City of Milwaukee

Office of the Comptroller

W. Martin Morics, C.P.A.
Comptroller

Michael J. Daun
Deputy Comptroller

John M. Egan, C.P.A.
Special Deputy Comptroller

Craig D. Kammholz
Special Deputy Comptroller

April 13, 2012

To the Honorable Common Council
City of Milwaukee

Dear Council Members:

As a component of the Comptroller's comprehensive information systems audit work plan, Securance Consulting was engaged to complete the information systems (IS) risk assessment. The Comptroller's Office recently received the enclosed final report detailing the results of the information systems risk assessment. The assessment was performed by Securance in March 2012. This thorough risk assessment will serve as the foundation of the Comptroller's three year information systems audit plan. This report helps to identify, classify and risk rate the auditable technologies within the City's computing environment.

The most recent attempt at completing a citywide information systems risk assessment was carried out by KPMG and a report was delivered in December, 2008. While KPMG's work product was not an IS risk assessment this report (IT Internal Development Report) took a risk based approach in planning and recommending an IS audit plan for 2009-2011. The most recent full scale, high level IS risk assessment was conducted by Jefferson Wells who delivered a report in 2005. The City's IS infrastructure and IS divisional leadership have gone through extreme change in the last two years. High value divisions such as Police, Fire, ITMD, and DPW all have new IS leadership that are open to reducing IS risk; thus, the 2012-2015 three year IS audit plan needs to be based on a current risk assessment for the IT audit function to be used efficiently.

The risk assessment was based on ten risk categories: organizational reliance, commercial vs. developed applications, prior audit status, internal customer impact, external customer impact, system future life, security threat, level of administrative tasks, financial exposure and a recent major change.

Securance identified several high-level deficiencies in the City's IS operations and made recommendations that echo very similar deficiencies and recommendations from the previous IS risk assessments performed by KPMG and Jefferson Wells.

Securance deficiency statement:

"The Information Technology (IT) Security Posture of the City is weak. The governance of IT processes and security practices are not centralized, and the City has not adopted a formal framework (e.g. CoBIT, ITIL, etc.) for governing IT security or IT related practices. For the exception of the Employee Retirement System [ERS], none of the divisions or departments interviewed were able to produce a comprehensive set of IT policies and procedures governing security practices, and as a result there are inconsistencies in the manner in which the information technology assets of the City are managed.

Given the de-centralized model, there are also minimal opportunities for departments or divisions to share IT best practices designed to mitigate known security risks. In addition, it is our opinion that the City could realize significant cost savings by centralizing the IT environment and leveraging the use of available technologies and resources. Given the current structure of the IT environment, there may be opportunities to streamline the number of supported hardware and network devices, resulting in less man-hours required to manage the technologies and reduced hardware/network device upgrade/replacement costs."

Securance recommendation:

A. *Consider the addition of a Chief Information Security Officer (CISO)* – the City should consider the addition of a CISO. The CISO is responsible for establishing and maintaining the enterprise vision and strategy and program to ensure information assets are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks, responding to incidents, establishing appropriate standards and controls, and directing the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance.

B. *Centralize the Governance of Information Technology (IT) Management* - Determine the best department/division to provide global oversight of the information technology security posture (the security posture refers to all controls, policies and procedures in place to maintain a controlled operating environment). In our opinion, and based on our understanding of the City's environment, the department that should take on the responsibility of oversight would be ITMD (Information Technology Management Division). Alternatively, if the City opted to add a CISO, this responsibility would fall under the role of the CISO. It is important to note that the recommendation to centralize the Governance of IT Management of the City has been documented and formally communicated to the City by two (2) other independent IT Audit Security firms prior to our assessment.

C. *Adopt a Best Practice IT Governance Framework* - Once the City has

designated a division/department to take responsibility over the governance of IT management, the responsible party should then assess Best Practice IT Governance frameworks and formally adopt and implement the controls defined within the framework. The City must give the designated division/department the authority to implement the IT Governance Framework. It is our opinion, and based on our experience with multiple other cities, counties and federal organizations, that the City should adopt either the CoBIT or ITIL frameworks; these frameworks are globally accepted best practices and have been adopted and are in use by a large number of government agencies within the United States.

The Comptroller strongly agrees with the recommendation to create a Chief Information Security Officer and to endow this position with City-wide IS security responsibility as well as enforcement authority.

The second recommendation concerning the centralization of information technology governance should be carefully evaluated and considered by a cross functional working group established by the City Information Management Committee. At a minimum the working group should consist of representatives from ITMD, DPW Infrastructure, Fire Department, Police Department, Budget Office, Mayor's Office, various departments throughout the City and be headed by a member of the Common Council. The working group should evaluate which IS operations and functions may be centralized and which would not be centralized with strong consideration given to the complexity of the current technology environment and the current need for customized IT operations within various divisions. The working group would report their conclusions and recommendations regarding IT centralization to the Mayor and Common Council.

The Comptroller agrees with the third recommendation concerning the adoption of a "best practice IT governance framework." This framework, once selected can only be implemented and enforced by a designated department/division with the authority to do so. Currently there is not a department/division with the authority and enforcement responsibilities to carry out the implementation of an IT governance framework. The CIMC established working group would also consider how an IT governance framework could be adopted and implemented.

The Comptroller thanks all parties involved in this assessment for their time and enthusiastic participation.

Sincerely,

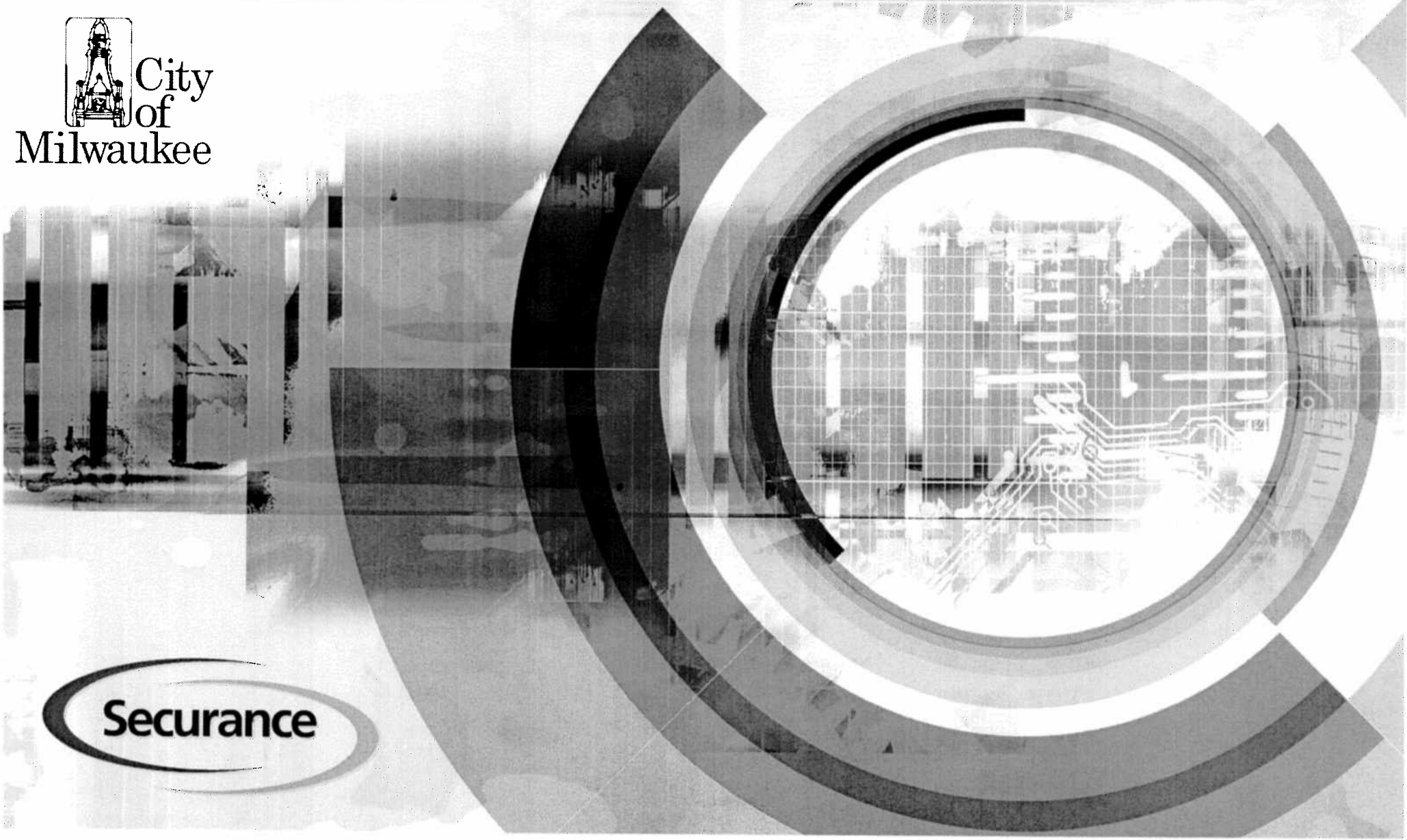
Michael J. Daun
Deputy Comptroller

CC: Tom Barrett, Mayor
CC: Nancy Olson, CIO

City of Milwaukee

Information Systems Risk Assessment

March 2012



City of Milwaukee

Securance

Risk-Based Security Planning

City of Milwaukee

Risk Assessment - is a process of estimating a risk score to be associated with each auditable technology. Risk assessments are typically undertaken to focus attention on significant areas, to allocate scarce resources to the most important areas and to help with prioritizing decisions such as frequency, intensity and timing.

The criteria used to assign risk scores are as follows:

- Corporate Reliance
- Vanilla vs. Heavily Customized
- Prior Audit
- Internal Customer Impact
- External Customer Impact
- Financial Exposure
- Security Threat
- Level of Administrative Tasks
- Recent Major Change
- Future Life

This points out that the level of risk associated with each auditable technology is based on multiple factors. Additionally, the risk score alone may not be a sufficient basis for making an audit planning decision. It may be necessary to factor in the cost of carrying out the audit as it relates to the relative risk an organization is willing to assume.

The general opinion, with respect to *Audit Frequency*, is that the riskier technologies should be assessed more frequently. This matrix is a guide that should be used in conjunction with a conditional audit frequency approach. Under a conditional frequency approach, all key technologies are monitored for signs of major changes. Examples of major changes include significant upgrades, reconfigurations and/or the addition of a large number of users.

Audit intensity should be determined by assessing the qualifications of the resources and the complexity of the technology. Generally, the more complex the technology, given the same level of staff skills, the more detailed the audit.

Audit timing is another component to be considered during planning. Again, audit planning is heavily dependent upon resource availability. A variety of approaches have been used to determine when audits should be scheduled. Fixed time audits are based on the assumption that there are fixed times that are best suited to conduct the audit; whereas, random timing audits are more unpredictable and may be used to motivate IT personnel to maintain their controls and procedures at reasonable levels.

Frequency, intensity, timing and *resources* are key components that should be considered when using the Technology Risk Matrix.

Securance

Introduction & Scope

During the first fiscal quarter of 2012, The City of Milwaukee's (COM) Internal Audit (IA) department engaged Securance Consulting to perform an IT risk assessment of the auditable technologies and processes deployed and implemented to protect the city's information assets. The objectives of the IT risk assessment were to: 1) better assess and understand the IT systems that store, process or transmit organizational information, and 2) enable management to make well-informed decisions related to implementing risk management techniques and processes, including IT audits.

The scope of this review included critical technology departments and their systems including all significant applications, interfaces, databases and operating system technologies and IT processes. The risk assessment focused on auditable technologies and IT processes and was not intended to be a comprehensive examination of the entire information systems function.

Approach & Methodology

The approach and methodology for performing the risk assessment included gaining an understanding of the COM's diverse IT environment to identify auditable technologies and processes. Internal Audit and IT Management selected applicable risk categories to assess each auditable technology/process against. Key personnel were interviewed independently to obtain risk ratings. Individual ratings were entered into a proprietary risk assessment engine for analysis.

Technologies/processes were prioritized based on the following scale:

- High Risk – score between 50 – 39 (recommended action within Year 1 of the audit plan);
- Medium Risk - score between 29 – 38 (recommended action within Year 2 of the audit plan); and
- Low Risk - score of 28 or less (presents less risk, consider higher priority items for Year 3 of the audit plan).

The remaining sections of the report include:

- Audit planning recommendations (see page 4);
- A three (3) - year IT audit plan;
- Listing of technology risk by category;
- Listing of auditable technologies (with risk score) by department/division;
- Category definitions and rating factors; and
- Appendix A - Modules of DPWAPP Application.

Audit Planning Recommendations

City of Milwaukee

Audit Planning Recommendations

The audit planning recommendations provided below are based on the results of the risk assessment analysis, our IT audit experience, and interviews of the following business personnel (presented by City Department/Division):

Internal Audit
- Isaak Lerner, Senior Information Systems Auditor

Treasurer
- Jim Klaybor, City Treasurer
- Joe-Marr Hooper, Deputy City Treasurer
- Carrie Urban, Special Assistant to the City Treasurer
- Lee Matthias, Business System Coordinator
- Bob Jorin, Netwok Coordinator Associate

Clerk's Office
- Jim Owczarski, Deputy City Clerk
- Kimberly Berry, Network Administrator

Comptroller
- Beverly LaFlex, Accounting Manager

Employee Retirement System
- Kelly Reid, CTO
- Marty Matson, Deputy Director
- Jay Patel, Program Manager

Fire Department
- Debbie Wilichowski, Technical Services Manager
- John Pederson, Administrative Captain
- Gerard Washington, Assistant Chief - Support Bureau

Health
- Jeff Hussinger, Telecommunications Analyst
- Yvette Rowe, Business Operations Manager

ITMD
- Nancy Olson, Chief Information Officer

Municipal Court
- Jane Tabaska, Network Manager
- Kristine Hinrichs, Chief Court Administrator

Police
- Kim Yung, Information Systems Manager
- Chuck Burki, Information Systems Director

Water
- Dick Rasmusen, Water Revenue Manager
- Eldin Gardsky, Network Manager
- Micheal Schaefer, Water Security Manager

Based on the result of the opinion-based risk assessment and knowledge of the COM's information technology operating environment, the following technology projects and/or audits should be scheduled to reduce the greatest technology risks currently being assumed by the COM:

Information Technology Security Posture

Finding

The Information Technology (IT) Security Posture of the City is weak. The governance of IT processes and security practices are not centralized, and the City has not adopted a formal framework (e.g. CoBIT, ITIL, etc.) for governing IT security or IT related practices. For the exception of the Employee Retirement System [ERS], none of the divisions or departments interviewed were able to produce a comprehensive set of IT policies and procedures governing security practices, and as a result there are inconsistencies in the manner in which the information technology assets of the City are managed. Given the de-centralized model, there are also minimal opportunities for departments or divisions to share IT best practices designed to mitigate known security risks.

Audit Planning Recommendations (continued)

Information Technology Security Posture - Finding (continued)

In addition, it is our opinion that the City could realize significant cost savings by centralizing the IT environment and leveraging the use of available technologies and resources. Given the current structure of the IT environment, there may be opportunities to streamline the number of supported hardware and network devices, resulting in less man-hours required to manage the technologies and reduced hardware/network device upgrade/replacement costs.

Risk

The current decentralized model increases the risk of an IT security breach and/or disruption of IT resources. In addition, the lack of global oversight of IT assets and processes presents the City with unnecessary difficulty identifying, understanding and addressing areas of high-risk.

Recommendation

We recommend that the City consider the following action items to address the risks identified above:

A. *Consider the addition of a Chief Information Security Officer (CISO)* – the City should consider the addition of a CISO. The CISO is responsible for establishing and maintaining the enterprise vision and strategy and program to ensure information assets are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks, responding to incidents, establishing appropriate standards and controls, and directing the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance.

Typically, the CISO's influence reaches the whole organization. Responsibilities include:

- Information security and information assurance;
- Information regulatory compliance;
- Information risk management;
- Information technology controls for financial and other systems;
- Information privacy;
- Computer Emergency Response Team / Computer Security Incident Response Team;
- Identity and access management;
- Information security architecture;
- IT investigations, digital forensics, eDiscovery;
- Disaster recovery and business continuity management; and
- Information Security Operations Center ISOC.

Having a CISO or the equivalent function in the organization has become a standard in most business, government and non-profit sectors.

Audit Planning Recommendations (continued)

Information Technology Security Posture - Recommendation (continued)

B. *Centralize the Governance of Information Technology (IT) Management* - Determine the best department/division to provide global oversight of the information technology security posture (the security posture refers to all controls, policies and procedures in place to maintain a controlled operating environment). In our opinion, and based on our understanding of the City's environment, the department that should take on the responsibility of oversight would be ITMD (Information Technology Management Division). Alternatively, if the City opted to add a CISO, this responsibility would fall under the role of the CISO.

   It is important to note that the recommendation to centralize the Governance of IT Management of the City has been documented and formally communicated to the City by two (2) other independent IT Audit Security firms prior to our assessment.

C. *Adopt a Best Practice IT Governance Framework* - Once the City has designated a division/department to take responsibility over the governance of IT management, the responsible party should then assess Best Practice IT Governance frameworks and formally adopt and implement the controls defined within the framework. The City must give the designated division/department the authority to implement the IT Governance Framework.

   It is our opinion, and based on our experience with multiple other cities, counties and federal organizations, that the City should adopt either the CoBIT or ITIL frameworks; these frameworks are globally accepted best practices and have been adopted and are in use by a large number of government agencies within the United States.

   - *The CoBIT Framework* - the framework provides good practices across a domain and process framework. The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor. It is positioned at a high level and has been aligned and harmonized with other, more detailed, IT standards and good practices such as COSO, ITIL, ISO 27000, CMMI, TOGAF and PMBOK. COBIT acts as an integrator of these different guidance materials, summarizing key objectives under one umbrella framework that link the good practice models with governance and business requirements.
   - *ITIL* - The Information Technology Infrastructure Library (ITIL), is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific, but can be customized and used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance with IT best practices and to measure improvement.

   Centralization of the role of IT Governance and adoption of the a best practice framework will significantly improve the overall IT security posture of the City.

Audit Planning Recommendations

City of Milwaukee

Audit Planning Recommendations (continued)

Based on the result of the opinion-based risk assessment and knowledge of the City's information technology operating environment, the following technology projects and/or audits should be scheduled to reduce the greatest technology risks currently being assumed by the City:

- *Perform a comprehensive audit over the Case Tracking System (CATS) system* – This project should focus on reviewing the security of the application and technologies supporting the CATS application (i.e. platforms, databases).
- *Perform a comprehensive audit over the Laboratory Information System (LIS)* – This project should focus on reviewing the security of the application and technologies supporting the LIS application (i.e. platforms, databases).
- *Perform a comprehensive assessment of the general controls security posture of the City* – This project should focus on assessing the policies (where available) and more importantly, the procedures in place to manage general computing controls. As mentioned in the previous finding, we are aware of the weaknesses within the general control environment, so we suggest that general controls testing should be performed using a best practice methodology (e.g. CoBIT or ITIL) and specific and actionable recommendations should be provided.
- *Perform a comprehensive audit over the Inovah system* – This project should focus on reviewing the security of the application and technologies supporting the Inovha application (i.e. platforms, databases).
- *Perform a comprehensive audit over the 911 Emergency System application* – This project should focus on reviewing the security of the application and technologies supporting the 911 Emergency System application (i.e. platforms, databases). In addition, the application should be assessed for controls around any data that may be considered sensitive. Note: The 911 Emergency System has not been audited by the Internal Audit department or any other audit agency.
- *Perform a comprehensive audit over the TRACS system* – This project should focus on reviewing the security of the application and technologies supporting the TRACS application (i.e. platforms, databases). In addition, the application should be assessed for controls around any data that may be considered sensitive.
- *Perform a comprehensive audit over the CAD and RMS systems* – This project should focus on reviewing the security of the application and technologies supporting the CAD and RMS systems (i.e. platforms, databases). In addition, the applications should be assessed for controls around any data that may be considered sensitive.
- *Perform a comprehensive PeopleSoft Financials Audit* – This project should focus on reviewing the security of the critical PeopleSoft modules and technologies supporting the PeopleSoft application (i.e. platforms, databases, and interfaces). The scope of the audit should be limited to those areas not audited by the organization's external audit firm (e.g. general computing controls - backup and recovery, physical security, etc.) in order to ensure duplicate audit efforts do not occur.
- *Perform a comprehensive audit over the Chili application* – This project should focus on reviewing the security of the application and technologies supporting the Chili application (i.e. platforms, databases). In addition, the application should be assessed for controls around any data that may be considered sensitive.

Proposed IT Audit Plan

City of Milwaukee

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DEPARTMENT|DIVISION	DESCRIPTION	Risk Score	Y1	Y2	Y3
1	Application	Case Automated Tracking System (CATS)	Municipal Court	Case Tracking System	50.0	1		
2	Application	Inovah	Treasurer	Cashier System	46.4		1	
3	Database	Oracle 10g	Municipal Court	Supporting CATS and MMCIS	46.0	1		
4	Application	LIS	Health	Laboratory Information System	45.0	2		
5	IT Process	Mobile Device Management	DPW	Blackberry Enterprise software	45.0	3		
6	Application	LIRA	Clerk	Business License Management Application	44.0			
7	Application	Intranet	Police	Publishes information internally	43.0			
8	Application	TRACS	Police	Mobile MDC access for citation and accident submission to State, MPD and courts (Municipal/Circuit)	43.0		3	
9	Application	MERITS	ERS	Public Pension Administration System	43.0			
10	Database	Oracle	Clerk	Supporting LIRA	43.0			
11	Application	CRM System	ITMD	Citizen Relationship Management System	42.5			
12	Application	Chili	Health	Licensing and Inspection	42.0			3
13	Application	RMS	Police	Tiburon Records Management System	42.0	2		1
14	Application	PeopleSoft Financials	Comptroller	PeopleSoft Financials System	41.0			2
15	Application	CAD	Police	includes AVL	41.0			1
16	Application	Sharepoint	Police	Sharepoint Servers	41.0			
17	Application	Media Solve	Police	Citizen | Arrest Information Tracking System	41.0			
18	Application	WinAce	Police	Evidence Management	41.0			
19	Database	SQL	Fire	Supports (New CAD, RMS)	40.7			1
20	Application	911 System	Fire	911 Emergency System	40.7		2	
21	Application	EnQuesta	Water	City Services Billing Application	40.5			
22	Application	Tax Collection System	ITMD	Tax Collection System	40.0			
23	Database	Adabase	ITMD	Supports the Tax Collection System	40.0			
24	Platform/Servers	Unix (Solaris & Linux)	Police	Media Solve, OpenSky	40.0			
25	IT Process	IT Asset Management	DPW	Manage HW, SW, laptops, desktops, purchasing	40.0	3		
26	IT Process	Desktop Management - Windows 7	DPW	Manage configuration of desktop and laptop systems	40.0	3		
27	IT Process	Change | Patch Management	DPW	Change management all systems	40.0	3		
28	IT Process	Configuration Management	DPW	Configuration management (network and systems)	40.0	3		

Securance

Proposed IT Audit Plan

City of Milwaukee

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DEPARTMENT|DIVISION	DESCRIPTION	Risk Score	Y1	Y2	Y3
29	IT Process	Data Center Controls (Phy & Envir)	DPW	Physical and environment data center controls	50.0	3		
30	IT Process	Email Usage, Archival, and Retention	DPW	Email usage, archival, and retention	46.4	3		
31	IT Process	Monitoring & Logging	DPW	Incident | event logging and automated audit trails	46.0	3		
32	IT Process	Software Development (SDLC)	DPW	Application development life cycle methodology	45.0	3		
33	IT Process	Software License Compliance	DPW	Software license compliance	45.0	3		
34	IT Process	Virus Protection	DPW	Enterprise virus protection	44.0	3		
35	Application	PeopleSoft HR/Payroll	Comptroller	PeopleSoft HR/Payroll Application	43.0			
36	Application	CAD	Fire	Computer Aided Dispatching System	43.0			
37	Application	InCar Video	Police	In Car Video System	43.0			
38	Database	AIX	Health	Supporting LIS	43.0	2		
39	Database	SQL	Health	Supporting Chili, Stellar, Citiwatch, Practice Point Manager	42.5			3
40	Platform/Servers	Windows 2000	Police	CAD, RMS, Intellinetics, SenCrimes, WinAce	42.0			1
41	Platform/Servers	Windows 2003	Police	911 System, ALRP, Crimes, InCar Video, SharePoint, TRACS, iWatch	42.0		3	
42	Database	Oracle	Fire	Supports (Old CAD, RMS, EIS)	41.0			
43	IT Process	SAN	ITMD	iScuzzy & FiberChannel	41.0			
44	Application	Tax Collection System	Treasurer	Tax Collection System	41.0			
45	Application	Milwaukee Municipal Court Case Information System (MMCCIS)	Municipal Court	Non-Confidential Case Information	41.0			
46	Application	Group Life Insurance	ERS	GLI Application	41.0			
47	Database	SQL	Police	911 System, AFIS, ALPR, Crimes, InCar Video, Intellinetics, Sharepoint, TRACS, WinAce, iWatch	40.7		3	
48	Application	Itron Meter Reading Software	Water	Meter Reader	40.7			
49	Application	ALPR	Police	License plate recognition System	40.5			
50	Application	SenCrimes	Police	Sensitiv Crim Databae	40.0			
51	Database	FileMaker	Police	SenCrimes	40.0			
52	Platform/Servers	RS6000	Water	Supporting EnQuesta	40.0			
53	Platform/Servers	Windows 2008	Fire	Supports (New CAD, RMS)	40.0			
54	Application	Scanners Docments	ERS	Imaging System	40.0			
55	Application	Active Directory	All Divisions	Network Authentication	40.0			
56	Database	Oracle DB	ITMD	Supporting HRMS, FMIS	40.0			2

Securance

Proposed IT Audit Plan

City of Milwaukee

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DEPARTMENT|DIVISION	DESCRIPTION	Risk Score	Y1	Y2	Y3
57	Application	File Server (All)	All Divisions	Internal File Servers	34.4			
58	Application	AFIS	Police	Fingerprint System, includes Fast ID	34.0			
59	Application	Crimes	Police	Crime Application	34.0			
60	Application	iWatch	Police	Citizens recording events System	34.0			
61	Database	Oracle	Police	Supports CAD/RMS and Media Solve	34.0			
62	Database	SQL Server 2000	ERS	MERITS, Cmers.com, Member Self Server	34.0			
63	Application	Nice Recording System	Fire	Call Recording System	33.8			
64	Platform/Servers	Windows 2008	Municipal Court	Supporting CATS and MMCIS	33.0			
65	Application	Control Pro	Police	Door Security going to be replaced	32.0			
66	Database	Access	Police	Control Pro	32.0			
67	Network Appliances	Internet Load Balancers - Commercial	DPW	Internet Load Balancers	32.0			
68	Application	Bentley Microstation	Water	Maintains design and GIS information	31.6			
69	Application	Practice Point Manager	Health	Billing Software (Medicaid, Title 19)	31.0			
70	Application	911 System	Police	includes freedom call check	31.0			
71	Application	GPS SQL Server	ERS	Lump Payment Processing (Global Pensions)	31.0			
72	Application	Asterisk	DPW	Voicemail Service	31.0			
73	Application	SymPro Portfolio Management System	Treasurer	Investment Portfolio System	30.6			
74	Platform/Servers	Windows 2003	Fire	Supports (Old CAD, RMS, EIS)	30.4			
75	Application	MS Exchange Server	All Divisions	Email	30.1			
76	Platform/Servers	RedHat Enterprise	Fire	Supports Nice Recording System	30.1			
77	Application	HR Plus!	Health	Positions | Training | HR Tracking	30.0			
78	Application	Open Sky	Police	LMR System	30.0			
79	Database	Oracle	Water	Supporting Bentley, EnQuesta, and SCADA	30.0			
80	Platform/Servers	Windows 2003	ERS	Supporting ERS Applications	30.0			
81	Platform/Servers	Windows 2008	ERS	Supporting ERS Applications	30.0			
82	IT Process	IT Training - Internal/External	DPW	Internal consistency, educate external on IT risk and processes	30.0			
83	IT Process	Helpdesk	DPW	End user support	30.0			
84	IT Process	Access Management	DPW	Network and application access management	30.0			

Proposed IT Audit Plan

City of Milwaukee

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DEPARTMENT|DIVISION	DESCRIPTION	Risk Score	Y1	Y2	Y3
85	IT Process	Backup | Restore	ITMD | DPW	Veritas Backup Exec	30.0			
86	IT Process	IT Governance	DPW	IT governance (risk assessment and IT policies)	30.0			
87	IT Process	IT Security Management	DPW	Internal | external vulnerability assessments and penetration tests	30.0			
88	IT Process	Job Scheduling	DPW	Batch job scheduling	30.0			
89	Application	EIS	Fire	EMS|Fire Reporting System	29.8			
90	Application	PeopleSoft Access	ERS	Financials and HR	29.5			
91	Application	Ccure	Water	Physical Security Software for Water Sites	29.0			
92	Application	BadgePro	Police	Id Card System - Employees and Photos for bartenders etc.	29.0			
93	Database	Progess	Water	Supporting Ccure	29.0			
94	Platform/Servers	Windows 2003	Health	Supporing File Servers, Chili, Stellar, Practice Point Manager	29.0			3
95	Application	CityTime	DPW	City-Wide Timekeeping Application	28.5			
96	Application	Communications Manager	DPW	Phone System	28.5			
97	Application	Telestaff	Fire	MFD Roster|Payroll|HR Records App	28.2			
98	Application	GRANICUS	Clerk	Legislative Management Suite	28.0			
99	Application	Citwatch	Health	Electronic Communications System	28.0			
100	Application	Intellinetics	Police	Document Imaging System	28.0			
101	Database	SQL Anywhere	Fire	Supports Telestaff	28.0			
102	Network Appliances	Avaya Layer 3	DPW	Routers & Switches	28.0			
103	Application	Stellar	Health	CDC Data Management System	27.0			
104	Application	RSEnergy	Water	Energy Monitoring and Reporting Software	27.0			
105	Application	FTP	ERS	B2B Communication	27.0			
106	Application	City's Internal Website	DPW	City's Internal Website	27.0			
107	Application	City's External Website	DPW	City's External Website	27.0			
108	Database	SQL	Clerk	Supporting Granicus	27.0			
109	Database	SQL	Water	Supporting RSEnergy, RSMACC, and SCADA	27.0			
110	Platform/Servers	Windows 2003 - GIS system too	Water	Supporting RSEnergy, RSMACC, and Bentley	27.0			
111	Network Appliances	Avaya Layer 2	DPW	Routers & Switches	27.0			
112	Application	SCADA (Supervisory Control and Data Acquisition)	Water	Controls Water Plant Operations	26.5			

Securance

Proposed IT Audit Plan

City of Milwaukee

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DEPARTMENT|DIVISION	DESCRIPTION	Risk Score	Y1	Y2	Y3
113	Database	Oracle	DPW	Supporting AutoProcess, LUKE, Parking Applications, Asterisk, CityTime, Communications Manager, Internal | External Websites.	26.5			
114	Platform/Servers	Windows 2008	Water	Supporting SCADA	26.5			
115	Application	Northwoods	ITMD	Web Content Management System	26.0			
116	Application	CMERS.COM	ERS	Access Portal	26.0			
117	Application	AutoProcess	DPW	Parking Ticket Application	26.0			
118	Application	LUKE	DPW	Parking Pay Stations	26.0			
119	Application	Parking Structures	DPW	Parking Structure Pay Stations	26.0			
120	Database	SQL Server Databases	ITMD	Supports Email Archive	26.0			
121	Database	SQL	DPW	Supports Voicemail Application	26.0			
122	Platform/Servers	Windows 2003	DPW	DPW Domain Cluster Servers 1-5	26.0			
123	Platform/Servers	Windows 2003	DPW	Database Servers	26.0			
124	Application	RSMACC	Water	Proprietary Change Management for PLC Programming	25.0			
125	Application	DPW Website	DPW	DWP Website (hosted by AT&T)	25.0			
126	Application	DPWAPP - Mulitple Modules (Defined in Appendix A)	DPW	Multi-Module Java Applications (See Appendix A)	25.0			
127	Platform/Servers	Windows 2008	Clerk	Supporting Lira & Granicus	25.0		2	
128	Platform/Servers	Windows 2003	DPW	Phone System	25.0			
129	IT Process	SAN	Water	Storage Area Network	25.0			
130	Platform/Servers	Windows 2003	DPW	VoiceMail Servers	24.5			
131	Platform/Servers	Windows 2003	DPW	Webserver	24.0			
132	Network Appliances	SONET	DPW	SONET Backbone	24.0			
133	Application	OpenSource Monitoring Tool	DPW	Monitors Up/Down Time of Servers	23.0			
134	Application	Telecom Expense Management	DPW	Internal Phone Billing System	23.0			
135	Database	SQL	DPW	Supports Public Website	23.0			
136	Network Appliances	Firewalls Security & Management	DPW	OpenSource Tools	23.0			
137	Application	ACCPAC	ERS	General Ledger	22.0			
138	Platform/Servers	Windows 2003	DPW	Network Attached Storage Servers	22.0			
139	Platform/Servers	Windows 2003	DPW	Infrastructure Servers	22.0			
140	Network Appliances	DNS, NTP, DHCP, etc.	DPW	OpenSource Network Services	22.0			

Securance

Proposed IT Audit Plan

City of Milwaukee

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DEPARTMENT|DIVISION	DESCRIPTION	Risk Score	Y1	Y2	Y3
141	Application	Northern Trust	ERS	Asset Custodian - Compliance Monitoring Tool	21.0			
142	Platform/Servers	Windows 2003	DPW	DPW Applications Servers	21.0			
143	Platform/Servers	Windows 2003	DPW	Monitor Servers	20.0			
144	Platform/Servers	Windows 2003	DPW	Primary File Servers	20.0			
145	IT Process	Disaster Recovery (IT)	DPW	IT disaster recovery	20.0			
146	Application	Legal Docs	ERS	Research Tool	19.0			
147	Application	Zypher Investment Research Tool	ERS	Investment Research Tool	19.0			
148	Application	Bloomberg	ERS	Investment Tool	19.0			
149	Application	LanGuard	DPW	Languard - Software Compliance	19.0			
150	Platform/Servers	Windows 2003	DPW	DPW Domain Cluster Server 6-9	19.0			
151	Platform/Servers	Windows 2003	DPW	DPW Printer/Desktop Management	19.0			
152	Platform/Servers	Windows 2003	DPW	Name Server	19.0			
153	Application	High Speed Printer	ERS	Payroll (Pension System)	18.5			
154	Platform/Servers	Windows 2003	DPW	Parking Server(s)	18.0			
155	Network Appliances	Wireless Access Point	DPW	Wireless Access Controller	17.0			
156	Application	ARIS	ERS	Research Tool	16.0			
157	Network Appliances	Time Source - Commercial	DPW	Network Synchronization	16.0			
158	Application	Tracker	ERS	Change Management System	14.5			

* *Based on the risk priorities, we have identified three (3) audits per audit year prioritized based on the definitions below. Where there are multiple technologies listed for an audit, it is our opinion that audit efficiencies can be gained and/or the technologies support each other and/or a process.*

1: Recommended highest audit priority for listed year.
2: Recommended second-highest audit priority for the listed year.
3: Recommended third-highest audit priority for listed year.

Securance