Managing Technology Risks Through Technological Proficiency: Guidance for Local Governments

Rutgers University has made this article freely available. Please share how this access benefits you. Your story matters. [https://rucore.libraries.rutgers.edu/rutgers-lib/50746/story/]

These Guides provide best practices and resources that can assist organizations in achieving technological proficiency as discussed in the report “Managing Technology Risks Through Technological Proficiency.” There are guides for each of the four Technology Profiles described in the report. The page numbers below refer to the pages of this PDF document. Each document has its own internal page numbers.

**CONTENTS**

<table>
<thead>
<tr>
<th>Profile</th>
<th>PDF Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Profile</td>
<td>3-8</td>
</tr>
<tr>
<td>Core Profile</td>
<td>9-16</td>
</tr>
<tr>
<td>Managed Profile</td>
<td>17-28</td>
</tr>
<tr>
<td>Sophisticated Profile</td>
<td>29-40</td>
</tr>
</tbody>
</table>
Technology Has Risks. Digital technology permeates everything we do. It goes beyond cyber security issues such as data breaches and network intrusions. This project identified the risks that face local governments and steps they can take to manage and mitigate them.

What is Digital Technology? Today’s technology can be broken down into three areas of application:

- **Information technology** – computers, their applications, and security services
- **Communications technology** – voice, video and data that move over wired and wireless networks
- **Operational technology** – digitally-driven devices such as video cameras, process controllers at water treatment plants, ice-detecting road sensors, meters, drones, including the so-called “internet of things.”

Impact of Digital Technology on Local Governments: Citizens are driving government to adopt new technology (web pages, social media, online services). The challenge is that citizens and businesses want their government to use more technology, but they don’t want to pay more for it. A further challenge is that managing technology is an ongoing process; it is not a short-term project that is completed and ignored.

Technology risks: The effects of these risks are significant; they overlap and break down into six categories.

- **Cybersecurity:** Data breach/theft and disclosure of personally identifiable information, data loss/corruption, network breach, cyber-extortion, website/social media attack.
- **Legal:** 3rd party liability for denial of services, discrimination, litigation costs, OPRA liability, police system failures, employee misuse
- **Operational:** loss of capacity to manage work, compromised physical security of technology, electrical system failures, contractor failures, failed backup systems
- **Financial:** cost of cyber insurance, responses to breaches (time and money), procurement delays, change from capital to operating expenses
- **Reputational:** loss of public trust, media risk, social media, political responses, bond rating agency evaluation
- **Societal:** differing expectations of the next generation of workers, speed of change and ability to manage it, increased expectations of government transparency that are rooted in technology

How Technological Proficiency can address risks: Becoming technologically proficient enables governments to: understand and manage their risks, be assured that technology will work when it needs to, and protect themselves from compromise. Technological proficiency has four interconnected elements:

1. **Governance:** governing body and executive management provide overall technology policy goals and guidance, evaluate risk, approve and fund plans, and monitor activities.
2. **Planning:** governance and technology managers combine to approve a Technology Plan that implements the long- and short-term goals and recommends risk management strategies.
3. **Secure Humans:** all employees understand and practice safe use of technology (cyber hygiene) and receive ongoing training to prevent technology compromise.
4. **Competence:** the staffing, management attention, and financial resources necessary for sound technology strategies are properly and adequately deployed to fulfill the plan.

How to Get Started: The principles of technological proficiency apply to all organizations regardless of the complexity of technology in use. The greater the level of proficiency, the great the maturity to manage risks. The project’s Report provides details, and the Best Practice and Resource Guides provide guidance on how to apply the four proficiency principles in organizations at different levels of complexity.

Project References and Resources: The full Report and Guides were prepared for the Municipal Excess Liability Joint Insurance Fund by the Bloustein Local Government Research Center, Bloustein Local Government Research Center, Rutgers University. The material is online at blousteinlocal.rutgers.edu/managing-technology-risk and http://tinyurl.com/NJMEL-Tech-Risks.
FOR BASIC* TECHNOLOGY PROFILE ORGANIZATIONS

* Basic: Stand-alone desktops with no internal network internet access and email managed via direct connection through an ISP; few if any third party service providers.

Accompanying the Research Project
Managing Technology Risks through Technological Proficiency

Conducted by:
Bloustein Local Government Research Center
Rutgers University
www.blousteinlocal.rutgers.edu

For the:
Municipal Excess Liability Joint Insurance Fund
www.njmel.org
READ THIS FIRST: Instructions for Using this Guide

Understand that all “rules” and recommendations do not apply to every circumstance; use discretion and judgment to ensure that the user's technology environment is consistent with the recommendations.

Users should also review the detailed explanation of technology governance and planning in the full Managing Technology Risks through Technological Proficiency report.

Goals of technology governance:

- Improve organizational accountability for results
- Strengthen working relationships between technology management, executive management, and working units
- Reduce operational risks/inefficiencies
- Attend to actions necessary for funding approval/Focus technology spending on established goals
- Establish reporting process: avoid problems or project overruns/failures stemming from false starts, scope creep or reactive re-prioritization
- Lead to limited technological complexity and greater systems integration
- Ensure an effective technology planning process

Technology governance includes the following elements, as appropriate to the organization. These steps should be carried out at least annually, and more frequently if necessary:

1. Establish Governing Entity: Established by the governing body, it defines the roles and responsibilities of the governance process, identifies those serving on it, and addresses the logistics of carrying out its obligations (meetings, relationship with administration and governing body); it needs to establish a reporting process that leads from technology management to executive management as well as to the governing body.

2. Establish Technology Planning process: identify the responsibilities of each individual, establish a timetable for preparation, review and approval, and tie it to the budget process. The Plan needs be tied to overall organization plans (to the extent they exist).

3. Adopt policies for the following items; find examples and adapt as necessary to local needs:
   - Acceptable Use and Social Media Policy
   - Internet Access Policy
   - Data Breach Policy/Response Plan
   - Email and Communications Policy
   - Privacy Policy

4. Assess technological risk maturity to establish the type of policies needed in order to show improve along the continuum. (See Page 3)

5. Conduct a technology risk assessment and integrate it with the technology plan (identify, analyze, mitigate, review).

6. Establish technology management model: because of the limited needs and staffing of this profile, employee and perhaps contractual expertise will be necessary to ensure that technology decisions are implemented as they are needed. Clear lines of authority for decision-making must be provided.
Assess Technological Risk Maturity

Complete the “20 Questions – Technological Risk Maturity Assessment” questionnaire at the end of this guide. Match your average to the stage that best describes your organization. You should design your governance policies so that your organization will be able to through the levels over time until you are able to reach stage 4 or 5.

**Stage 1: Unaware:** The organization sees technology management as largely irrelevant, and it does not form part of the organization's management process. The organization is not aware of its level of interconnectedness and its risks. They are doing nothing or consciously ignoring the risks.

**Stage 2: Fragmented:** Management recognizes technology issues as a potential source of risk, and has limited insight to its technology management practices. The organization has a “silo” approach to technology and its management, with fragmented and incidental reporting.

**Stage 3: Top Down:** Management has set the tone for technology management and has initiated standards, but does not view technology management as a critical issue.

**Stage 4: Managed:** The organization's leadership takes full ownership of technology management, has developed policies and plans, and has defined responsibilities and oversight mechanisms. It makes calculated decisions on technological needs. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

**Stage 5: Optimized:** The organization is highly connected to its community, peers and partners, sharing information, meeting citizen and client expectations, and coordinating technology risk mitigation as part of its day-to-day operations. Its people show exceptional technological acumen and cyber-awareness and the organization is a leader in technology management.

<table>
<thead>
<tr>
<th>Stage 1</th>
<th>• Unaware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 2</td>
<td>• Fragmented</td>
</tr>
<tr>
<td>Stage 3</td>
<td>• Top Down/Evolving</td>
</tr>
<tr>
<td>Stage 4</td>
<td>• Managed/Pervasive</td>
</tr>
<tr>
<td>Stage 5</td>
<td>• Optimized/Networked</td>
</tr>
</tbody>
</table>
Technology planning requires the use of resources: time, attention and in some cases money. How much of each depends on your organization’s governance model, its risk maturity and its technology profile. Find something that works for your agency.

The following are the essential elements of any Technology Plan:

- **Identify your current technology environment**: technology uses/applications, profile, staffing competencies, metrics, hardware/software inventory, management model, operating status (i.e., growth, stable, reductions); identify risks

- **Establish your desired technology environment**: match technology to organizational goals by consulting with staff as well as internal and external stakeholders. Identify their interests; scan technology horizons for opportunities

- **Identify the gap** between your current environment and your desired environment

- **Identify strategies to fill the gap**: match strategies to available resources (time, attention, money) and continually review and modify them with the governance process (i.e., budget) until they all align

- **Recommend risk mitigation** strategies to your organization’s governance entity

- **Implement**

- **Measure** results (identify metrics or expected outcomes)

- **Repeat** as necessary to meet goals

### Cyber Hygiene

**Apply these best practices of cyber-hygiene:**

- a. Only utilize business-related websites
- b. Check with the sender if you are not expecting an attachment
- c. Cooperate with IT management’s instructions regarding security patches
- d. NEVER open suspicious attachments or unexpected email
- e. NEVER install hardware or software without IT approval
- f. NEVER download any programs without IT approval
- g. NEVER use a USB drive whose source is uncertain
- h. Understand and apply your organization’s technology policies
- i. Only uses services and products approved by IT management
- j. Use strong passwords:
  - i. At least eight characters
  - ii. Use a phrase relevant to the user
  - iii. Include a minimum of 2 numbers
  - iv. Never write down (unless password protected) or divulge your password
  - v. Change your password every 30-90 days
Cyber Hygiene Resource Guide

- SANS Secured Human - [www.securingthehuman.org](http://www.securingthehuman.org)
- MS-ISAC guides at: [http://msisac.cisecurity.org/resources/guides/](http://msisac.cisecurity.org/resources/guides/)
- [www.StopThinkConnect.org](http://www.StopThinkConnect.org)
- [www.StaySafeOnline.org](http://www.StaySafeOnline.org)
- KnowBe4 - [www.knowbe4.com](http://www.knowbe4.com)

In addition, security training resources may be available through your local public library, board of education, county technology school or county college.

Basic Technical Competency Actions

- Minimum for all systems: firewalls, anti-virus, anti-spam, anti-malware software running on all desktops
- Backups! Stored on- **and** off-site (or in the cloud) as appropriate
- Restrict user installation of applications (whitelisting)
- Ensure that operating systems are patched with current updates
- Ensure that software applications have current updates assuming that vendor advises they are compatible with operating system(s) in use.
- Protect online financial transactions: to prevent inadvertent infection, social engineered hacks and harmful downloads, dedicate a computer for financial transactions that prohibits email and general web-surfing
- Periodically test system failure and disaster recovery plans

Test for data breaches regularly and make sure that your organization meets all compliance standards for any HIPPA, PCI and CJIS related services.
### 20 Questions – Technological Risk Maturity Assessment Checklist

*Note: This assessment addresses the range of technology risks facing a government organization. It can also be used to address just the cyber risk component. Because the evaluation is subjective and will vary from one entity to another, and in the absence of metrics for each of the variables below, these benchmarks are not intended for use in comparing one entity against another. In addition, this assessment is not intended to promote one particular technology model or to advocate against any set of rules or expectations.*

<table>
<thead>
<tr>
<th>Governance</th>
<th>1: Does not describe my organization at all... 5: Accurately describes my organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The governing body and senior management (governance team) are responsible for overseeing the development of a technology plan and confirming its implementation</td>
</tr>
<tr>
<td>2.</td>
<td>The governance team ensures that the plan is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued</td>
</tr>
<tr>
<td>3.</td>
<td>The team demonstrates visible and active commitment to the implementation of the plan</td>
</tr>
<tr>
<td>4.</td>
<td>Executives and managers are responsible for understanding at the appropriate level how technology risks could impact the organization and originate from their activities</td>
</tr>
<tr>
<td>5.</td>
<td>Senior leadership understands who is responsible for mitigating cyber risk when managing security incidents</td>
</tr>
<tr>
<td>6.</td>
<td>The organization has access to technology and cyber expertise at its highest management level</td>
</tr>
<tr>
<td>7.</td>
<td>The organization undertakes to continuously improve the integration of its technology risk management plan with its other risk management initiatives</td>
</tr>
<tr>
<td>8.</td>
<td>The chief executive has a clear path for action and communication in response to a significant security failure or accident</td>
</tr>
</tbody>
</table>

| Plan | |
| 9. | The organization conducts comprehensive assessments of its vulnerabilities to internal and external risks appropriate for its size and technological profile |
| 10. | The organization monitors the effectiveness of its risk management strategy |
| 11. | The organization periodically internally verifies its compliance with rules and regulations |
| 12. | The organization’s commitment to the Plan is reflected in its policies and practices |
| 13. | Managers, employees and agents receive specific training on plan elements, tailored to relevant needs and circumstances |
| 14. | The organization has identified its data and information as vital assets, and organizes its plan around the recognition that data and information have value that can be separately recognized and protected |
| 15. | The risk management elements of the plan includes all material third-party relationships and information flows |
| 16. | The organization conducts comprehensive internal short- and long-term cyber risk impact assessments |

| Relationships | |
| 17. | The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization’s specific cyber risk management standards or industry best practices, in line with the plan, and formalizes this requirement using contractual obligations |
| 18. | The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents |
| 19. | The risk management plan element includes all material third-party relationships and information flows |
| 20. | Executed plans reflect technology services that meet the needs of the organization’s employees, constituents, clients. |

**Average (gives maturity stage) – total the numbers for each question and divide by 20.**

\[
\text{Total: } \frac{\text{Total}}{20} = \]

---

1 Adapted from World Economic Forum, 2012, Partnering for Cyber Resilience, C-Suite Executive Checklist
**FOR CORE** technology profile organizations

*Core: Has a small internal network and may use Microsoft Exchange. Other services are purchased through third party providers. The police department and other agencies may run their own technology separate from the rest of the system.

<table>
<thead>
<tr>
<th>Conducted by:</th>
<th>For the:</th>
</tr>
</thead>
</table>
| Bloustein Local Government Research Center  
Rutgers University  
[www.blousteinlocal.rutgers.edu](http://www.blousteinlocal.rutgers.edu) | Municipal Excess Liability Joint Insurance Fund  
[www.njmel.org](http://www.njmel.org) |

Accompanying the Research Project

**Managing Technology Risks through Technological Proficiency**
READ THIS FIRST: Instructions for Using this Guide

Understand that all “rules” and recommendations do not apply to every circumstance; use discretion and judgment to ensure that the user's technology environment is consistent with the recommendations.

Users should also review the detailed explanation of technology governance and planning in the full Managing Technology Risks through Technological Proficiency report.

Establish Core Technology Governance

Goals of technology governance:

- Improve organizational accountability for results
- Strengthen working relationships between technology management, executive management, and working units
- Reduce operational risks/inefficiencies
- Attend to actions necessary for funding approval/Focus technology spending on established goals
- Establish reporting process: avoid problems or project overruns/failures stemming from false starts, scope creep or reactive re-prioritization
- Lead to lower technological complexity and greater systems integration
- Ensure an effective technology planning process

Technology governance includes the following elements, as appropriate to the organization and over an appropriate time frame that is no less than annual, and more frequent if necessary:

1. Establish Governing Entity: Established by the governing body, it defines the roles and responsibilities of the governance process, who serves on it, and logistics (meetings, relationship with administration and governing body); establish reporting process from technology management to executive management and governing body.

2. Establish Technology Planning process: identify responsibilities of individuals, establish timetable for preparation, review and approval, and tie it to the budget process. Plan is tied insofar as possible to overall organization plans (to the extent they exist).

3. Consider adopting the following policies. Find examples and adapt as necessary to local needs.
   a. Acceptable Use and Social Media Policy
   b. Internet Access Policy
   c. Data Breach Policy/Response Plan
   d. Email and Communications Policy
   e. Privacy Policy Network Security Policy
   f. Contractor security practices
   g. Privacy Policy
   h. Cloud based software/storage solution

4. Assess technological risk maturity to establish what type of policies will be needed in order for the organization to improve along the continuum. (See Page 3)

5. Conduct a technology risk assessment and integrate it with the technology plan (identify, analyze, mitigate, review).

6. Establish technology management model: based on the technology plan, the IT manager and staff members are assigned well-defined responsibilities regarding day-to-day decisions and the implementation of the organization's plan. Those assignments may include authorizing specific individuals to make decisions regarding matters of technical architecture, infrastructure, strategies and project management.
Assess Technological Risk Maturity

Complete the “20 Questions – Technological Risk Maturity Assessment” questionnaire at the end of this guide. Match your average to the stage that best describes your organization. You should design your governance policies so that your organization will be able to through the levels over time until you are able to reach stage 4 or 5.

Stage 1: Unaware: The organization sees technology management as largely irrelevant, and it does not form part of the organization's management process. The organization is not aware of its level of interconnectedness and its risks. They are doing nothing or consciously ignoring the risks.

Stage 2: Fragmented: Management recognizes technology issues as a potential source of risk, and has limited insight to its technology management practices. The organization has a “silo” approach to technology and its management, with fragmented and incidental reporting.

Stage 3: Top Down: Management has set the tone for technology management and has initiated standards, but does not view technology management as a critical issue.

Stage 4: Managed: The organization's leadership takes full ownership of technology management, has developed policies and plans, and has defined responsibilities and oversight mechanisms. It makes calculated decisions on technological needs. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

Stage 5: Optimized: The organization is highly connected to its community, peers and partners, sharing information, meeting citizen and client expectations, and coordinating technology risk mitigation as part of its day-to-day operations. Its people show exceptional technological acumen and cyber-awareness and the organization is a leader in technology management.
Core Technology Planning

- Technology planning requires the use of resources: time, attention and in some cases money. How much of each depends on your organization’s governance model, its risk maturity and its technology profile. Find something that works for your agency.

- The following are the essential elements of any Technology Plan:
  - Identify your current technology environment: technology uses/applications, profile, staffing competencies, metrics, hardware/software inventory, management model, operating status (i.e., growth, stable, reductions); identify risks
  - Establish your desired technology environment: match technology to organizational goals by consulting with staff as well as internal and external stakeholders. Identify their interests; scan technology horizons for opportunities
  - Identify the gap between your current environment and your desired environment
  - Identify strategies to fill the gap: match strategies to available resources (time, attention, money) and continually review and modify them with the governance process (i.e., budget) until they all align
  - Recommend risk mitigation strategies to your organization’s governance entity
  - Implement
  - Measure results (identify metrics or expected outcomes)
  - Repeat as necessary to meet goals

Cyber Hygiene

Apply these best practices of cyber-hygiene:

a. Only utilize business-related websites
b. Check with the sender if you are not expecting an attachment
c. Cooperate with IT management’s instructions regarding security patches
d. NEVER open suspicious attachments or unexpected email
e. NEVER install hardware or software without IT approval
f. NEVER download any programs without IT approval
g. NEVER use a USB drive whose source is uncertain
h. Understand and apply your organization’s technology policies
i. Only uses services and products approved by IT management
j. Use strong passwords:
   - At least eight characters
   - Use a phrase relevant to the user
   - Include a minimum of 2 numbers
   - Never write down (unless password protected) or divulge your password
   - Change your password every 30-90 days
Cyber Hygiene Resource Guide

b. SANS Secured Human: www.securingthehuman.org
a. MS-ISAC guides at: http://msisac.cisecurity.org/resources/guides/
c. www.StopThinkConnect.org
d. www.StaySafeOnline.org
e. KnowBe4 - www.knowbe4.com

In addition, security training resources may be available through your local public library, board of education, county technology school, or county college.

Technology Management Actions

a. Join MS-ISAC to monitor cyber threats: http://msisac.cisecurity.org and take advantage of their employee training resources.

b. Join GMIS International and NJ-GMIS– a US-based association for government IT leaders with a NJ chapter; this group is dedicated to providing best practice solution, professional development, conferences and networking opportunities: www.gmis.org and www.njgmis.org

c. Test for data breaches regularly and make sure that your organization meets all compliance standards for any HIPPA, PCI and CJIS related services.

d. Be aware of government cyber security resources and use them as appropriate
   i. NJCCIC – the state website that coordinates state cyber security resources, including resources for conducting vulnerability assessments www.cyber.nj.gov/.
   ii. NJ InfraGuard – a public and private sector alliance whose mission is to share information and protect critical infrastructures www.njinfragard.org/
   iii. N.J. State Police Cyber Crime Unit – the State Police unit that investigates cyber crimes - www.njsp.org/divorg/invest/cyber-crimes-unit.html
   iv. US Cert – a US government agency that provides security alerts (membership in this organization comes with with your agency’s participation in MS-ISAC) www.us-cert.gov/ and Cyber Resilience Review at www.us-cert.gov/ccubedvp/self-service-crr
   v. New Jersey Regional Computer Forensic Laboratory – an FBI managed facility that provides digital forensic services and training to any law enforcement agency in New Jersey www.njrcfl.org/

Technical Competency Actions

a. Minimum for all systems: anti-virus, firewalls, anti-spam, anti-malware software running on all desktops
For CORE Technology Profile Organizations

b. Backups! Stored on and off-site (or in the cloud) as appropriate

c. Restrict user installation of applications (whitelisting)

d. Ensure that operating systems are patched with current updates

e. Ensure that software applications have current updates after testing to ensure they are compatible with operating system(s) in use.

f. Protect online financial transactions: to prevent inadvertent infection, social engineered hacks, and harmful downloads, dedicate a computer for financial transactions that prohibits email and general web-surfing

g. Periodically test system failure and disaster recovery plans

h. Restrict administrative privileges and regularly review them

**Adopt Additional Cyber Hygiene Best Practices**¹

a. Count: Know what’s connected to your network as well as what’s running on it.

b. Configure: Implement key security settings to help protect your systems.

c. Control: Limit and manage those who have admin privileges to change, bypass or override your security settings.

d. Patch: Regularly update all apps, software and operating systems.

e. Repeat: Make monitoring these priority items a routine to form a solid foundation of cybersecurity for your organization.

**Consider the Applicability of “Steps to Successful Cyber Risk Management”² and Apply Accordingly**

a. Manage incidents - Establish an incident response and disaster recovery policy. Produce and test incident management plans. Provide specialized training to members of the incident management team. Report criminal incidents to law enforcement agencies.

b. Limit privileges - Establish processes to manage accounts and limit the number of privileged account holders. Restrict user privileges and monitor user activity. Control access to activity and audit logs.

c. Control removable media - Develop a policy to control employee access to removable media. Limit media types and their use. Scan all media for malware before importing it onto the network.

d. Monitor - Establish a monitoring strategy and develop supporting policies. Continuously audit all technology systems and networks. Analyze logs for unusual activity that could indicate an attack; contract with third-party vendors to provide services as necessary.

e. Secure system configurations - Apply security patches to ensure that all systems are securely configured and maintained. Create a system inventory and define a baseline build for all devices.

f. Network security - Protect your networks against external and internal attacks. Manage the network perimeter. Filter out unauthorized access and malicious content. Monitor and test security controls.

---

¹ Center for Internet Security, [https://www.cisecurity.org/about/CyberCampaign2014.cfm](https://www.cisecurity.org/about/CyberCampaign2014.cfm)

20 Questions – Technological Risk Maturity Assessment Checklist

Note: This assessment addresses the range of technology risks facing a government organization. It can also be used to solely address the cyber risk component. Because of the subjectivity of evaluation from one entity to another and the absence of metrics for each of the variables below, the benchmarking is not intended for use in comparing one entity against another, nor the conformity of a particular technology environment against any set of rules or expectations.

<table>
<thead>
<tr>
<th>Governance</th>
<th>1: Does not describe my organization at all ......5: Accurately describes my organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The governing body and senior management (governance team) are responsible for overseeing the development of a Technology Plan and confirming its implementation</td>
</tr>
<tr>
<td>2.</td>
<td>The governance team ensures that the Plan is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued</td>
</tr>
<tr>
<td>3.</td>
<td>The team demonstrate visible and active commitment to the implementation of the Plan</td>
</tr>
<tr>
<td>4.</td>
<td>Executives and managers are responsible for understanding at the appropriate level how technology risks could impact and originate from their activities</td>
</tr>
<tr>
<td>5.</td>
<td>Senior leadership understands who is responsible for managing cyber risk when managing security incidents</td>
</tr>
<tr>
<td>6.</td>
<td>The organization has access to technology and cyber expertise at its highest management levels</td>
</tr>
<tr>
<td>7.</td>
<td>The organization undertakes to continuously improve the integration of its technology risk management with its other risk management initiatives</td>
</tr>
<tr>
<td>8.</td>
<td>The organization conducts comprehensive assessments of its vulnerabilities to internal and external risks appropriate for its size and technological profile</td>
</tr>
<tr>
<td>9.</td>
<td>The organization monitors the effectiveness of its risk management strategy</td>
</tr>
<tr>
<td>10.</td>
<td>The organization periodically internally verifies its compliance with rules and regulations</td>
</tr>
<tr>
<td>11.</td>
<td>The organization’s commitment to the Plan is reflected in its policies and practices</td>
</tr>
<tr>
<td>12.</td>
<td>Managers, employees and agents receive specific training on Plan elements, tailored to relevant needs and circumstances</td>
</tr>
<tr>
<td>13.</td>
<td>The organization has identified its data and information as vital assets, and organizes its Plan around the recognition that data and information have value that can be separately recognized and protected</td>
</tr>
<tr>
<td>14.</td>
<td>The organization’s risk management plan includes all material third-party relationships and information flows</td>
</tr>
<tr>
<td>15.</td>
<td>The organization conducts comprehensive internal short- and long-term cyber risk impact assessments</td>
</tr>
<tr>
<td>16.</td>
<td>Executed plans reflect technology services that meet the needs of the organization’s employees, constituents, clients.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Plan</th>
<th>1: Does not describe my organization at all ......5: Accurately describes my organization</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Relationships</th>
<th>1: Does not describe my organization at all ......5: Accurately describes my organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization’s specific cyber risk management standards or industry best practices, in line with the Plan, and formalizes this requirement using contractual obligations</td>
</tr>
<tr>
<td>18.</td>
<td>The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents</td>
</tr>
<tr>
<td>19.</td>
<td>The risk management plan element includes all material third-party relationships and information flows</td>
</tr>
<tr>
<td>20.</td>
<td>Executed plans reflect technology services that meet the needs of the organization’s employees, constituents, clients.</td>
</tr>
</tbody>
</table>

Average (gives maturity stage) – total the numbers for each question and divide by 20. Total: \( \frac{1+2+3+4+5}{20} = \)

3 Adapted from World Economic Forum, 2012, Partnering for Cyber Resilience, C-Suite Executive Checklist

© 2015, Municipal Excess Liability Joint Insurance Fund and Rutgers, the State University
Best Practice and Resource Guide
For Achieving Technological Proficiency

FOR MANAGED* TECHNOLOGY PROFILE ORGANIZATIONS

*Managed: Fully wired and/or wireless internal network with small staff or contractor management, using local servers for hosting third party software and connected to cloud-based services; police services may be mixed in or supported by the

Accompanying the Research Project
Managing Technology Risks through Technological Proficiency

Conducted by:
Bloustein Local Government Research Center
Rutgers University
www.blousteinlocal.rutgers.edu

For the:
Municipal Excess Liability Joint Insurance Fund
www.njmel.org
READ THIS FIRST: Instructions for Using this Guide

Understand that all “rules” and recommendations do not apply to every circumstance; use discretion and judgment to ensure that the user's technology environment is consistent with the recommendations.

Users should also review the detailed explanation of technology governance and planning in the full Managing Technology Risks through Technological Proficiency report.

Establish Managed Technology Governance

Goals of technology governance:

- Improve organizational accountability for results
- Strengthen working relationships between technology management, executive management, and working units
- Reduce operational risks/inefficiencies
- Attend to actions necessary for funding approval/Focus technology spending on established goals
- Establish reporting process: avoid problems or project overruns/failures stemming from false starts, scope creep or reactive re-prioritization
- Lead to lower technological complexity and greater systems integration
- Ensure an effective technology planning process

Technology governance includes the following elements, as appropriate to the organization. These steps should be carried out at least annually, and more frequently if necessary:

1. Establish governing entity: Established by the governing body, it defines the roles and responsibilities of the governance process, identifies those serving on it, and addresses the logistics of carrying out its obligations (meetings, relationship with administration and governing body); it needs to establish a reporting process that leads from technology management to executive management as well as to the governing body.

2. Establish technology planning process: identify the responsibilities of each individual, establish a timetable for preparation, review and approval, and tie it to the budget process. The Plan needs be tied to overall organization plans (to the extent they exist).

3. Adopt policies; find examples and adapt as necessary to local needs.

| a. Acceptable Use and Social Media Policy | b. Internet Access Policy |
| c. Data Breach Policy/Response Plan | d. Email and Communications Policy |
| e. Privacy Policy | f. Contractor security practices |
| g. Network Security Policy | h. Cloud based software/storage solution |
| i. Optional, depending on need: 1) Remote Access Policy; 2) BYOD Policy, 3) Encryption Policy |

4. Assess technological risk maturity to establish what type of policies will be needed in order for the
For MANAGED Technology Profile Organizations

organization to improve along the continuum. (See Page 3)

5. Conduct a technology risk assessment and integrate it with the technology plan (identify, analyze, mitigate, review).

6. Establish technology management model: the authority to make decisions must be delegated to staff members empowered to execute the technology plan. Among those issues are the needs of the organization as they pertain to business applications, technical architecture, infrastructure, strategies and project management. Organizations must delegate these responsibilities in a way that is consistent with the competencies of their staff members.

Assess Technological Risk Maturity

Complete the “20 Questions – Technological Risk Maturity Assessment” questionnaire at the end of this guide. Match your average to the stage that best describes your organization. You should design your governance policies so that your organization will be able to through the levels over time until you are able to reach stage 4 or 5.

Stage 1: Unaware: The organization sees technology management as largely irrelevant, and it does not form part of the organization's management process. The organization is not aware of its level of interconnectedness and its risks. They are doing nothing or consciously ignoring the risks.

Stage 2: Fragmented: Management recognizes technology issues as a potential source of risk, and has limited insight to its technology management practices. The organization has a “silo” approach to technology and its management, with fragmented and incidental reporting.

Stage 3: Top Down: Management has set the tone for technology management and has initiated standards, but does not view technology management as a critical issue.

Stage 4: Managed: The organization's leadership takes full ownership of technology management, has developed policies and plans, and has defined responsibilities and oversight mechanisms. It makes calculated decisions on technological needs. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

Stage 5: Optimized: The organization is highly connected to its community, peers and partners, sharing information, meeting citizen and client expectations, and coordinating technology risk mitigation as part of its day-to-day operations. Its people show exceptional technological acumen and cyber-awareness and the organization is a leader in technology management.
Technology planning requires the use of resources: time, attention and in some cases money. How much of each depends on your organization’s governance model, its risk maturity and its technology profile. Find something that works for your agency.

- The following are the essential elements of any Technology Plan:
  - **Identify your current technology environment**: technology uses/applications, profile, staffing competencies, metrics, hardware/software inventory, management model, operating status (i.e., growth, stable, reductions); identify risks
  - **Establish your desired technology environment**: match technology to organizational goals by consulting with staff as well as internal and external stakeholders. Identify their interests; scan technology horizons for opportunities
  - **Identify the gap** between your current environment and your desired environment
  - **Identify strategies to fill the gap**: match strategies to available resources (time, attention, money) and continually review and modify them with the governance process (i.e., budget) until they all align
  - **Recommend risk mitigation** strategies to your organization’s governance entity
  - **Implement**
  - **Measure** results (identify metrics or expected outcomes)
  - **Repeat** as necessary to meet goals

**Apply these best practices of cyber hygiene:**

- a. Only utilize business-related websites
- b. Check with the sender if you are not expecting an attachment
- c. Cooperate with IT management’s instructions regarding security patches
- d. NEVER open suspicious attachments or unexpected email
- e. NEVER install hardware or software without IT approval
- f. NEVER download any programs without IT approval
- g. NEVER use a USB drive whose source is uncertain
- h. Understand and apply your organization’s technology policies
- i. Only uses services and products approved by IT management
- j. Use strong passwords:
  - At least eight characters
  - Use a phrase relevant to the user
  - Include a minimum of 2 numbers
  - Never write down (unless password protected) or divulge your password
  - Change your password every 30-90 days
Cyber Hygiene Resource Guide

b. SANS Secured Human - www.securingthehuman.org
c. MS-ISAC guides at: http://msisac.cisecurity.org/resources/guides/
e. www.StopThinkConnect.org
f. www.StaySafeOnline.org
g. KnowBe4 - www.knowbe4.com

In addition, security training resources may be available through your local public library, board of education, county technology school, or county college.

Technology Management Actions

a. Join MS-ISAC to monitor cyber threats: http://msisac.cisecurity.org and take advantage of their employee training resources.


c. Join GMIS International and NJ-GMIS– a US-based association for government IT leaders with a NJ chapter; this group is dedicated to providing best practice solution, professional development, conferences and networking opportunities: www.gmis.org and www.njgmis.org

d. Sign up for the AT&T ThreatTraq weekly video/audio podcast/RSS Feed for the latest in security news and trends: http://techchannel.att.com/showpage.cfm?threattraq

e. Test for data breaches regularly and make sure that your organization meets all compliance standards for any HIPPA, PCI and CJIS related services.

f. Be aware of government cyber security resources and use them as appropriate
   i. NJCCIC – the state website that coordinates state cyber security resources, including resources for conducting vulnerability assessments www.cyber.nj.gov/
   ii. NJ InfraGuard – a public and private sector alliance whose mission is to share information and protect critical infrastructures www.njinfragard.org/
   iii. N.J. State Police Cyber Crime Unit – the State Police unit that investigates cyber crimes - www.njsp.org/divorg/invest/cyber-crimes-unit.html
   iv. US Cert – a US government agency that provides security alerts (membership in this organization comes with with your agency’s participation in MS-ISAC) www.us-cert.gov/ and Cyber Resilience Review at www.us-cert.gov/ccubedvp/self-service-crr
   v. New Jersey Regional Computer Forensic Laboratory – an FBI managed facility that provides digital forensic services and training to any law enforcement agency in New Jersey www.njrclf.org/
Management Actions

a. Have your full-time IT manager take the Certified Government Chief Information Officer program through Rutgers-Newark: http://spaa.newark.rutgers.edu/cgcio

b. Consult with your technology staff to ensure that they have adequate resources for ongoing technical training and continuing education through online services such as: www.lynda.com, www.CBTnuggets.com, www.nhcomputerlearning.com, www.brighttalk.com/information-technology. In addition, they can learn security management basics at SANS Cyber Aces Online training www.cyberaces.org/.

c. Protect against cyber threats by conducting periodic IT audits, vulnerability assessments, and penetration/intrusion testing. A range of organizations offer these services: MS-ISAC, KnowBe4.com, and various local, commercial IT organizations. Consult with your cyber security insurer for guidance or support. See http://en.wikipedia.org/wiki/Information_technology_audit for an detailed overview of the subject.

Technical Competency Actions

a. Minimum for all systems: anti-virus, firewalls, anti-spam, anti-malware software running on all desktops

b. Backups! Stored on- and off-site (or in the cloud) as appropriate

c. Restrict user installation of applications (whitelisting)

d. Ensure that operating systems are patched with current updates

e. Ensure that software applications have current updates after testing to ensure they are compatible with operating system(s) in use.

f. Protect online financial transactions: to prevent inadvertent infection, social engineered hacks, and harmful downloads, dedicate a computer for financial transactions that prohibits email and general web-surfing

g. Periodically test system failure and disaster recovery plans

h. Restrict administrative privileges and regularly review them

Adopt Additional Cyber Hygiene Best Practices

a. Count: Know what’s connected to your network as well as what’s running on it.

b. Configure: Implement key security settings to help protect your systems.

c. Control: Limit and manage those who have admin privileges to change, bypass or override your security settings.

d. Patch: Regularly update all apps, software and operating systems.

e. Repeat: Make monitoring these priority items a routine to form a solid foundation of cybersecurity for your organization.

---

1 Center for Internet Security, https://www.cisecurity.org/about/CyberCampaign2014.cfm
Consider the Applicability of “Steps to Successful Cyber Risk Management”\(^2\) and Apply Accordingly

a. Manage incidents - Establish an incident response and disaster recovery policy. Produce and test incident management plans. Provide specialized training to members of the incident management team. Report criminal incidents to law enforcement agencies.

b. Limit privileges - Establish processes to manage accounts and limit the number of privileged account holders. Restrict user privileges and monitor user activity. Control access to activity and audit logs.

c. Control removable media - Develop a policy to control employee access to removable media. Limit media types and their use. Scan all media for malware before importing it onto the network.

d. Monitor - Establish a monitoring strategy and develop supporting policies. Continuously audit all technology systems and networks. Analyze logs for unusual activity that could indicate an attack; contract with third-party vendors to provide services as necessary.

e. Secure system configurations - Apply security patches to ensure that all systems are securely configured and maintained. Create a system inventory and define a baseline build for all devices.

f. Network security - Protect your networks against external and internal attacks. Manage the network perimeter. Filter out unauthorized access and malicious content. Monitor and test security controls.

**Additional Technical Actions as Appropriate and Applicable to the Organization**

a. Apply Table #1, “20 Key Security Actions for Server-based profiles” and Table #2, “20 Critical Security Controls for Effective Cyber Defense”

b. Adopt Bring Your Own Device/mobile system management practices - review online resources: [http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf](http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf)

**Table #1 – 20 Key Security Actions for Server-Based Profiles**

- **Identify your weaknesses.** Make sure every entry point is secured with passwords and encryption, and controlled to limit user access as appropriate. Force periodic password replacement and regular identity management

- **Install perimeter security solutions.** There are three types of network perimeter security measures your organization can take:
  - i. Firewalls – Prevent unauthorized Internet users from accessing your private network via the Internet
  - ii. Intrusion Detection Systems – Monitor and report on threats to your network
  - iii. Intrusion Prevention Programs – Stop threats as well as report on them

Installing a firewall can usually be accomplished without professional assistance. The more stringent intrusion detection and prevention solutions typically require in-house or third-party IT expertise.

- **Use a spam filter.** Your organization should install spam filtering software on computer or network devices.

---

servers. You may also choose to buy a dedicated appliance or outsource spam filtering to an online service provider. The software option is typically more budget-friendly, but online services may be more effective and more suitable for higher volumes of emails.

d. **Test your security systems periodically.** Conduct a formal intrusion test (“white-hat” hacking).

e. **Adopt intrusion or data breach policies** – make sure your technology staff understands it and know how to apply it. Test it periodically.

f. **Backup your data and key system files.** Identify the vital data you need to protect - accounting records, vendor information, user files, databases, worksheets, document files, etc. Then, choose from offline and offsite or online data backup solutions to ensure the security and availability of your critical information. Set a backup schedule and test your solutions regularly.

g. **Encrypt appropriate files, hard drives and backup disks.** By encrypting appropriate hardware and data, only people with a valid password will have access. It’s an important step.

h. **Adopt NIST CyberSecurity Framework.** Model your security planning along NIST recommendations: Identify, Protect, Detect, Respond, Recover

i. **Set up a virtual private network (VPN).** By creating a VPN, staff working from home or on the road using Wi-Fi in public won’t be exposing your network to security threats.

j. **Automate security updates.** Be aware of auto updates, they ensure devices will always have the most recent form of software and anti-virus programs installed. *But test as necessary to ensure compatibility with all applications before installing!*

k. **Restrict total access.** Don’t give all staff universal access to every part of your network. Protect sensitive files and databases with passwords that only your key people know.

l. **Monitor network traffic.** Install software or hardware that keeps an eye on who is visiting which sites and which of your computers they’re using. And periodically check the logs (yourself or a contractor)!

m. **Review your security periodically.** Stay aware of new security threats and improved solutions by visiting your security software/service vendor websites. As your technology profile evolves, you may need to take new security measures.

n. **Don’t host your website yourself.** Consider using a website hosting service that will take care of your website’s security needs and provide redundancy, which will allow your website to be properly restored if attacked.

o. **Keep software up-to-date.** Subscribe to update services and apply updates on a timely basis – test when appropriate before applying.

p. **Educate your IT staff about your security policy.** Create a policy that spells out what actions your employees should and shouldn’t take online and when managing emails. Make sure everyone knows what’s expected.

q. **Review vendor access.** Regularly review the access possessed by third-party vendors that run applications on your system; make sure only necessary access is granted; review system logs to make sure they have not accessed resources outside their limits.

r. **Audit offsite systems.** When using a third-party vendor’s premises in a cloud or software-as-a-
service environment, understand their security environment; ask for or require audits of their systems. Make sure they adhere to industry best practices and formalize this using contract documents.

s. **Carefully plan and implement mobile and Bring Your Own Device (BYOD) policies.** Review the 10 Commandments of [BYOD/Mobile system management](#) and apply as relevant.

t. **Know your 20 Critical Controls.** Initiated by the US government, 20 Critical Controls is a checklist of recommended security protocols used to prevent cyber attacks. Visit [www.sans.org/critical-security-controls/](http://www.sans.org/critical-security-controls/) to review and download your copy.

### Table #2 – 20 Critical Security Controls for Effective Cyber Defense

3

- Inventory authorized and unauthorized devices
- Inventory of authorized and unauthorized software
- Develop secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
- Continually assess and remediate system vulnerabilities
- Augment your system’s malware defenses
- Strengthen your system’s application software security
- Limit wireless access control
- Increase data recovery capability
- Fill the gaps in your staff’s IT knowledge with security skills assessments and appropriate training
- Develop secure configurations for network devices such as firewalls, routers, and switches
- Limit and control network ports, protocols and services
- Limit the the number of employees with administrative privileges
- Set up a boundary defense
- Maintain, monitor and analyze audit logs
- Control system access based on the need to know
- Monitor and control user accounts
- Protect data
- Establish a plan to deal with incident response and management
- Secure network engineering
- Adopt procedures for penetration testing and red team exercises

---

Note: This assessment addresses the range of technology risks facing a government organization. It can also be used to solely address the cyber risk component. Because of the subjectivity of evaluation from one entity to another and the absence of metrics for each of the variables below, the benchmarking is not intended for use in comparing one entity against another, nor the conformity of a particular technology environment against any set of rules or expectations.4

<table>
<thead>
<tr>
<th>Governance</th>
<th>1: Does not describe my organization at all ......5: Accurately describes my organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The governing body and senior management (governance team) are responsible for overseeing the development of a Technology Plan and confirming its implementation</td>
</tr>
<tr>
<td>2.</td>
<td>The governance team ensures that the Plan is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued</td>
</tr>
<tr>
<td>3.</td>
<td>The team demonstrate visible and active commitment to the implementation of the Plan</td>
</tr>
<tr>
<td>4.</td>
<td>Executives and managers are responsible for understanding at the appropriate level how technology risks could impact and originate from their activities</td>
</tr>
<tr>
<td>5.</td>
<td>Senior leadership understands who is responsible for managing cyber risk when managing security incidents</td>
</tr>
<tr>
<td>6.</td>
<td>The organization has access to technology and cyber expertise at its highest management levels</td>
</tr>
<tr>
<td>7.</td>
<td>The organization undertakes to continuously improve the integration of its technology risk management with its other risk management initiatives</td>
</tr>
<tr>
<td>8.</td>
<td>The chief executive has a clear decision path for action and communication in response to a significant security failure or accident</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Plan</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>The organization conducts comprehensive assessments of its vulnerabilities to internal and external risks appropriate for its size and technological profile</td>
</tr>
<tr>
<td>10.</td>
<td>The organization monitors the effectiveness of its risk management strategy</td>
</tr>
<tr>
<td>11.</td>
<td>The organization periodically internally verifies its compliance with rules and regulations</td>
</tr>
<tr>
<td>12.</td>
<td>The organization’s commitment to the Plan is reflected in its policies and practices</td>
</tr>
<tr>
<td>13.</td>
<td>Managers, employees and agents receive specific training on Plan elements, tailored to relevant needs and circumstances</td>
</tr>
<tr>
<td>14.</td>
<td>The organization has identified its data and information as vital assets, and organizes its Plan around the recognition that data and information have value that can be separately recognized and protected</td>
</tr>
<tr>
<td>15.</td>
<td>The risk management elements of the Plan includes all material third-party relationships and information flows</td>
</tr>
<tr>
<td>16.</td>
<td>The organization conducts comprehensive internal short- and long-term cyber risk impact assessments</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relationships</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization’s specific cyber risk management standards or industry best practices, in line with the Plan, and formalizes this requirement using contractual obligations</td>
</tr>
<tr>
<td>18.</td>
<td>The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents</td>
</tr>
<tr>
<td>19.</td>
<td>The risk management plan element includes all material third-party relationships and information flows</td>
</tr>
<tr>
<td>20.</td>
<td>Executed plans reflect technology services that meet the needs of the organization’s employees, constituents, clients.</td>
</tr>
</tbody>
</table>

Average (gives maturity stage) – total the numbers for each question and divide by 20. Total: \( \frac{\text{Match the number to the Stage description on Page 3}}{20} = \)

4 Adapted from World Economic Forum, 2012, Partnering for Cyber Resilience, C-Suite Executive Checklist
Best Practice and Resource Guide
For Achieving Technological Proficiency

FOR SOPHISTICATED* TECHNOLOGY PROFILE ORGANIZATIONS

*Sophisticated: Fully networked wired or wireless environment with a mix of owned and licensed, hosted and cloud applications, supporting specialized servers and robust technical management using well-trained staff and service providers.

Accompanying the Research Project
Managing Technology Risks through Technological Proficiency

Conducted by:
Bloustein Local Government Research Center
Rutgers University
www.blousteinlocal.rutgers.edu

For the:
Municipal Excess Liability Joint Insurance Fund
www.njmel.org
READ THIS FIRST: Instructions for Using this Guide

Understand that all “rules” and recommendations do not apply to every circumstance; use discretion and judgment to ensure that the user’s technology environment is consistent with the recommendations.

Users should also review the detailed explanation of technology governance and planning in the full Managing Technology Risks through Technological Proficiency report.

Goals of technology governance:

- Improve organizational accountability for results
- Strengthen working relationships between technology management, executive management, and working units
- Reduce operational risks/inefficiencies
- Attend to actions necessary for funding approval/Focus technology spending on established goals
- Establish reporting process: avoid problems or project overruns/failures stemming from false starts, scope creep or reactive re-prioritization
- Lead to limited technological complexity and greater systems integration
- Ensure an effective technology planning process

Technology governance includes the following elements, as appropriate to the organization. These steps should be carried out at least annually, and more frequently if necessary:

1. Establish governing entity: Established by the governing body, it defines the roles and responsibilities of the governance process, identifies those serving on it, and addresses the logistics of carrying out its obligations (meetings, relationship with administration and governing body); it needs to establish a reporting process that leads from technology management to executive management as well as to the governing body.

2. Establish technology planning process: identify the responsibilities of each individual, establish a timetable for preparation, review and approval, and tie it to the budget process. The Plan needs be tied to overall organization plans (to the extent they exist).

3. Adopt policies; find examples and adapt as necessary to local needs.
   a. Acceptable Use and Social Media Policy
   b. Internet Access Policy
   c. Data Breach Policy/Response Plan
   d. Email and Communications Policy
   e. Privacy Policy
   f. Contractor security practices
   g. Network Security Policy
   h. Cloud based software/storage solution
   i. Optional, depending on need: 1) Remote Access Policy; 2) BYOD Policy, 3) Encryption Policy

4. Assess technological risk maturity to establish what type of policies will be needed in order for the organization to improve along the continuum. (See Page 3)

5. Conduct a technology risk assessment and integrate it with the technology plan (identify, analyze, mitigate, review).
6. Establish technology management model: At this level, technology management requires its own governance model to address issues such as business application needs, technical architecture, infrastructure strategy and project management. Agencies should review the range of management models and choose the one that is consistent with the organization’s technical, application, infrastructure and staffing capacity needs.

Assess Technological Risk Maturity

Complete the “20 Questions – Technological Risk Maturity Assessment” questionnaire at the end of this guide. Match your average to the stage that best describes your organization. You should design your governance policies so that your organization will be able to through the levels over time until you are able to reach stage 4 or 5.

Stage 1: Unaware: The organization sees technology management as largely irrelevant, and it does not form part of the organization's management process. The organization is not aware of its level of interconnectedness and its risks. They are doing nothing or consciously ignoring the risks.

Stage 2: Fragmented: Management recognizes technology issues as a potential source of risk, and has limited insight to its technology management practices. The organization has a “siloh approach to technology and its management, with fragmented and incidental reporting.

Stage 3: Top Down: Management has set the tone for technology management and has initiated standards, but does not view technology management as a critical issue.

Stage 4: Managed: The organization's leadership takes full ownership of technology management, has developed policies and plans, and has defined responsibilities and oversight mechanisms. It makes calculated decisions on technological needs. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

Stage 5: Optimized: The organization is highly connected to its community, peers and partners, sharing information, meeting citizen and client expectations, and coordinating technology risk mitigation as part of its day-to-day operations. Its people show exceptional technological acumen and cyber-awareness and the organization is a leader in technology management.
• Technology planning requires the use of resources: time, attention and in some cases money. How much of each depends on your organization’s governance model, its risk maturity and its technology profile. Find something that works for your agency.

• The following are the essential elements of any Technology Plan:
  - **Identify your current technology environment**: technology uses/applications, profile, staffing competencies, metrics, hardware/software inventory, management model, operating status (i.e., growth, stable, reductions); identify risks
  - **Establish your desired technology environment**: match technology to organizational goals by consulting with staff as well as internal and external stakeholders. Identify their interests; scan technology horizons for opportunities
  - **Identify the gap** between your current environment and your desired environment
  - **Identify strategies to fill the gap**: match strategies to available resources (time, attention, money) and continually review and modify them with the governance process (i.e., budget) until they all align
  - **Recommend risk mitigation** strategies to your organization’s governance entity
  - **Implement**
  - **Measure** results (identify metrics or expected outcomes)
  - **Repeat** as necessary to meet goals

**Apply these best practices of cyber hygiene:**

  a. Only utilize business-related websites
  b. Check with the sender if you are not expecting an attachment
  c. Cooperate with IT management’s instructions regarding security patches
  d. NEVER open suspicious attachments or unexpected email
  e. NEVER install hardware or software without IT approval
  f. NEVER download any programs without IT approval
  g. NEVER use a USB drive whose source is uncertain
  h. Understand and apply your organization’s technology policies
  i. Only uses services and products approved by IT management
  j. Use strong passwords:
     - At least eight characters
     - Use a phrase relevant to the user
     - Include a minimum of 2 numbers
     - Never write down (unless password protected) or divulge your password
     - Change your password every 30-90 days
Cyber Hygiene Resource Guide

- Municipal Excess Liability Fund training resources: http://tinyurl.com/NJMEL-Tech-Risks
- SANS Secured Human: www.securingthehuman.org
- MS-ISAC guides at: http://msisac.cisecurity.org/resources/guides/
- Security Mentor: www.securitymentor.com/
- www.StopThinkConnect.org
- www.StaySafeOnline.org
- KnowBe4 - www.knowbe4.com

In addition, security training resources may be available through your local public library, board of education, county technology school or county college.

Sophisticated Technical Competency

Technology Management Actions

a. Join MS-ISAC to monitor cyber threats: http://msisac.cisecurity.org and take advantage of their employee training resources.


c. Join GMIS International and NJ-GMIS– a US-based association for government IT leaders with a NJ chapter; this group is dedicated to providing best practice solution, professional development, conferences and networking opportunities: www.gmis.org and www.njgmis.org

d. Sign up for the AT&T ThreatTraq weekly video/audio podcast/RSS Feed for the latest in security news and trends: http://techchannel.att.com/showpage.cfm?threattraq

e. Test for data breaches regularly and make sure that your organization meets all compliance standards for any HIPPA, PCI and CJIS related services.

f. Be aware of government cyber security resources and use them as appropriate
   i. NJCCIC – the state website that coordinates state cyber security resources, including resources for conducting vulnerability assessments www.cyber.nj.gov/. 
   ii. NJ InfraGuard – a public and private sector alliance whose mission is to share information and protect critical infrastructures www.njinfragard.org/
   iii. N.J. State Police Cyber Crime Unit – the State Police unit that investigates cyber crimes - www.njsp.org/divorg/invest/cyber-crimes-unit.html
   iv. US Cert – a US government agency that provides security alerts (membership in this organization comes with with your agency’s participation in MS-ISAC) www.us-cert.gov/ and Cyber Resilience Review at www.us-cert.gov/ccubedvp/self-service-crr
   v. New Jersey Regional Computer Forensic Laboratory – an FBI managed facility that provides digital forensic services and training to any law enforcement agency in New Jersey www.njrcfl.org/
Management Actions

a. Have your full-time IT manager take the Certified Government Chief Information Officer program through Rutgers-Newark: http://spaa.newark.rutgers.edu/cgio

b. Consult with your technology staff to ensure that they have adequate resources for ongoing technical training and continuing education through online services such as: www.lynda.com, www.CBTnuggets.com, www.nhcomputerlearning.com, www.brighttalk.com/information-technology. In addition, they can learn security management basics at SANS Cyber Aces Online training www.cyberaces.org/.

c. Protect against cyber threats by conducting periodic IT audits, vulnerability assessments, and penetration/intrusion testing. A range of organizations offer these services: MS-ISAC, KnowBe4.com, and various local, commercial IT organizations. Consult with your cyber security insurer for guidance or support. See http://en.wikipedia.org/wiki/Information_technology_audit for an detailed overview of the subject.

Technical Competency Actions

a. Minimum for all systems: anti-virus, firewalls, anti-spam, anti-malware software running on all desktops

b. Backups! Stored on- and off-site (or in the cloud) as appropriate

c. Restrict user installation of applications (whitelisting)

d. Ensure that operating systems are patched with current updates

e. Ensure that software applications have current updates after testing to ensure they are compatible with operating system(s) in use.

f. Protect online financial transactions: to prevent inadvertent infection, social engineered hacks, and harmful downloads, dedicate a computer for financial transactions that prohibits email and general web-surfing

g. Periodically test system failure and disaster recovery plans

h. Restrict administrative privileges and regularly review them

Adopt Additional Cyber Hygiene Best Practices

a. Count: Know what’s connected to your network as well as what’s running on it.

b. Configure: Implement key security settings to help protect your systems.

c. Control: Limit and manage those who have admin privileges to change, bypass or override your security settings.

d. Patch: Regularly update all apps, software and operating systems.

e. Repeat: Make monitoring these priority items a routine to form a solid foundation of cybersecurity for your organization.

---

1 Center for Internet Security, https://www.cisecurity.org/about/CyberCampaign2014.cfm
Consider the Applicability of “Steps to Successful Cyber Risk Management”\(^2\) and Apply Accordingly

a. Manage incidents - Establish an incident response and disaster recovery policy. Produce and test incident management plans. Provide specialized training to members of the incident management team. Report criminal incidents to law enforcement agencies.

b. Limit privileges - Establish processes to manage accounts and limit the number of privileged account holders. Restrict user privileges and monitor user activity. Control access to activity and audit logs.

c. Control removable media - Develop a policy to control employee access to removable media. Limit media types and their use. Scan all media for malware before importing it onto the network.

d. Monitor - Establish a monitoring strategy and develop supporting policies. Continuously audit all technology systems and networks. Analyze logs for unusual activity that could indicate an attack; contract with third-party vendors to provide services as necessary.

e. Secure system configurations - Apply security patches to ensure that all systems are securely configured and maintained. Create a system inventory and define a baseline build for all devices.

f. Network security - Protect your networks against external and internal attacks. Manage the network perimeter. Filter out unauthorized access and malicious content. Monitor and test security controls.

Take Additional Technical Actions as Appropriate and Applicable to the Organization

a. Apply Table #1, “20 Key Security Actions for Server-based profiles“ and Table #2, “20 Critical Security Controls for Effective Cyber Defense“

b. Apply Table #3, NIST Recommendations to Share Cyber Threat Information

c. Adopt Bring Your Own Device/mobile system management practices - review online resources: http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf

d. Review Table #4, “The Types of Network and User Controls” and apply as relevant.

e. Consider implementing a technology control environment:
   - NIST Cyber Framework – federal government recommendations for improving critical infrastructure for increased cyber security www.nist.gov/cyberframework/
   - ISACA – an association of IT professionals that manages the development, adoption and use of globally accepted industry-leading knowledge and practices for all enterprises that use information systems. Known as “COBIT 5” www.isaca.org
   - COSO – this committee has established a common internal control model against which companies and organizations may assess their own control systems www.coso.org/guidance.htm

---
Table #1 – 20 Key Security Actions for Server-Based Profiles

a. **Identify your weaknesses.** Make sure every entry point is secured with passwords and encryption, and controlled to limit user access as appropriate. Force periodic password replacement and regular identity management.

b. **Install perimeter security solutions.** There are three types of network perimeter security measures your organization can take:
   
   i. **Firewalls** – Prevent unauthorized Internet users from accessing your private network via the Internet
   
   ii. **Intrusion Detection Systems** – Monitor and report on threats to your network
   
   iii. **Intrusion Prevention Programs** – Stop threats as well as report on them
   
   Installing a firewall can usually be accomplished without professional assistance. The more stringent intrusion detection and prevention solutions typically require in-house or third-party IT expertise.

c. **Use a spam filter.** Your organization should install spam filtering software on computer or network servers. You may also choose to buy a dedicated appliance or outsource spam filtering to an online service provider. The software option is typically more budget-friendly, but online services may be more effective and more suitable for higher volumes of emails.

d. **Test your security systems periodically.** Conduct a formal intrusion test (“white-hat” hacking).

e. **Adopt intrusion or data breach policies** – make sure your technology staff understands it and know how to apply it. Test it periodically.

f. **Backup your data and key system files.** Identify the vital data you need to protect - accounting records, vendor information, user files, databases, worksheets, document files, etc. Then, choose from offline and offsite or online data backup solutions to ensure the security and availability of your critical information. Set a backup schedule and test your solutions regularly.

g. **Encrypt appropriate files, hard drives and backup disks.** By encrypting appropriate hardware and data, only people with a valid password will have access. It’s an important step.

h. **Adopt NIST CyberSecurity Framework.** Model your security planning along NIST recommendations: Identify, Protect, Detect, Respond, Recover

i. **Set up a virtual private network (VPN).** By creating a VPN, staff working from home or on the road using Wi-Fi in public won’t be exposing your network to security threats.

j. **Automate security updates.** Be aware of auto updates, they ensure devices will always have the most recent form of software and anti-virus programs installed. *But test as necessary to ensure compatibility with all applications before installing!*

k. **Restrict total access.** Don’t give all staff universal access to every part of your network. Protect sensitive files and databases with passwords that only your key people know.

l. **Monitor network traffic.** Install software or hardware that keeps an eye on who is visiting which sites and which of your computers they’re using. And periodically check the logs (yourself or a contractor)!

m. **Review your security periodically.** Stay aware of new security threats and improved solutions by visiting your security software/service vendor websites. As your technology profile evolves, you may
For SOPHISTICATED Technology Profile Organizations

need to take new security measures.

n. **Don’t host your website yourself.** Consider using a website hosting service that will take care of your website’s security needs and provide redundancy, which will allow your website to be properly restored if attacked.

o. **Keep software up-to-date.** Subscribe to update services and apply updates on a timely basis – test when appropriate before applying.

p. **Educate your IT staff about your security policy.** Create a policy that spells out what actions your employees should and shouldn’t take online and when managing emails. Make sure everyone knows what’s expected.

q. **Review vendor access.** Regularly review the access possessed by third-party vendors that run applications on your system; make sure only necessary access is granted; review system logs to make sure they have not accessed resources outside their limits.

r. **Audit offsite systems.** When using a third-party vendor’s premises in a cloud or software-as-a-service environment, understand their security environment; ask for or require audits of their systems. Make sure they adhere to industry best practices and formalize this using contract documents.

s. **Carefully plan and implement mobile and Bring Your Own Device (BYOD) policies.** Review the 10 Commandments of [BYOD/Mobile system management](http://www.counciloncybersecurity.org/critical-controls/) and apply as relevant.

t. **Know your 20 Critical Controls.** Initiated by the US government, 20 Critical Controls is a checklist of recommended security protocols used to prevent cyber attacks. Visit [www.sans.org/critical-security-controls/](http://www.sans.org/critical-security-controls/) to review and download your copy.

### Table #2 – 20 Critical Security Controls for Effective Cyber Defense

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Inventory authorized and unauthorized devices</td>
<td></td>
</tr>
<tr>
<td>b. Inventory of authorized and unauthorized software</td>
<td></td>
</tr>
<tr>
<td>c. Develop secure configurations for hardware and software on mobile devices, laptops, workstations, and servers</td>
<td></td>
</tr>
<tr>
<td>d. Continually assess and remediate system vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>e. Augment your system’s malware defenses</td>
<td></td>
</tr>
<tr>
<td>f. Strengthen your system’s application software security</td>
<td></td>
</tr>
<tr>
<td>g. Limit wireless access control</td>
<td></td>
</tr>
<tr>
<td>h. Increase data recovery capability</td>
<td></td>
</tr>
<tr>
<td>i. Fill the gaps in your staff’s IT knowledge with security skills assessments and appropriate training</td>
<td></td>
</tr>
<tr>
<td>j. Develop secure configurations for network devices such as firewalls, routers, and switches</td>
<td></td>
</tr>
<tr>
<td>k. Limit and control network ports, protocols and services</td>
<td></td>
</tr>
</tbody>
</table>

---

For SOPHISTICATED Technology Profile Organizations

- Limit the number of employees with administrative privileges
- Set up a boundary defense
- Maintain, monitor and analyze audit logs
- Control system access based on the need to know
- Monitor and control user accounts
- Protect data
- Establish a plan to deal with incident response and management
- Secure network engineering
- Adopt procedures for penetration testing and red team exercises

**Table #3 – NIST Recommendations to Share Cyber Threat Information**

Organizations should:

a. Perform an inventory that catalogs the information an organization possesses and the information that it is capable of producing. The inventory should also document the circumstances in which the information could be shared.

b. Exchange threat intelligence, tools and techniques with sharing partners. When sharing threat intelligence, organizations learn from each other; gain a more complete understanding of an adversary’s tactics, technique and procedures; craft effective strategies to protect systems; and take action, either independently or collectively, to address known threats.

c. Employ open, standard data formats and transport protocols to ease the efficient and effective exchange of cyber-threat information. This fosters interoperability and allows different products, data repositories and tools to rapidly exchange data.

d. Enhance their cybersecurity posture and maturity by augmenting local data collection, analysis and management processes using information from outside sources. This can help organizations develop a deeper understanding about activities on their networks, identify cyber-attack campaigns and better detect blended threats that use multiple methods of attack.

e. Define an approach to cybersecurity that adapts to the lifecycle of an attack by developing defensive measures that detect, limit or prevent reconnaissance and delivery of malicious payloads. This adaptive approach also should mitigate the execution of exploits that allow an adversary to establish or maintain a persistent presence on an organization's network.

f. Ensure that the resources required for continuing participation in a sharing community are available. Participation might require an organization, for example, to commit personnel; deliver training; and provide hardware, software, services and other infrastructure needed to support continuing data collection, storage, analysis and dissemination.

g. Protect sensitive information by maintaining a continuing awareness of information security, vulnerabilities and threats. Organizations should implement the security controls necessary to

---

For SOPHISTICATED Technology Profile Organizations

- protect its sensitive information, enforce its information-sharing rules and ensure that information received from external sources is protected in accordance with applicable data-sharing agreements.

- Establish the foundational infrastructure necessary to maintain their cybersecurity posture and clearly identify the roles and responsibilities for installing, operating and maintaining these capabilities. Organizations should have basic asset, vulnerability and configuration management capabilities in place to ensure that they can monitor and manage the hardware and software on their networks and ensure that vulnerabilities are patched in a timely way.

**Table #4 – Types of Network and User Controls**

a. Firewalls  
b. Email security and spam filtering  
c. Endpoint protection (antivirus, anti-spyware)  
d. Virtual private networks  
e. Data encryption  
f. Gateway antivirus or anti-malware software  
g. Patch management  
h. Intrusion prevention or intrusion detection; wireless security enforcement  
i. Log analysis, security event management or security information management  
j. Identity/credential management  
k. Vulnerability assessment or penetration testing  
l. Web application firewalls  
m. Data loss prevention  
n. Mobile device or application management  
o. Portable device security  
p. Network access controls

---

# 20 Questions – Technological Risk Maturity Assessment Checklist

*Note: This assessment addresses the range of technology risks facing a government organization. It can also be used to address just the cyber risk component. Because the evaluation is subjective and will vary from one entity to another, and in the absence of metrics for each of the variables below, these benchmarks are not intended for use in comparing one entity against another. In addition, this assessment is not intended to promote one particular technology model or to advocate against any set of rules or expectations.*

<table>
<thead>
<tr>
<th>Governance</th>
<th>1: Does not describe my organization at all…5: Accurately describes my organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The governing body and senior management (governance team) are responsible for overseeing the development of a technology plan and confirming its implementation</td>
</tr>
<tr>
<td>2.</td>
<td>The governance team ensures that the plan is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued</td>
</tr>
<tr>
<td>3.</td>
<td>The team demonstrates visible and active commitment to the implementation of the plan</td>
</tr>
<tr>
<td>4.</td>
<td>Executives and managers are responsible for understanding at the appropriate level how technology risks could impact the organization and originate from their activities</td>
</tr>
<tr>
<td>5.</td>
<td>Senior leadership understands who is responsible for mitigating cyber risk when managing security incidents</td>
</tr>
<tr>
<td>6.</td>
<td>The organization has access to technology and cyber expertise at its highest management level</td>
</tr>
<tr>
<td>7.</td>
<td>The organization undertakes to continuously improve the integration of its technology risk management plan with its other risk management initiatives</td>
</tr>
<tr>
<td>8.</td>
<td>The chief executive has a clear path for action and communication in response to a significant security failure or accident</td>
</tr>
</tbody>
</table>

| Plan | |
| 9. | The organization conducts comprehensive assessments of its vulnerabilities to internal and external risks appropriate for its size and technological profile |
| 10. | The organization monitors the effectiveness of its risk management strategy |
| 11. | The organization periodically internally verifies its compliance with rules and regulations |
| 12. | The organization’s commitment to the Plan is reflected in its policies and practices |
| 13. | Managers, employees and agents receive specific training on plan elements, tailored to relevant needs and circumstances |
| 14. | The organization has identified its data and information as vital assets, and organizes its plan around the recognition that data and information have value that can be separately recognized and protected |
| 15. | The risk management elements of the plan includes all material third-party relationships and information flows |
| 16. | The organization conducts comprehensive internal short- and long-term cyber risk impact assessments |

| Relationships | |
| 17. | The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization’s specific cyber risk management standards or industry best practices, in line with the plan, and formalizes this requirement using contractual obligations |
| 18. | The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents |
| 19. | The risk management plan element includes all material third-party relationships and information flows |
| 20. | Executed plans reflect technology services that meet the needs of the organization’s employees, constituents, clients. |

**Average (gives maturity stage)** – total the numbers for each question and divide by 20. **Total:** 

\[
\frac{\text{Total}}{20} = \text{Average (gives maturity stage)}
\]

---

Adapted from World Economic Forum, 2012, Partnering for Cyber Resilience, C-Suite Executive Checklist

© 2015, Municipal Excess Liability Joint Insurance Fund and Rutgers, the State University
The Bloustein Local Government Research Center

New Jersey is served by more than 1,500 distinct local government agencies: municipalities, school districts, utilities, counties, and more. Yet, even with this wealth of opportunity, precious little substantive research as been done within the local government environment to inform some of our state’s most pressing policy issues.

The Bloustein Local Government Research Center, or Bloustein Local http://blousteinlocal.rutgers.edu/, serves as a focal point and engages in a range of services, including:

- Encouraging and conducting applied and academic research on local government fiscal and administrative issues, emphasizing application and support to New Jersey local government.

- Developing resources that can assist others in conducting research and analysis.

- Organizing and hosting conferences and symposia on New Jersey local government fiscal and administrative issues.

- Supporting New Jersey local government fiscal and administrative policy development, implementation, and analysis through contract research and on-call advice for organizations and institutions that engage in local government policy setting and policymaking.

- Promoting and increasing public understanding of local government issues by partnering with and supporting civic and media organizations that inform and educate the public on local government matters.

A list of the Center’s current projects may be found online at http://blousteinlocal.rutgers.edu/projects/.

About the Author

Marc H. Pfeiffer retired in 2012 from a 37-year career in New Jersey local government administration, having served as a municipal administrator in several municipalities, and 26 years of service in the State’s local government oversight agency, the Division of Local Government Services. At DLGS he served as Deputy Director for 14 years, and periodically as Acting Director.

Marc has broad experience in many areas of local government policy and administration, including specific expertise in areas such as finance and property taxation, public procurement, shared services and consolidation, technology, energy, labor relations, and general government administration. He also has deep experience in the legislative process and as a regulatory officer. He is currently engaged in research concerning the use of technology in local government.

In addition to participating in Bloustein Local, Marc makes his extensive government experience available as a guest lecturer at the Bloustein School and other collaborative efforts. He is also assisting the Rutgers School of Public Affairs and Administration with the State’s Certified Public Manager Program in curriculum development and instruction. He can be reached at marc.pfeiffer@rutgers.edu.