Risk Assessment

IT Controls and Policies	Impact Scale		IT Risks								Compos Risk Sc and Lev	
			Quality of IT Controls		Availability		Integrity		Confidentiality			
	L	I	L	I	L	I	L	I	L	I		
Access Control Policies	3	3	2	1	3	2	3	3	3	3	26	H
IT Security and Governance	3	2	2	2	3	2	1	2	1	1	20	M
IT Change Management	1	2	1	2	2	1	1	1	2	2	15	L
Strategic Plan and Governance	2	2	1	1	2	1	2	1	2	2	16	L
L= Likelihood I = Impact												

The four areas I selected for improvement are the Access Control Policies, IT Security and Governance, IT Change Management, and Strategic Plan and Governance. I have selected these policies for further review because of the lack of or partial implementation of proper procedures as defined by the internal city audit reports and recommendations. It is imperative that we correct these deficiencies as directed by the audit and recommendations as soon as possible to mitigate any potential future damages or breaches.

My risk assessment illustrated above explains the severity of the situations and why the proper implementation is important to the city of Atlanta. The Access control policies are very severe and need correcting as soon as possible. The IT Security and Governance is moderately severe and should be resolved quickly. The IT Change Management and Strategic Plan and Governance are low-risk and mildly severe so they should not be resolved as urgently as the above two IT controls and policies.

The Access Control Policies are what allows access to the systems containing sensitive data. What we should do. The complete lack of Access Control Policies could spell disaster for affected companies and systems in regards to assets and reputation. Quality of IT controls should this occur is not as big of a factor in regard to day to day operation, but should still be followed up on. The availability, integrity, and confidentiality of all data stored within is completely vulnerable to any attempt at accessing the system without these policies reinforced.

The recommended procedures that should be implemented: Ensure all accounts are checked for legitimacy and follow proper security protocols and password policies. Any

illegitimate accounts should be permanently locked. This should be followed up with one year after implementation.

The IT Security and Governance are focused on specialized on-site training for professionals working with these systems and establishing a relationship with the city of Atlanta's Department of Information Technology. To maintain the quality of our IT controls and the integrity of the systems, these individuals working with these systems need to be able to know how to maintain the systems or have close access to the Department of Information Technology.

The recommended procedures that should be implemented: training, including confidentiality training for sensitive data and establishing a working relationship with the Department of Information Technology. This should be followed up with two years after implementation.

The IT Change Management is how involved from the onset of implementation that higher ups and people that make decisions are with the systems. Being available and establishing how integral the systems are, should a disaster strike, the IT Department should be able to swiftly make decisions and to further development of policies and procedures to address future concerns. Integrity and confidentiality of sensitive data are not a huge concern here, as management would not likely be directly interfacing with the systems containing sensitive data, although proper confidentiality training should be given as directed.

The recommended procedures should be implemented: Inclusion of key stakeholders and members of management when systems are implemented, establishing a direct relationship to expedite decisions should a disaster strike, and proper confidentiality training should someone have access to sensitive data. This should be followed up with two years after implementation.

The Strategic Plan and Governance addresses needs of the city's systems. Failure to have a proper plan could hamper day to day work should a disaster strike. quality, accessibility, and integrity of systems are low-risk here. Confidentiality is of moderate risk though because lack of a strategic plan should a disaster strike could lead to the loss of sensitive information.

The recommended procedures should be implemented: The chief information officer should update the strategic plan to reflect the city's current needs, while anticipating future needs. This should be followed up with three years after implementation.

I look forward to your future success with the implementation of these control and security policies per my risk assessment.

-James Shannon