OCTAVE-based TRAs analyzes risks of IT assets from an information security perspective.
	There are no calculations in a SysTrust audit.	Octave is based on calculating risks. Risks calculation is a function of both impact/consequence and probability. Risk calculation can be either qualitative or quantitative. Quantitative risk calculation requires significant amount of calculations and some statistical calculations for the probability/likelihood.
	SysTrust is usually one time a year audit exercise.	OCTAVE methodology promotes a process approach in which IT assets are analyzed in an ongoing basis. Risk profiles are updated each year or when a significant change occurs; these updated profiles might result in different risk calculations/findings hence ending up with new set of recommendations. OCTAVE calls to continue conducting IT risk assessment for next critical IT assets that have not been assessed before.

	All needed controls should be in place and working for at least 2 months for the system to pass a SysTrust audit.	Missing controls can be corrected or implemented right away if identified as action items while mitigation plans might take more time to be implemented. Though, the OCTAVE-based TRA is completed by the delivering the final analysis and recommendation report. No need to wait for implementation of recommendations.
Who can perform it?	Only licensed Certified Public Accountant by AICPA and CICA can perform a SysTrust audit.	Octave-based TRAs can be performed by: internal resources, external vendor/consultant, or combination of both. Ideally, OCTAVE-based TRAs is self-directed; A small team of people from the operational (or business) units and the IT department work together to analyze risks of IT asset(s) as internal resources understand their IT asset nature, dynamics, dependencies, and history. Though, external vendors/consultants might be helpful for first time TRAs or complex-asset TRAs.
Cost	100 K CAD for initial SysTrust 50 K CAN for annual renewal	Cost depends on resources performing OCTAVE-based TRAs. Internal resources will tend to cost less. An average Octave-based TRA conducted by external consultant will cost around 15-20 K CAN.
Time factor	SysTrust seal of assurance is valid for one year and it needs to be renewed each year. Initial SysTrust audit for a web application/system might range from 6 months to 2 years depending on organization and system readiness for SysTrust (Figures are based on Government of Alberta departments past experience)	A time to conduct Threat Risk Assessment activity (TRA) based on OCTAVE defer based on the IT asset type as well as who is conducting the TRA (i.e. internal or external resources). A typical TRA for a web application can take around 3 months.
Others	SysTrust is a more objective exercise as the CPA assigned to conduct the audit is independent entity which is external to the organization.	If conducted with internal resources only, OCTAVE-based TRA calculations and subsequently findings might be biased based on information provided by internal participants. To mitigate this risk, OCTAVE-based TRAs should: 1. Include equal representation from all classes of internal stakeholders in the evaluations (e.g. business and IT staff, management and staff, development and support, ... etc). 2. TRA exercise to have an objective facilitator.
	SysTrust is a snapshot in time that addresses only couple of IT assets under SysTrust Audit. Once the SysTrust seal is awarded, the CPA will wait for one year to perform the next SysTrust audit regardless of changes to IT system during this period. Though, management of the IT system who was awarded SysTrust seal signs an agreement with AICPA/CICA that they will maintain the same controls that were in place during the SysTrust audit.	TRA is a process: 1. It will establish timelines/schedule to assess IT assets and when to re-assess them 2. It will be part of any new IT project or major change to existing IT assets hence making sure to assess impact of changes on existing risk profile. This means that OCTAVE-based TRAs will be part of the IT processes for development and ongoing support and maintenance.

	SysTrust audit does not include usually any technical assessment. For example, it does not include vulnerability assessment.	OCTAVE calls for a vulnerability assessment part of its approach. This can be done by either a security scanning tool (e.g. Nessus) or by technology checklists (e.g. Oracle database checklist).
	SysTrust mainly fulfil management and customers needs. SysTrust provides assurances about IT systems/applications. This assurance is mainly based with financial needs in mind.	TRAs (based on any information security risk methodology) are required by: 1. SysTrust states "A risk assessment is prepared and reviewed on a regular basis or when a significant change occurs in either the internal or external physical environment" 2. Office of the Auditor General of Alberta states in General Computer Controls Report has allocated one control objective "2.1 Assessment of Risks".

APPENDIX B: OCTAVE-S SECURITY PRACTICES MAPPING TO SYSTRUST CONTROLS

OCTAVE-S Security Practice Statement	SysTrust Criteria/Illustrative Controls
1. Security Awareness and Training	
Staff members understand their security roles and responsibilities. This is documented and verified.	S 2.2.2 A 2.2.2 PI 2.2.2 C 2.2.2 C 2.2.3
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g. logging, monitoring, or encryption), including their secure operation. This is documented and verified.	S 1.2.j S 3.9 S 3.10.4 A 1.2.j A 3.12 A 3.13.4 PI 1.2.j PI 3.13 PI 3.14.4 C 1.2.j C 3.12 C 3.13.4
Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	S 2.2.3 S 2.4.2 S 2.5 A 2.2.3 A 2.4.3 A 2.5 PI 2.2.3 PI 2.4.2 PI 2.5 C 2.2.4 C 2.4.2 C 2.5
Staff members follow good security practice, such as: ==> securing information for which they are responsible ==> not divulging sensitive information to others (resistance to social engineering) ==> having adequate ability to use information technology ha	Note 7
2. Security Strategy	
The organization's business strategies routinely incorporate security considerations.	Note 6
Security strategies and policies take into consideration the organization's business strategies and goals.	Note 6
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Note 6

3. Security Management								
Management allocates sufficient funds and resources to information security activities.	S 3.10.4	A 3.9.8	A 3.13.4	A 4.2.2	PI 3.14.4	PI 4.2.2	C 3.13.4	
Security roles and responsibilities are defined for all staff in the organization.	S 1.3	S 3.9.1	S 3.11.1	A 1.3	A 3.2.3	A 3.12.1	A 3.14.1	PI 1.3
	PI 3.13.2	PI 3.15.1	PI 3.18.3	C 1.3	C 3.12.1	C 3.14.1		
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Note 7							
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	S 1.1.1	S 1.2	A 1.1.1	A 1.2	PI 1.1.1	PI 1.2	C 1.1	C 1.2
	C 3.1	C 3.2						
The organization's hiring and termination practices for staff take information security issues into account.	S 3.9	A 3.12	PI 3.13	C 3.12	S 3.1.C.4	A 3.4.C.4	PI 3.5.C.4	C 3.4.C.4
The organization manages information security risks, including: ==> assessing risks to information security. ==> Taking steps to mitigate information security risks.	C 3.3.6	C 4.1	C 3.8.7	A 3.6.6	A 3.11.7	A 4.1	A 3.1	
	PI 3.7.6	PI 4.1	C 3.6.6	C 3.11.7	C 4.1			
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	C 3.3.6	C 4.1	C 3.8.7	A 3.6.6	A 3.11.7	A 4.1		
	PI 3.7.6	PI 4.1	C 3.6.6	C 3.11.7	C 4.1			

4. Security Policies and Regulations								
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	S 1.1	S 1.2	A 1.1	A 1.2	PI 1.1	PI 1.2	C 1.1	C 1.2
There is a documented process for management of security policies, including: ==> creation ==> administration (including periodic reviews and updates) ==> communication	S 1.1	S 2.3	A 1.1	A 2.3	PI 1.1	PI 2.3	C 1.1	C 2.3
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	S 4.1	S 4.2	A 4.1	A 4.2	PI 4.1	PI 4.2	C 4.1	C 4.2
The organization uniformly enforces its security policies.	Note 1							

5. Collaborative Security Management				
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including: ==> protecting information belonging to other organizations ==>	C 3.1.3	C 3.3.1	C 3.8	Note 3
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.	S 2.2	A 2.2	PI 2.2	C 2.2
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	A 3.3	Note 3		
The organization has policies and procedures for collaborating with all third-party organizations that: ==> provide security awareness and training services N/A ==> develop security policies for the organization N/A ==> develop contingency plans for the o	Note 3			

6. Contingency Planning/Disaster Recovery	
An analysis of operations, applications, and data criticality has been performed.	A 3.2
The organization has documented, reviewed, and tested: ==> contingency plan(s) for responding to emergencies. ==> disaster recovery plan(s) ==> business continuity or emergency operation plans.	A 3.2
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	A 3.1.8
All staff are: ==> aware of the contingency, disaster recovery, and business continuity plans. ==> understand and are able to carry out their responsibilities	A 3.2

7. Physical Access Control					
If staff from your organization is responsible for this area:					
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	S 3.2	A 3.5	PI 3.6	C 3.5
There are documented policies and procedures for managing visitors.	Note 1			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	A 3.1			
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	S 3.2	A 3.5	PI 3.6	C 3.5
If staff from a third party is responsible for this area:				
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	Note 3			
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	Note 3			

8. Monitoring and Auditing Physical Security				
If staff from your organization is responsible for this area:				
Maintenance records are kept to document the repairs and modifications of a facility's physical components	A 3.1			
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.	Note 1			
Audit and monitoring records are routinely examined for abnormalities, and corrective action is taken as needed.	S 3.2.2	A 3.5.2	PI 3.6.2	C 3.5.2
If staff from a third party is responsible for this area:				
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	Note 3			
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	Note 3			

9. System and Network Management

If staff from your organization is responsible for this area:

There are documented and tested security plan(s) for safeguarding the systems and networks.	S 4.1	S 4.2	S 4.3	A 4.1	A 4.2	A 4.3	A 3.1	A 3.2
	PI 4.1	PI 4.2	PI 4.3	C 4.1	C 4.2	C 4.3		
Sensitive information is protected by secure storage (e.g. backups stored off site, discard process for sensitive information)	S 3.1	A 3.2	A 3.3	A 3.4	PI 3.5	C 3.4	C 3.1	C 3.2
	C 3.3							
The integrity of installed software is regularly verified.	S 4.1	A 4.1	PI 4.1	C 4.1				
All systems are up to date with respect to revisions, patches, and recommendations in security advisories.	S 3.10	A 3.13	PI 3.14	C 3.13				
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	A 3.2	A 3.3						
Changes to IT hardware and software are planned, controlled, and documented.	S 3.11	S 3.12	A 3.14	A 3.15	PI 3.15	PI 3.16	C 3.14	C 3.15
IT Staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. ==> Unique user identification is required for all information system users, including third-party access. ==> Default accounts and defa	Note 7							
Only necessary services are running on systems - all unnecessary services have been removed.	S 3.3.4	A 3.6.4	PI 3.7.4	C 3.6.4				
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.	S 3.3	A 3.6	PI 3.7	C 3.6				

If staff from a third party is responsible for this area:

The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	Note 3
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	Note 3

10. Monitoring and Auditing IT Security

If staff from your organization is responsible for this area:

System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.	S 3.3	S 4.1	S 4.2.1	A 3.6	A 4.1	A 4.2	PI 3.7	PI 4.1
	PI 4.2	C 3.6	C 4.1	C 4.2.1				
Firewall and other security components are periodically audited for compliance with policy.	S 3.3	S 3.10	A 3.6	A 3.13	PI 3.7	PI 3.14	C 3.6	C 3.13

If staff from a third party is responsible for this area:

The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	Note 3
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	Note 3

11. Authentication and Authorization

If staff from your organization is responsible for this area:

Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	S 3.1	A 3.4	PI 3.5	C 3.4				
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	S 3.1	S 3.3.1	A 3.4	A 3.6.1	PI 3.5	PI 3.7.1	C 3.4	C 3.6.1
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.	C 3.1	S 3.5	A 3.8	PI 3.9	C 3.8	Note 2		

If staff from a third party is responsible for this area:

The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization.	Note 3
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	Note 3

12. Vulnerability Management

If staff from your organization is responsible for this area:

There is a documented set of procedures for managing vulnerabilities, including: ==> selecting vulnerability evaluation tools, checklists, and scripts. ==> keeping up to date with known vulnerability types and attack methods. ==> reviewing sources of info	Note 1						
Vulnerability management procedures are followed and are periodically reviewed and updated.	Note 2						
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	C 3.3.6	C 4.1	C 3.8.7	A 3.6.6	A 3.11.7	A 4.1	Note 5
	PI 3.7.6	PI 4.1	C 3.6.6	C 3.11.7	C 4.1		

If staff from a third party is responsible for this area:

The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	Note 3						
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	Note 3						

13. Encryption

If staff from your organization is responsible for this area:

Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).	S 3.5	A 3.8	PI 3.9	C 3.8	PI 3.1.8	PI 3.1.9
Encrypted protocols are used when remotely managing systems, routers, and firewalls.	C 3.3.2	A 3.6.2	PI 3.7.2	C 3.6.2	Note 1	

If staff from a third party is responsible for this area:

The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	Note 3						
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	Note 3						

14. Security Architecture and Design

If staff from your organization is responsible for this area:

System architecture and design for new and revised systems include considerations for: ==> security strategies, policies, and procedures. ==> history of security compromise ==> results of security risk assessments	S 3.8	A 3.11	PI 3.12	C 3.11
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.	Note 1			

If staff from a third party is responsible for this area:

The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	Note 3
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	Note 3

15. Incident Management

If staff from your organization is responsible for this area:

Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	C 3.6	C 2.4	A 3.9	A 2.4	PI 3.10	PI 2.4	C 2.4	C 3.9
Incident management procedures are periodically tested, verified, and updated.	Note 2							
There are documented policies and procedures for working with law enforcement agencies.	Note 1							

If staff from a third party is responsible for this area:

The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	Note 3
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	Note 3

Mapping Notes:

1	OCTAVE-S Security practices statements are very specific or directly related to IT and Physical Security. The background of OCTAVE-S is IT/Physical Security while the background of SysTrust is Systems/Transactions. This is why we find many OCTAVE-S statements with no match or exact match in the SysTrust criteria and controls. (e.g. Working with Law Enforcement)
2	SysTrust concentrates on Policies administrative controls; in the sense of policies needs to be reviewed periodically and updated. It does not mention same administrative controls to other types of documents: standards, processes, procedures, and guidelines.
3	OCTAVE-S pays attention to outsourcing by adding a specific section in many security practices domains for "If staff from a third party is responsible for this area:"
4	Many SysTrust Illustrative Controls are duplicated in Security, Availability, Processing Integrity, and Confidentiality but with focus on that area (e.g. incidents/breaches).
5	Many SysTrust Illustrative controls are listed in more than one criteria in the same security domain (e.g. conduct periodic security reviews and vulnerability assessments)
6	SysTrust does not mention security strategy. This topic might be implied from the security policies section, though no specific mention of security strategy. SysTrust talks about a Backup and Restoration strategies only.
7	This security statement is difficult to measure. Some security indicators might provide relative information (e.g. number of security incidents with user as root cause).

APPENDIX C: APPLICATION THREAT PROFILE MAPPED TO SYSTRUST

Threat		Risks			SysTrust Mapping - Controls											
Id	Title	C	I	A												
1	Changing information/data without authorisation				S 3.1	A 3.4	PI 3.5	C 3.4	PI 3.1	PI 3.2	PI 3.3	PI 3.4	PI 3.10	PI 3.11	PI 3.17	A 3.10
					A 3.9											
2	Changing system privileges without authorisation				S 3.1	S 3.11	A 3.4	A 3.14	PI 3.2	PI 3.5	PI 3.15	C 3.4	C 3.14			
					A 4.1	A 4.2	PI 4.1	PI 4.2								
3	Computer viruses impact (Worms, Trojan Horses, Spyware, Adware)				S 3.4	A 3.7	PI 3.8	C 3.7	S 3.6	A 3.9	PI 3.10	C 3.9				
4	Cracking Encryption keys				S 3.5	A 3.8	PI 3.9	C 3.8	PI 3.1.8	PI 3.1.9						
5	Cracking passwords				S 3.1 b	A 3.4 b	PI 3.5 b	C 3.4 b	S 3.3	A 3.6	PI 3.7	C 3.6				
6	Damage to or loss of facility environmental control equipments				A 3.1	A 3.2	A 3.3	PI 3.17	PI 3.18	PI 3.19						
7	Damage to, or loss of, computer facilities				A 3.1	A 3.2	A 3.3	PI 3.17	PI 3.18	PI 3.19						
8	denial of service attacks				S 3.3	A 3.6	PI 3.7	C 3.6	S 3.6	A 3.9	PI 3.10	C 3.9	S 4.1	A 4.1	PI 4.1	C 4.1
9	Disclosure of business information				C 3.1	C 3.2	C 3.9	C 3.10	C 2.2	C 2.4						
10	Eavesdropping				S 3.5	A 3.8	PI 3.9	C 3.8	PI 3.1.8	PI 3.1.9						
11	Fruad				S 3.1	A 3.4	PI 3.5	C 3.4	PI 3.2	PI 3.4						
12	Hacking Activities (rootkits, malicious probes, defacing sites)				S 3.3	A 3.6	PI 3.7	C 3.6	S 3.6	A 3.9	PI 3.10	C 3.9	S 4.1	A 4.1	PI 4.1	C 4.1
13	Identity Theft				S 2.2	A 2.2	PI 2.2	C 2.2	S 3.6	A 3.9	PI 3.10	C 3.9				
14	IT staff mistakes				PI 3.1	PI 3.2	PI 3.3	PI 3.4	PI 3.10	PI 3.11	PI 3.17	A 3.10	A 3.9	A 3.1		
					S 3.11	S 3.12	A 3.14	A 3.15	PI 3.18	PI 3.19	C 3.14	C 3.15				
15	Loss of power				A 3.1	PI 3.17										
16	Malfunction of application software developed in-house				A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.12	A 3.15	PI 3.16	C 3.15	A 3.1	A 3.2	PI 3.17	PI 3.18

17	Malfunction of business application software acquired from a third party				A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.12	A 3.15	PI 3.16	C 3.15	A 3.1	A 3.2	PI 3.17	PI 3.18
18	Malfunction, Damage, or losss of computer / network equipment				A 3.1	A 3.2	A 3.3	PI 3.17	PI 3.18	PI 3.19	S 4.1	A 4.1	PI 4.1	C 4.1	PI 3.2	
					A 4.2	PI 4.2										
19	Malfunction of system software				A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.12	A 3.15	PI 3.16	C 3.15	A 3.1	A 3.2	PI 3.17	PI 3.18
20	Misusing systems to cause disruption				PI 3.1	PI 3.2	PI 3.3	PI 3.4	A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.6	A 3.9	PI 3.10	C 3.9
21	Modifying network traffic				S 3.5	A 3.8	PI 3.9	C 3.8	PI 3.1.8	PI 3.1.9						
22	Natural disasters				A 3.1	A 3.2	A 3.3	PI 3.17	PI 3.18	PI 3.19						
23	Not revoking access of terminated employees on time				S 3.1.c	A 3.4.c	PI 3.5.c	C 3.4.c								
24	Passwords disclosure (sharing it)				S 3.1 b	A 3.4 b	PI 3.5 b	C 3.4 b	S 3.3	A 3.6	PI 3.7	C 3.6	S 2.2	A 2.2	PI 2.2	C 2.2
25	Social engineering/Phishing				S 2.2	A 2.2	PI 2.2	C 2.2	S 3.6	A 3.9	PI 3.10	C 3.9				
26	Software changes without authorisation (installing, modifying, or deleting)				A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.10	A 3.13	PI 3.14	C 3.13	S 2.2	A 2.2	PI 2.2	C 2.2
27	Software Piracy				S 3.6	A 3.9	PI 3.10	C 3.9	C 3.1	C 3.2	C 3.9	C 3.10	C 2.2	C 2.4	S 2.2	A 2.2
					PI 2.2	C 2.2										
28	SPAM				S 2.2	A 2.2	PI 2.2	C 2.2	S 4.2	A 4.2	PI 4.2	C 4.2				
29	System/Network Performance (e.g. traffic load)				S 4.1	A 4.1	PI 4.1	C 4.1	S 4.2	A 4.2	PI 4.2	C 4.2				
30	Theft of authentication information (eg passwords)				S 3.6	A 3.9	PI 3.10	C 3.9	S 2.2	A 2.2	PI 2.2	C 2.2	S 3.1.b	A 3.4.b	PI 3.5.b	C 3.4.b
31	Theft of mobile computing and storage devices				S 3.6	A 3.9	PI 3.10	C 3.9	S 3.1	A 3.4	PI 3.5	C 3.4	C 2.2	C 2.4	S 2.2	A 2.2
32	Theft of proprietary business information/data				S 3.6	A 3.9	PI 3.10	C 3.9	C 3.1	C 3.2	C 3.9	C 3.10	C 2.2	C 2.4		

33	Unforeseen effects of change (software, system, user processes, information/data)				S 3.11	S 3.12	A 3.14	A 3.15	PI 3.18	PI 3.19	C 3.14	C 3.15	A 4.1	A 4.2	PI 4.1	PI 4.2							
					A 3.1	A 3.2																	
34	Unforeseen effects of change (network and facilities)				S 3.11	S 3.12	A 3.14	A 3.15	PI 3.18	PI 3.19	C 3.14	C 3.15	A 4.1	A 4.2	PI 4.1	PI 4.2							
					A 3.1	A 3.2																	
35	Unforeseen effects of changes to user processes or facilities				A 3.1	A 3.2	A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.12	A 3.15	PI 3.16	C 3.15									
36	Unforeseen effects of introducing new / upgraded business processes				A 3.1	A 3.2	A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.12	A 3.15	PI 3.16	C 3.15									
37	Unforeseen effects of change (organisational)				A 3.1	A 3.2	A 4.1	A 4.2	PI 4.1	PI 4.2	S 3.12	A 3.15	PI 3.16	C 3.15									
38	User mistakes				PI 3.1	PI 3.2	PI 3.3	PI 3.4	PI 3.10	PI 3.11	PI 3.17	A 3.10	A 3.9	A 3.1									
39	Working with inappropriate content (download, upload, email, handle)				S 2.2	A 2.2	PI 2.2	C 2.2	S 4.2	A 4.2	PI 4.2	C 4.2											

APPENDIX D: ORACLE DATABASE THREAT PROFILE MAPPED TO SYSTRUST

APPENDIX E: UNIX SERVER THREAT PROFILE MAPPED TO SYSTRUST