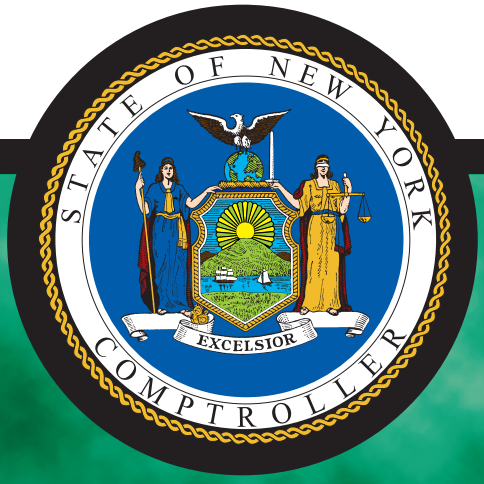
Office of the New York State Comptroller
Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability

LOCAL GOVERNMENT MANAGEMENT GUIDE

Information Technology Governance



Thomas P. DiNapoli State Comptroller

Table of Contents

Many local governments and school districts invest a considerable amount of resources in information technology (IT) including computers and related equipment, software and costs related to Internet access and personnel training. They rely on IT systems for storing important financial and nonfinancial information, accessing the Internet, communicating through email and reporting to State and federal agencies. These systems and the data they hold are valuable and need to be protected from unauthorized, inappropriate and wasteful use. Protecting IT assets is especially important as the number of instances of people with malicious intent trying to harm computer networks or gain unauthorized access to information through the use of viruses, malware and other types of attacks continues to rise.

Although no single practice or policy on its own can adequately safeguard your technology investment, there are a number of controls that, if appropriately implemented and monitored, collectively increase the odds that your systems and data will remain safe. Management, including the governing board, is responsible for ensuring that the right IT controls are in place, and that they are performing as intended. Given the rapid pace of technological innovation, the ever increasing sophistication and number of threats facing computer systems and the fact that IT is only one aspect of management's responsibilities, this can be a formidable task.

The following guidance is intended to make the oversight of information technology less daunting by providing a template for understanding and strengthening controls over IT. It includes a Security Self-Assessment structured around 12 key areas of IT security that is intended to help you exercise effective oversight of IT operations and serve as a starting point for discussions with personnel who are responsible for the day-to-day management of your computer operations. Since the assessment is geared toward small- to medium-sized computer operations, we limited the number of questions; there are many more questions you could and possibly should ask about your IT internal controls.

Although no single practice or policy on its own can adequately safeguard your technology investment, there are a number of controls that, if appropriately implemented and monitored, collectively increase the odds that your systems and data will remain safe.

Responsibility for IT Internal Controls

Internal controls over IT seek to ensure that computer systems and the data they process, transmit and store can be trusted, are available when needed, and are adequately protected from unauthorized access and use.

Internal controls are essential to the effective operation of local governments and school districts. They encompass the policies, procedures and activities designed to provide reasonable assurance that operations are going according to plan. In general, properly designed and functioning controls reduce the likelihood that significant errors or fraud will occur and remain undetected. Internal controls over IT seek to ensure that computer systems and the data they process, transmit and store can be trusted, are available when needed, and are adequately protected from unauthorized access and use.

The governing board's responsibilities for internal controls primarily involve oversight, authorization and ethical leadership. Generally, governing boards do not design internal controls or develop the written policies they adopt. The governing board relies upon management, primarily the chief executive officer (CEO), to create the policies needed to ensure that services are provided effectively and assets are safeguarded. The CEO in turn relies upon managers and department heads to recommend and implement procedures. Some local governments and school districts employ an IT vendor for assistance with IT internal controls.

An important way that governing boards fulfill their oversight responsibilities is by asking questions related to controls over financial and IT systems. Depending on how IT responsibilities are assigned, those questions might be directed to the CEO, IT manager, department head(s), or an IT vendor. Asking the right questions is not only an effective way to exercise oversight, it can be done at little or no cost. On the other hand, not asking the right questions may potentially expose computer systems, software and data to loss or unauthorized use, which could prove to be very expensive.

It is understandable that someone with little or no IT knowledge might be apprehensive about asking questions concerning IT internal controls. However, a governing board has responsibility for the oversight of the organization's IT operations – whether or not its members are knowledgeable about computers or feel comfortable discussing IT. As you will note after reviewing the IT Governance Security Self-Assessment included at the end of this document, a background in IT is not necessary to ask questions about key IT internal controls and understand the answers. Extensive IT knowledge is also not necessary to perform certain procedures (e.g., review documents or reports) that can corroborate the answers to the self-assessment questions and help you understand the controls better.

Introduction to IT Security Fundamentals

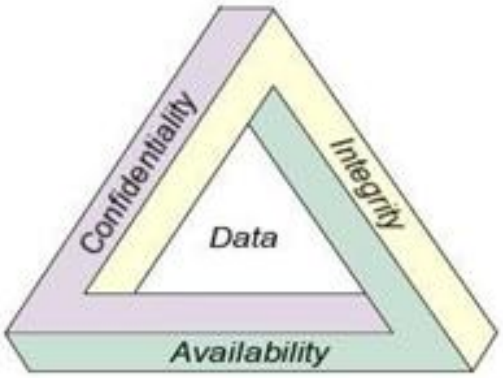
Prior to examining your organization's IT internal controls, it is important to understand two concepts that are fundamental to how IT professionals approach data, network and system security: the CIA triad and defense-in-depth. These concepts highlight the importance of looking at controls both individually and collectively and will help you place the internal controls in context.

The CIA triad is a well-known model in information security development. It is applied in various situations to identify problems or weaknesses and to establish security solutions.

CIA Triad

The CIA triad refers to an information security model made up of three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security. The CIA triad is a well-known model in information security development. It is applied in various situations to identify problems or weaknesses and to establish security solutions. The model is an industry standard with which most information systems professionals should be familiar.

- **Confidentiality** is closely linked with privacy and relates to preventing or minimizing unauthorized access to and disclosure of data and information. To ensure confidentiality, information must be organized in terms of who ought to have access to it as well as its sensitivity.



- **Integrity** is focused on ensuring that data is not tampered with during or after submission. Having accurate and complete data is essential for good decision-making. What good is the information if it cannot be trusted?

- **Availability** means that the information is available when it is needed. Data that cannot be accessed will prove to be of little value. The most available systems are accessible at all times and have safeguards against power outages, natural disasters, hardware failures, systems upgrades, and attempts by individuals with malicious intent to cause disruption.

Building successive layers of defense mechanisms can reduce the risk of a successful attack by someone with malicious intent and is considered a best practice by IT security professionals.

Defense-in-depth

Defense-in-depth refers to the implementation of multiple layers of security to protect data, networks and systems. Building successive layers of defense mechanisms can reduce the risk of a successful attack by someone with malicious intent and is considered a best practice by IT security professionals. A combination of controls helps ensure that your system does not become overly dependent on any one control or layer of security and provides added protection in case a layer of security fails to function properly or does not prevent or stop a threat to your data or system. There is no single control that can be used to adequately protect against today's sophisticated threats; only a combination of multiple preventive and detective controls will keep your data and systems safe.

Information Technology Governance: Security Self-Assessment

The Security Self-Assessment at the end of this document addresses key areas of IT internal controls such as policy, training, access and monitoring. Several of the main questions include follow-up questions that will provide information helpful for evaluating the answers. For example, one of the questions is, "Were all computer users provided IT security training?" The question is followed by a prompt to record the date(s) of training and who attended, if applicable. If all computer users were provided with IT security training but that training occurred six years ago, the governing board may want to consider arranging for additional training or a refresher in the near future. Likewise, if only a small handful of computer users have received IT security training, the governing board should be aware of that as well.

Some questions are followed by a suggested step you can take to verify and better understand the answer provided. For example, if an up-to-date list of computer equipment is maintained, you could obtain a copy of the inventory listing and review it for reasonableness (i.e., does the inventory make sense given what you know about the organization and its operations). This would help you assess whether the list is truly up-to-date. For example, if the inventory of computer equipment does not include any laptop computers yet you have observed local government or school district staff working on laptop computers, you may want to ask a follow-up question about the apparent omission from the records. Similarly, when completing the access controls section of the assessment, you could review a current list of authorized computer users and their levels of access. If names on the list are unrecognizable or if the list contains individuals no longer employed by the organization, you could ask appropriate follow-up questions. In addition, questions about access to particular software applications may arise. For example, a member of the governing board may notice that someone with no accounting responsibilities has access to the organization's accounting program.

Since computing environments change over the course of time, governing boards should periodically review IT controls. We recommend that this be done at least once a year.

The following guidance will help you to understand each control on the self-assessment and why it is important to the security and oversight of your computer operations. It should be noted that the manner in which the answers to the questions are obtained is up to the governing board. Board members could interview the IT manager or IT vendor (if applicable) in person and ask follow-up questions or obtain additional information for clarification purposes at that time. Alternatively, the governing board could give the self-assessment to the appropriate responsible parties and ask that they complete and return it. In any event, the governing board will probably need to speak with IT personnel to ask additional questions, obtain more details regarding the answers provided and discuss the next steps to be taken. Since computing environments change over the course of time, governing boards should periodically review IT controls. We recommend that this be done at least once a year.

IT Security: Top 12 Areas of Concern

Area #1 – IT Policy

Computer policies define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations.

Computer policies define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations. The governing board should provide important oversight and leadership by establishing computer policies that take into account people, processes and technology; communicating the policies throughout the organization and ensuring there are procedures in place to monitor compliance with policies.

Your unique computing environment should dictate the content and number of policies necessary. A small entity with uncomplicated, modest computing resources may only need a few policies to cover relevant computing issues adequately. Larger entities with complex systems may need several policies to convey management's expectations and ensure effective operation. While computer policies will not guarantee the safety of your computer system, a lack of appropriate policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

Possible types of computer policies include but are not limited to:

- **Breach Notification Policy –** New York State Technology Law (State Technology Law) requires municipalities and other local agencies to have a breach notification policy or local law.[1] Such policy or local law must require that notification be given to certain individuals when there is a breach of the security of the system as it relates to private information. If you fail to adopt an information breach notification policy and private information is compromised, officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.

- **Internet, Email, and Personal Computer Use –** This policy should describe what constitutes appropriate and inappropriate use of IT resources, along with your expectations concerning personal use of IT equipment and user privacy (e.g., management reserves the right to examine email,

[1] Section 208 (8) of the State Technology Law requires municipalities and other local agencies to have adopted a breach notification policy or local law consistent with the requirements contained in Section 208 by April 6, 2006. Pursuant to Section 208, notification is required to be given to certain individuals when there is a "breach of the security of the system" as it relates to "private information." "Breach of the security of the system" is generally defined as meaning unauthorized acquisition of computer data which compromises the security, confidentiality or integrity of personal information maintained by the entity. "Private information" is defined as personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password which would permit access to an individual's financial account.

personal file directories, web access and other information stored on local government computers, at any time and without notice). It should also describe the consequences for policy violations (e.g., an employee found to have violated the policy may be subject to disciplinary action, up to and including termination of employment).

- **Use of and Access to Personal, Private, and Sensitive Information –** This policy should define personal, private and sensitive information (PPSI); explain the entity's reasons for collecting PPSI; and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities.
- **Password Security –** This policy should address password complexity, length, age requirements, reuse of old passwords and the number of failed log-on attempts the system will allow.
- **Wireless Security Policy –** This policy should specify the conditions that wireless devices must satisfy to connect to the organization's network. The policy should also indicate who is covered by the policy (e.g., all employees, contractors, consultants, temporary and other workers) and describe the consequences of violating the policy.
- **Mobile Computing and Storage Device Policy –** The purpose of this policy is to control mobile computing and storage devices that contain or access your information resources. It should define the devices covered (e.g., organizationally owned or personally owned), procedures for reporting lost or stolen mobile computing and storage devices, the process used for gaining approval before connecting new devices to the system and other user responsibilities.
- **Online Banking –** Before an organization begins processing financial transactions electronically, it should have a comprehensive policy that addresses online banking activities. The policy should include the following, consistent with the statutory and other legal responsibilities of the officers and employees involved:
  - what online banking activities will be used
  - what specific transaction types will be allowed
  - who will authorize transactions
  - who will record transactions/transfers
  - who has access to online banking
  - who will review and reconcile transfers, and how often
  - the procedures that will be followed when responding to potential fraudulent activity.

While computer policies will not guarantee the safety of your computer system, a lack of appropriate policies significantly increases the risk that data, hardware, and software systems may be lost or damaged by inappropriate access and use.

Area #2 – IT Security Training and Awareness

IT security training should explain the proper rules of behavior for using your IT systems and data, and communicate the policies and procedures that need to be followed.

A well-informed work force is the strongest link in the chain to secure electronic data and computer systems. Entities cannot protect the confidentiality, integrity and availability of their data and systems without ensuring that the people who use and manage IT understand organizational IT security policies and procedures and their roles and responsibilities related to IT security. While the IT policies tell computer users what to do, cybersecurity training provides them with the skills to do it.

There have been many accounts of users whose actions caused significant harm to computer systems or financial losses. They may have been fooled, via social engineering scams,[2] into providing their passwords, opening harmful attachments or visiting malicious websites. Even system administrators, who are typically regarded as having advanced IT knowledge, have been tricked into performing actions that threatened or caused harm to their systems. The success of social engineering, coupled with the never-ending flow of new and innovative threats, underscores the importance of including all users in IT security training. It is also important to update the training material periodically to address new technologies, threats and any changes to your computing environment.

IT security training should explain the proper rules of behavior for using your IT systems and data, and communicate the policies and procedures that need to be followed. The content of training programs should be directed at the specific audience (e.g., user or system administrator) and include everything related to IT security that attendees need to know in order to perform their jobs. IT security awareness efforts should reinforce your IT policies and training and can focus attention on security in general or some narrow aspect of security (e.g., the dangers of opening an unknown email or attachment, or how to maintain laptop security while traveling).

The failure to provide IT security training and raise awareness increases the risk that users will not understand their responsibilities, putting the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse. For example, without training and awareness, officers and employees may not be prepared to fulfill their legal obligation to notify affected individuals when personal, private or sensitive information is compromised.

[2] Social engineering refers to the methods attackers use to deceive victims into performing an action such as opening a malicious webpage or running an unwanted file attachment. Many social engineering efforts are focused on tricking users into disclosing usernames or passwords.

Local officials sometimes say that they cannot afford the cost of IT security training and awareness. Fortunately there are a number of no-cost or low-cost solutions available from a variety of sources. The following organizations offer free or low-cost IT security training and awareness materials:

Center for Internet Security
https://www.cisecurity.org/

Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/

New York State Office of Information Technology Services
https://www.its.ny.gov/

New York State Office of the State Comptroller
http://www.osc.state.ny.us/

TEEX Domestic Preparedness Campus
https://teex.org/Pages/homeland-security.aspx

United States Computer Emergency Readiness Team
https://www.us-cert.gov/

Municipal and school district associations (e.g., New York Conference of Mayors, New York State School Boards Association) also periodically offer low-cost cybersecurity training. Lastly, developing and delivering IT security training, and maintaining IT security awareness, does not have to be an elaborate, expensive endeavor. It can be as simple as gathering staff together to review your policies collectively and having a roundtable discussion on security matters applicable to your computing environment. The discussions could center on emerging trends in information theft and other social engineering reminders; limiting the type of personal, private and sensitive information collected, accessed or displayed to that which is essential for the function being performed; malicious software; virus protection; the dangers of downloading files and programs from the Internet; passwords; Wi-Fi security; or how to respond if a virus or an information security breach is detected. Awareness efforts could also include disseminating the free security alerts from the organizations mentioned above, or sending out periodic security reminders via email that address some aspect of your IT security policy.

IT security training and awareness is an essential part of protecting computer systems and data. Your personnel should understand their IT responsibilities, be knowledgeable about potential threats and be prepared to respond appropriately to everyday computing challenges, as well as less frequent events such as the loss of personal information. The growing availability and ease of obtaining free and low-cost training and awareness materials eliminates any excuse for not having a well-informed work force.

Your personnel should understand their IT responsibilities, be knowledgeable about potential threats and be prepared to respond appropriately to everyday computing challenges, as well as less frequent events such as the loss of personal information.

Area #3 – Computer Hardware, Software, and Data Inventories

Since different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored.

Organizations should maintain detailed, up-to-date inventory records for all computer hardware, software and data. The information maintained for each piece of computer equipment should include a description of the item including the make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the acquisition date. Software inventory records should include a description of the item including the version and serial number, a description of the computer(s) on which the software is installed and any pertinent licensing information.

In addition to hardware and software inventories, organizations should maintain an inventory of information assets (i.e., data) that classifies the data according to its sensitivity and identifies where the data resides (e.g., servers, workstations and laptops). Since different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored. Data classification is the process of assigning data to a category that will help determine the level of internal controls over that data. In some instances, laws, regulations or an organization's policies predefine the classification of each data type. Here is an example of a data classification scheme:

- **Public –** Information that is widely available to the public through publications, pamphlets, web content and other distribution methods.

- **Internal Use –** Routine operational information that is not approved for general circulation and where unauthorized access, modifications or disclosure would be inconvenient but would not result in financial loss or damage to public credibility. Examples include routine correspondence, employee newsletters, internal phone directories and internal policies and procedures.

- **Confidential –** Confidential data is information that, in the event of unauthorized access, modifications or disclosure, could result in significant adverse impacts on an organization's ability to perform critical work or compromise the integrity of the organization, its employees, its customers or third parties. Examples include data used to produce payroll or vendor payments, preliminary drafts of bid specifications, and employee system passwords. It also includes any information concerning a person that can be used to identify, or assume the identity of, the individual. Examples include Social Security numbers and the combination of name, address and date of birth.

- **Restricted Confidential –** Information where loss, unauthorized modification or disclosure is likely to result in the most serious impacts to an organization's ability to fulfill its responsibilities. Examples include the organization's strategy for defending lawsuits, preliminary investigation results and assessments of security vulnerabilities.

Organizations cannot properly protect their computer resources, including data, if they do not know what resources they have and where those resources reside. The failure to maintain detailed, up-to-date hardware, software, and information inventory records exposes these valuable assets to an increased risk of loss, theft, or misuse. Without proper identification of all devices on a network, unauthorized devices and software can be easily introduced, putting organizational data at risk. A single compromised device can become a launching point for further network attacks, quickly turning one compromised machine into many. Furthermore, accurate inventory records are essential for effective patch management (see Area #6 – Patch Management) and software licensing compliance.[3] Poor records makes it unlikely that software patches necessary to address known security vulnerabilities can be applied on a timely basis, if at all. In addition, insufficient records increase the likelihood that you may inadvertently violate copyright laws by having more software users than licenses for a particular application and incur penalties as a result. The accuracy of inventory records should be verified through periodic physical inventories.

The failure to maintain detailed, up-to-date hardware, software, and information inventory records exposes these valuable assets to an increased risk of loss, theft, or misuse.

[3] Software typically comes with a license that grants end-users permission to use one or more copies of the product. Organizations commonly closely track their license usage to help ensure they don't inadvertently utilize software in a manner that might constitute copyright infringement. The illegal use or distribution of software, also known as software piracy, can result in considerable penalties.

Area #4 – Contracts for IT Services

In our experience, many of the IT contracts or service level agreements (SLAs) organizations enter into are vague in terms of the services contracted for and the expected quality of those services.

Local governments and school districts increasingly rely on third parties to provide a variety of IT-related services. For your protection and to avoid potential misunderstandings, there should be a written agreement between your organization and the IT service provider that clearly states your organizational needs and expectations including those relating to the confidentiality and protection of personal, private and sensitive data and specify the level of service to be provided by the vendor. In our experience, many of the IT contracts or service level agreements (SLAs) organizations enter into are vague in terms of the services contracted for and the expected quality of those services. Such poorly worded agreements can, among other things, contribute to confusion over who has responsibility for various aspects of the IT environment (i.e., the organization or contractor), which ultimately puts the organization's data and computer resources at greater risk for unauthorized access, misuse or loss.

The components of an SLA vary but can include identification of the parties to the contract; definitions of terminology; term/duration of agreement; scope/subject; limitations (what, if anything, is excluded); service level objectives and performance indicators; roles and responsibilities; nonperformance impact; pricing, billing and terms of payment; security procedures; audit procedures; reporting; review/update and approvals. Generally speaking, the more specific the SLA, the better; there should be no uncertainty about what the contractor will deliver, when it will be delivered and how much it's going to cost. A vague agreement can lead to additional costs or cost increases you were not expecting.

An SLA should establish measurable targets of performance so a common understanding of services can be achieved. For example, if you contract with an IT vendor to administer patch management with the goal of ensuring that patches and updates that are released throughout the year are installed on a timely basis, the SLA should indicate exactly what operating system(s) and application(s) are covered and what "timely" means (e.g., is the expectation that patches be applied as soon as available, on a weekly basis or on a quarterly basis?). An SLA with a cloud service provider could, for example, indicate that you will have availability to an application 99.95 percent of the time and allow the municipality to reduce its payment by a given percentage if that is not achieved.

In addition, it is very important for local governments and school districts to know who (IT vendor(s) or their sub-contractor(s), if any) has access to its personal, private and sensitive information, and to then convey the organization's security expectations to the vendor(s) through the written contract(s). Any legal requirements relating to the protection of specific type(s) of data, for example, health-related information, should also be considered, discussed with the vendor and included in the contract, as appropriate. Local governments should also consult New York State Archives[4] guidance prior to entering into contracts, especially those relating to data storage services.

Many IT service providers have standard SLAs – reflecting various levels of service at different prices – that can be a good starting point for negotiation. SLAs should be reviewed by the organization's legal counsel and IT staff, as appropriate. They should also be periodically reexamined, especially if your IT environment or needs change significantly. Developing a good SLA takes some effort, but can help avoid potentially costly misunderstandings and establish an efficient, secure computing environment.

In addition, it is very important for local governments and school districts to know who (IT vendor(s) or their sub-contractor(s), if any) has access to its personal, private and sensitive information, and to then convey the organization's security expectations to the vendor(s) through the written contract(s).

Area #5 – Virus Protection

Malicious software, or malware, are software programs that are designed to harm computer systems. These programs can wreak havoc on both systems and electronic data by, for example, deleting files, gathering sensitive information such as passwords without the computer user's knowledge and making systems inoperable. Computer users can inadvertently install malware on their computers by many methods including opening email attachments, downloading content from the Internet or merely visiting infected websites. Damage caused by malware can be expensive to fix and can cause significant losses in productivity until corrected.

One way to detect and stop some forms of malware before it can affect its targets is through the use of antivirus software. Antivirus software should be installed and kept current with signature (a set of characteristics also referred to as virus definitions) and software updates. Antivirus definitions should be updated daily and set to scan for threats throughout the day. Without current virus definitions, protection is limited and leaves computers at risk of being compromised by new types of threats.

[4] **http://www.archives.nysed.gov/**

These programs can wreak havoc on both systems and electronic data by, for example, deleting files, gathering sensitive information such as passwords without the computer user's knowledge and making systems inoperable.

Some organizations use a mix of purchased and free antivirus software (downloaded from the Internet). While there is nothing inherently wrong with using different kinds of antivirus software, it may make timely, coordinated management of antivirus protection more challenging. The use of free antivirus software should be carefully considered. Due to the nature of the free license agreements, most free antivirus software is for home use only.

In addition, some malicious programs are written to automatically propagate, or spread across, any new system they discover. Because malware can be embedded onto a wide variety of devices, a best practice is to force scans of any new devices connected to computers, such as flash drives and digital cameras, and disable the autoplay feature for such devices.

Area #6 – Patch Management

A "patch" is software that is used to correct a problem, such as a security vulnerability, that exists within an application or an operating system. Security vulnerabilities in software can be exploited to infect a computer with a virus, spyware or other malicious agents or to gain access privileges illicitly. When security vulnerabilities in software are discovered, the software vendor typically issues a free patch (fix) to correct the problem.

Patches should be applied as soon as possible to reduce the likelihood that someone with malicious intent could successfully exploit a known vulnerability. You should adopt patch management policies and procedures that ensure that all patches and updates are rolled out on a regular basis.

Area #7 – Access Controls

Computer access controls prescribe who or what computer process may have access to a specific computer resource, such as a particular software program or database. For example, access controls can be implemented to limit who can view electronic files containing employee names and Social Security numbers. The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources. The objectives of limiting access are to ensure that outsiders (e.g., attackers) cannot gain unauthorized access to your systems or data, access to sensitive resources such as operating systems and security software programs are limited to very few individuals who have a valid business need for such access and employees and contractors are restricted from performing incompatible functions or functions beyond their responsibilities.

The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources.

There should be written procedures in place for granting, changing and terminating access rights to the overall networked computer system and to specific software applications. These procedures should establish who has the authority to grant or change access (e.g., department manager approval) and allow users to access only what is necessary to complete their job duties. Access rights should be updated as necessary; inactive, retired, or terminated accounts should be disabled or removed from the network in a timely manner.

You should periodically compare the employee master list (as maintained by the personnel or payroll department) to the list of network user accounts to determine if user accounts belong to current employees. A review of all system accounts should be periodically conducted and any account that cannot be associated with an authorized user or application should be disabled. Furthermore, you should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or vendor. After an account is disabled, any files associated with that account should be moved to a secure file server for analysis by IT or management personnel. Where possible, system administrators should monitor attempts to access disabled accounts through audit logging.

To help ensure individual accountability within the network, each user should have his or her own network account (username and password). Likewise, to help ensure individual accountability within software applications, each user should have his or her own user account (username and password). If users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Access should be assigned within the network based upon what resources a user needs to complete their job duties.

Access should be assigned within the network based upon what resources a user needs to complete their job duties. For example, if there are shared folders on the network, a user within the highway department should only have access to the folders he or she needs, which would most likely not include the personnel department's folders. Likewise, someone with accounting duties should only have access to the portion of your financial accounting system he or she needs to perform their job.

Users should be able to set their own passwords. If passwords are set for users, there is limited accountability because someone else knows the password.

Holding passwords to certain requirements makes passwords more difficult to crack or be easily guessed. Here are some criteria you should consider with regard to passwords:

- **Complexity Requirements**–A complex password should contain at least one uppercase character, one lowercase character, one numeric character and one special character (e.g., %, #, @) and not include names or words that can be easily guessed or identified using a password-cracking mechanism or dictionary. Furthermore, the password should not contain any part of the account, network or municipality names.
- **Length**–Passwords should be sufficiently long; that is, at least eight characters in length. Passwords longer than eight characters may provide greater security, but those benefits could be offset by people having to write down the password in order to remember it.
- **Aging–**Passwords should be changed periodically, about every 30 to 90 days. The more sensitive the system or data involved, the more frequently passwords should be changed.
- **Reuse of Old Passwords–**Organizations should consider placing limitations on the reuse of old passwords.
- **Failed Log-On Attempts–**To prevent password guessing and online password attacks, failed log-on attempts should be limited to three to seven consecutive attempts.

Area #8 – Online Banking

There has been a significant increase in fraud involving the exploitation of valid online banking credentials. Some of the more popular types of electronic fraud targeting online banking that have emerged are phishing attacks[5] and malware.[6] In a typical scenario, the targeted user receives an email which either contains an infected attachment or directs the recipient to a malicious website. Once the recipient opens the attachment or visits the website, malware containing a key logger or other data harvesting and reporting mechanism is installed on their computer, or the user is prompted to input their username and password, which are collected for malicious use. A key logger is a small application that harvests login information, allowing the perpetrator to masquerade as the legitimate user or create another user account. Thereafter, fraudulent electronic cash transfers are initiated and directed to bank accounts in the United States or foreign countries.

Despite online banking establishments' security controls, there is no way to absolutely guarantee the safety of online banking. The tactics used to commit fraud can range dramatically in sophistication and continually evolve over time. Likewise, there is no single control that is most effective against cyberattacks. A best practice for protecting IT systems and information is to build successive layers of defense mechanisms, a strategy referred to as defense-in-depth, a concept discussed earlier in this document.

Organizations should have both technology-based (e.g., up-to-date virus protection) and nontechnical controls (e.g., written policies and recurring information security awareness training for all employees who use computers connected to the Internet or the local government's network). Furthermore, although online banking fraud is often committed by external parties, risks posed by employees must also be considered. The ease and speed with which large amounts of money can be transferred between accounts and banks requires heightened attention to traditional internal controls, such as the proper segregation of duties and timely reviews of online banking transactions.

Organizations should have both technology-based (e.g., up-to-date virus protection) and nontechnical controls (e.g., written policies and recurring information security awareness training for all employees who use computers connected to the Internet or the local government's network).

[5] Phishing attacks use fake email messages pretending to represent a bank. The email requests information such as name, password and account number and provides links to a counterfeit website.

[6] Malware is malicious software that is typically installed without the user's knowledge or consent. Such programs can capture keystrokes for login information, monitor and capture other data to authenticate identity, generate web pages that appear to be legitimate but are not, and hijack a browser to transfer funds without the user's knowledge, among other things. Viruses, trojans and spyware are all examples of malware.

Since wireless networks are used as extensions of wired networks, even minor flaws in the configuration and implementation of a wireless segment can impact the security of an entire network.

Whenever possible, a wired rather than wireless network should be used for financial transactions. If a wireless network must be used, certain security measures should be in place (see Area #9 – Wireless Network). **It is also critical that bank accounts be monitored on a timely basis, at least every two or three days, for unauthorized or suspicious activity. Any suspicious activity should be immediately report to banking officials and/or law enforcement**. The window of time in which recoveries can be made from fraudulent online banking transactions is limited, and a rapid response may prevent additional losses.

Area #9 – Wireless Network

Wireless networks are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access and loss of data. However, they are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted into the air. These traveling signals potentially can be intercepted and exploited by individuals with malicious intent. Since wireless networks are used as extensions of wired networks, even minor flaws in the configuration and implementation of a wireless segment can impact the security of an entire network. A wireless environment, therefore, requires certain additional security precautions.

Although wireless environments and their related security systems can be quite complex, government personnel can implement effective controls with relative ease and without incurring additional costs. Some best practices relating to wireless technology include:

- Adopting written policies and procedures;
- Determining the optimal number, physical location and broadcasting power of wireless access points;
- Maintaining an inventory of and monitoring wireless access points;
- Changing the service set identifier (the SSID or name of the wireless network) using a naming convention that excludes identifiable information about the organization, the location, technology, manufacturer and type of data traversing the network;
- Requiring an access password for users and enabling the most sure encryption available (currently WPA2);

- Changing the default administrative password used by the administrator who set up the wireless access point;
- Updating and patching all software and hardware devices; and
- Considering other security controls that may be necessary given the organization's unique computing environment and security needs.

A further discussion of wireless technology and security can be found in the State Comptroller's publication entitled *Local Government Management Guide: Wireless Technology and Security*.[7]

Area #10 – Firewalls and Intrusion Detection

Firewalls

Networks that are connected to the Internet are physically connected to unknown networks and their users all over the world. While such connections are often useful, they also increase the vulnerability of computerized information to access and attack from unauthorized individuals. Firewalls consist of hardware and/or software that enforce boundaries between computer systems and the Internet. Firewalls control network traffic flows, using rule sets which specify which services will pass through the firewall and which services are kept out. Firewalls can also act as effective tracking tools and can perform important logging and auditing functions. For these reasons, the network administrator should log and periodically review firewall activities/events.

There are several types of firewalls, each with varying capabilities to analyze network traffic and allow or block specific instances by comparing traffic characteristics to existing policies. Understanding the capabilities of each type of firewall, designing firewall policies and acquiring firewall technologies that effectively address an organization's needs are critical to achieving protection for network traffic flows.

Firewalls consist of hardware and/or software that enforce boundaries between computer systems and the Internet.

[7] **http://www.osc.state.ny.us/localgov/pubs/lgmg/wirelesstechnologysecurity.pdf**

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

There are many aspects to firewall management. For example, choosing the type or types of firewalls to deploy and their positions within the network can significantly affect the security policies that the firewalls can enforce. Firewall rules may need to be updated as the organization's requirements change, such as when new applications or hosts are added to the network. Firewall performance also needs to be monitored so that potential resource issues can be identified and addressed before components become overwhelmed. Logs and alerts that firewalls generate should also be continuously monitored to identify attempts to bypass network security controls—both successful and unsuccessful. Firewall rule sets and policies should be managed by a formal change management control process because of their potential impact to security and business operations, with rule set reviews or tests performed periodically to ensure continued compliance with the organization's policies. Firewall software should be patched regularly as vendors provide updates to address vulnerabilities and increase functionality.

Intrusion Detection

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Network-based intrusion detection systems (IDSs) capture or "sniff" and analyze network traffic in various parts of a network; host-based IDSs analyze activity to and from a particular computer or host.

Because the log information maintained may be too voluminous to review on a routine basis, the IDS should be implemented to selectively identify unauthorized, unusual and sensitive access activity, such as:

- attempted unauthorized access;
- access trends and deviations from those trends;
- access to sensitive data and resources;
- highly sensitive privileged access, such as the ability to override security controls;
- floods of data coming from or going to a particular host or group of hosts;
- access modifications made by security personnel; and
- unsuccessful attempts to log on to a system.

Unauthorized, unusual or sensitive access activity identified by the IDS should be reviewed and any apparent or suspected violations should be investigated. When a security violation occurs, appropriate action should be taken to identify and remedy the control weaknesses that allowed the violation to occur, repair any damage that has been done and determine and discipline the perpetrator. It is important that an organization have formal written procedures for reporting security violations or suspected violations to the IT manager or other appropriate IT personnel so that multiple related incidents can be identified, other employees can be alerted to potential threats, and appropriate investigations can be performed. Such incidents might include multiple attacks by a common hacker or repeated infections with the same computer virus. It is important to note that seemingly innocuous or legitimate behavior could be a manual probe to collect data about a network or security over a network, and thus it is important that you provide for periodic manual review of network activity even with an automated IDS in place.

Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment.

Area #11 – Physical Controls

Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment. Such controls include guards, gates and locks, and also environmental controls such as smoke detectors, fire alarms and extinguishers, protection from water damage and uninterruptible power supplies.

Larger local governments and school districts may have a server room while smaller units may place servers next to a desk, under a desk, in a closet, in the middle of the room or other high-traffic area. You should inspect the location of computers and server areas/rooms and ensure that there are adequate physical security controls commensurate with the risks of physical damage or access.

IT contingency planning refers to the plans, policies, procedures and technical measures that enable the recovery of IT operations after an unexpected incident.

Area #12 – Information Technology Contingency Planning

Written Contingency Plan

The impact of an unplanned IT disruption involving the corruption or loss of data or other computer resources from human error, malware or hardware failure, could significantly curtail an organization's operations. Proactively anticipating and planning for such IT disruptions will prepare local government and school district personnel for the actions they must take in the event of an incident.

IT contingency planning refers to the plans, policies, procedures and technical measures that enable the recovery of IT operations after an unexpected incident. A disruptive event could include a major natural disaster such as a flood, or something smaller, such as malfunctioning software caused by a computer virus. The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of your organization's computerized operations.

Some best practices relating to IT contingency planning include:

- assembling a team responsible for drafting the plan;
- identifying and prioritizing critical business processes and services;
- developing and distributing the plan to all responsible parties;
- training personnel expected to execute the plan;
- testing the plan, as appropriate; and
- reviewing and as necessary, revising the plan to ensure it still meets organizational needs.

Backup Procedures

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. Establishing backup procedures is a necessary part of IT contingency planning and often critical for restoring operations quickly and effectively following a service disruption.

Some best practices relating to backup procedures include:

- adopting a data backup policy that defines the frequency and scope of backups, the location of stored backup data, the specific method for backing up;
- backing up data at regular intervals;
- verifying data has been backed up and can be restored in the event of an emergency; and
- storing backups in an offsite location that meets the organization's data security requirements.

A further discussion of IT contingency planning and backup procedures can be found in the State Comptroller's publication entitled *Local Government Management Guide: Information Technology Contingency Planning*.[8]

Establishing backup procedures is a necessary part of IT contingency planning and often critical for restoring operations quickly and effectively following a service disruption.

[8] **http://www.osc.state.ny.us/localgov/pubs/lgmg/itcontingencyplanning.pdf**

Additional Resources

Center for Internet Security
https://www.cisecurity.org/

Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/

National Institute of Standards and Technology
http://www.nist.gov/

New York State Office of Information Technology Services
https://www.its.ny.gov/

New York State Office of the State Comptroller
http://www.osc.state.ny.us/

United States Computer Emergency Readiness Team
https://www.us-cert.gov/

Information Technology Governance

Security Self-Assessment

Date Assessment Completed: _____

		YES	NO	N/A
IT Policy				
1a	Are computer policies adopted, distributed, and updated as necessary?			
	List policies and dates adopted or last revised:			
1b	Was a data breach notification policy adopted?			
	Date adopted:			
IT Security Training and Awareness				
2a	Were all computer users provided IT security training?			
	Date(s) of training:			
	Who attended the training:			
2b	Are there other efforts to raise IT security awareness?			
	Describe awareness efforts:			
Computer Hardware, Software and Data Inventories				
3a	Is a detailed, up-to-date inventory of computer hardware maintained?			
	Review a copy of the hardware inventory and note when last updated:			

		YES	NO	N/A
3b	Is a detailed, up-to-date inventory of authorized software maintained?			
	Review a copy of the software inventory and note when last updated:			
3c	Has data been assigned to categories (data classification) that will help determine the appropriate level of controls?			
	Review a copy of the data classification, noting the categories and types of information in each:			
3d	Is a detailed, up-to-date inventory of data maintained?			
	Review a copy of the data inventory and note when last updated:			
Contracts for IT Services				
4a	Do contracts for IT services specify the level of service to be received?			
	Review the contract(s) and note the date signed:			
4b	Are there adequate controls over third-party (e.g., IT vendors or IT service organizations) access to personal, private and/or sensitive information?			
	Describe the controls in place to protect the data:			
	Describe how access by third parties is monitored:			

		YES	NO	N/A
Virus Protection				
5a	Is antivirus protection up-to-date on all computers?			
	Describe the process for updating antivirus protection:			
	Date of last antivirus protection update:			
5b	Is the autoplay feature for USB devices disabled?			
5c	Are USB and other removable media devices scanned upon connection to municipal devices?			
Patch Management				
6	Are software and operating system patches applied in a timely manner?			
	Describe the process for applying patches:			
	Describe the process for updating when an application is no longer supported by the vendor:			
Access Controls				
7a	Are unique network accounts created for each computer user?			
7b	Are unique software accounts created for each user where applicable?			
7c	Do any accounts exist that cannot be tied to an authorized user or application?			
	Describe the process for disabling terminated employee/vendor accounts:			
7d	Are passwords held to complexity requirements?			
	Describe the complexity requirement:			
7e	Are password changes enforced on a regular basis (e.g., 30 to 90 days)?			

		YES	NO	N/A
	Indicate how often passwords are changed and describe how the change is enforced:			
7f	Is sharing user IDs and passwords prohibited?			
7g	Are changes to access rights made on a timely basis (i.e., within three to five days of duty changes)?			
7h	Is a current list of authorized users and their levels of access maintained and periodically reviewed?			
	Review the list of authorized users and their levels of access.			
Online Banking				
8a	Do you have an online banking policy?			
	Review the policy.			
8b	Are online bank accounts monitored?			
	Who monitors the accounts?			
	How often are online accounts monitored?			
8c	Are two-person controls in place over transactions?			
	Who has access to online bank account(s)?			
8d	Are there dollar limits on transfers?			
	What is the limit?			
8e	Are there controls limiting what accounts money can be transferred to?			
	List accounts money can be transferred to:			

		YES	NO	N/A
8f	Is online banking only conducted from a wired rather than wireless network?			
8g	Is there a written agreement or contract with the bank?			
	Review the agreement and note the date signed:			
Wireless Network				
9a	Are wireless access points set up to limit broadcasting from beyond your offices?			
	Where are the wireless access points located?			
	How far does the wireless signal broadcast?			
9b	Has the service set identifier (SSID) been changed from the factory default?			
	What is/are the SSID(s)?			
9c	Is/are SSID(s) changed periodically?			
9d	Has the SSID broadcasting feature has been disabled?			
9e	Is the strongest encryption available used?			
	Note type of encryption used:			
Firewalls and Intrusion Detection				
10a	Does the unit have a firewall(s)?			
	Who is responsible for maintaining firewall updates and configurations?			
10b	Have firewall default accounts been removed/changed?			
10c	Are firewall activities/events logged?			
	Who reviews the logs?			

		YES	NO	N/A
	Are alerts about suspicious activities emailed to a certain individual? If so, who?			
10d	Does the unit have an intrusion detection system (IDS)?			
	How does the system respond to a suspicious event?			
	Who is responsible for reviewing the events captured by the IDS and taking appropriate action?			
	Are alerts about suspicious activities emailed to a certain individual? If so, who?			
Physical Controls				
11a	Is physical access to computers, servers, and wiring closets (if any) restricted?			
	View the computer, server and wiring closet areas/rooms.			
11b	Are areas with computers, servers and wiring closets climate-controlled and protected from fire and water damage?			
11c	Is there an uninterrupted power source?			
11d	Are manual inspections conducted for violations of physical security controls?			
	Who conducted the last inspection and on what date:			
Service Continuity and Disaster Recovery				
12a	Are systems, including data, applications and operating systems, periodically backed up?			
	How often?			

		YES	NO	N/A
	Date of last backup:			
	Date information was successfully restored from a backup copy:			
12b	Are backups stored offsite?			
	Where is the offsite storage and how is it secured?			
12c	Are backups of sensitive data encrypted?			
12d	Does the unit have a disaster recovery plan?			
	Review the plan and note date adopted:			
12e	Has the plan been distributed to responsible parties?			
	When was the last time the plan was tested?			
	What was the outcome of the testing?			
12f	Is the plan periodically adjusted based on test results and changing conditions?			
	Date plan last updated:			

Division of Local Government and School Accountability

Central Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

(Area code for the following is 518 unless otherwise specified)

Executive 474-4037
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

Audits, Local Government Services and Professional Standards 474-5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line ..... (866) 321-8503 or 408-4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

New York State & Local Retirement System

Retirement Information Services
Inquiries on Employee Benefits and Programs 474-7736

Bureau of Member and Employer Services ..... (866) 805-0990 or 474-1101
Monthly Reporting Inquiries 474-1080
Audits and Plan Changes 474-0167
All Other Employer Inquiries 474-6535

Division of Legal Services

Municipal Law Section 474-5586

Other OSC Offices

Bureau of State Expenditures 486-3017

Bureau of State Contracts 474-4622

Mailing Address for all of the above:

Office of the New York State Comptroller,
110 State Street, Albany, NY 12236
email: **localgov@osc.state.ny.us**

Division of Local Government and School Accountability

Regional Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

Gabriel F. Deyo, Deputy Comptroller (518) 474-4037
Tracey Hitchen Boyd, Assistant Comptroller

Cole H. Hickland, Director • **Jack Dougherty**, Director
Direct Services (518) 474-5480

BINGHAMTON REGIONAL OFFICE - H. Todd Eames, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313 • **Email:** Muni-Binghamton@osc.state.ny.us
Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • **Fax** (716) 847-3643 • **Email:** Muni-Buffalo@osc.state.ny.us
Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

GLENS FALLS REGIONAL OFFICE - Jeffrey P. Leonard, Chief Examiner
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (518) 793-0057 • **Fax** (518) 793-5797 • **Email:** Muni-GlensFalls@osc.state.ny.us
Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534 • **Fax** (631) 952-6530 • **Email:** Muni-Hauppauge@osc.state.ny.us
Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725
Tel (845) 567-0858 • **Fax** (845) 567-0080 • **Email:** Muni-Newburgh@osc.state.ny.us
Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (585) 454-2460 • **Fax** (585) 454-3545 • **Email:** Muni-Rochester@osc.state.ny.us
Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner
State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428
Tel (315) 428-4192 • **Fax** (315) 426-2119 • **Email:** Muni-Syracuse@osc.state.ny.us
Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

STATEWIDE AUDIT - Ann C. Singer, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313

For additional copies of this report, contact:

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: lgsapaws@osc.state.ny.us

www.osc.state.ny.us

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller

Original Release March 2012
Updated March 2016