Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

Getting Started With The MEL's Cyber Risk Management Program 2nd Edition

Step-By-Step

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL · MEL

Secure Data Consulting Services

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

The availability of Cyber Insurance is becoming very restrictive, and insurers are cancelling coverage for entities that do not implement safeguards to protect themselves from cyber-attacks.

We may actually find ourselves in a position where insurers require compliance with these standards to be eligible for coverage.

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

- **Introduction**
- **Differences**
  - ✓Tier 1
  - ✓Tier 2
  - ✓Tier 3
- **Certification**
- **Financial Impact**
- **Deductible Reimbursement Certification**
- **Program Rollout**
  - ✓Documents
  - ✓Process
  - ✓Gap Assessment & Actionable Report
- **Financial Assistance**
- **Questions**

Introduction

- **The MEL has revised its Cyber Risk Management Program to reduce the potential risk of a cyber incident and improve the overall security posture of its member.**

- **The new program consist of 3 Tiers**

Tier 1	Tier 2	Tier 3
Information Backups	Server Security	Network Segmentation
Security Patches and Updates	Access Privilege Controls	Remote Access Policy - MFA
Defensive Software	Technology Support	Password Integrity
Security Awareness Training	System and Event Logging	System and Event Logging - Review
Password Management	Protected Information	Third-Party Risk Management
Email Warning Label	Remote Access - VPN	
Cyber Incident Response Plan	Leadership Expertise	
Technology Practice Policy	IT Business Continuity Planning	
Government Cyber Membership	Banking Controls	

Differences – Tier 1

Tier 1	
Information Backups	Same
Security Patches and Updates	Same
Defensive Software	Same
Security Awareness Training	Same
New Password Management	Two password options – MEL's Requirements or NIST Standards
New Email Warning Label	Email banner to identify external incoming emails
New Cyber Incident Response Plan	Same
New Technology Practice Policy	Adoption of Tier 1 Technology Policy
Government Cyber Membership	Register with NJCCIC and MS-ISAC

NJCCIC – New Jersey Cybersecurity & Communications Integration Cell
MS-ISAC – Multi-State Information Sharing & Analysis Center

Differences – Password Management

Two Flavors

MEL's Minimal Requirements

Change Frequency

Network users' passwords are updated every three (3) months.

Construction

- ✓ Passwords must be a minimum of ten (10) characters.
- ✓ Passwords must be unique from passwords used on all other programs, websites, devices, etc., both personal and work.
- ✓ Sequential or repetitive characters of more than two in succession are not to be permitted.
  - Example: "123", "AAA", etc.
- ✓ Commonly used passwords are not to be permitted.
  - Example, "password", "123456789", "abc123", etc.
- ✓ Context-specific words are not to be permitted.
  - Example, the name of the application or website being logged into.

Failed Login Lockout

- ✓ The user account shall be locked out after five (5) failed attempts for a period of no less than 30 minutes.

NIST Standard 800-63B

Change Frequency

Only change if there is evidence of compromise

Construction

- ✓ Length - 8 characters minimum to at least 64 characters maximum
- ✓ Password
  - Suggest users use "memorized secrets" instead of passwords
  - Memorized Secrets are secret values intended to be chosen and memorized by the user; something you know.
- ✓ Screening **-** Screen passwords against a list of known compromised passwords
- ✓ Composition Restrictions – Do not allow
  - Dictionary words
  - Repetitive or sequential characters
  - Context-specific words (i.e. service name or username)
- ✓ Composition Minimums - Skip character composition rules
- ✓ Hints - Disable password hints and knowledge-based security questions
- ✓ Copy & Paste - Allow copying and pasting passwords from a password manager
- ✓ Other Characters - Allow ASCII and UNICODE, including emojis

Failed Login Lockout

- ✓ Limit the number of failed authentication attempts

Differences – Email Warning Label

Email warning labels, reduces the possibility of a spoofed email and social engineering scams by identifying emails that are coming from outside the organization.

Easy and cheap to implement – No Brainer !

Example:

CAUTION:

This email originated from outside of our email domain. Do not click on links or open attachments unless you recognize the sender and know the content is safe. If unsure, do not reply to this email and call the sender directly.

Differences –
Technology Practice Policy

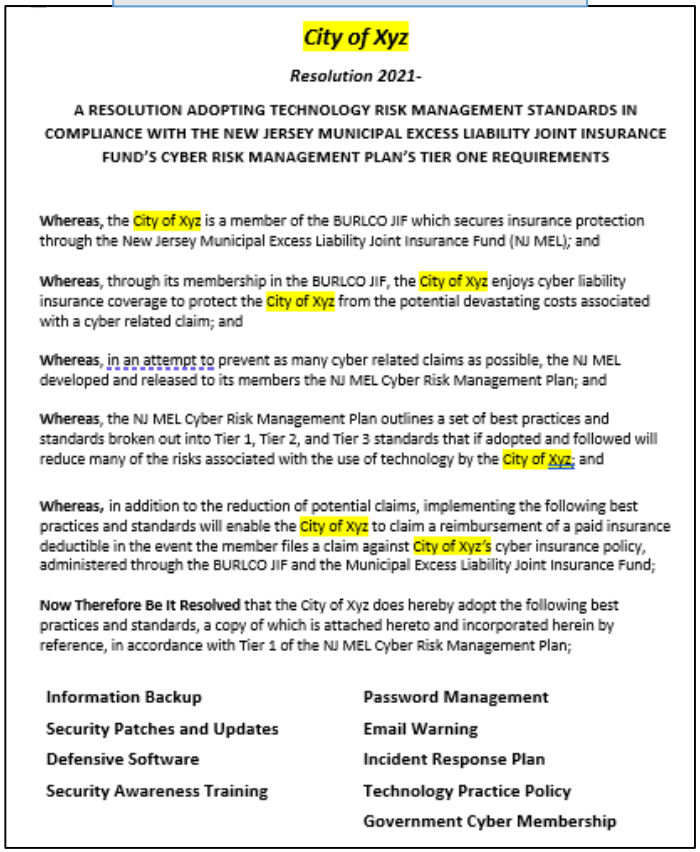
Ensures that management/governing bodies adopt a Technology Practice Policy that includes all the subject items outlined in the MEL Cyber Risk Management Program.

This can be done via a resolution and resolution templates have been developed for the JIF.

There are three resolutions for adoption:

- ✓ Tier 1
- ✓ Tier 2
- ✓ Tier 3

Sample Tier 1 Resolution



City of Xyz

Resolution 2021-

A RESOLUTION ADOPTING TECHNOLOGY RISK MANAGEMENT STANDARDS IN COMPLIANCE WITH THE NEW JERSEY MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND'S CYBER RISK MANAGEMENT PLAN'S TIER ONE REQUIREMENTS

Whereas, the City of Xyz is a member of the BURLCO JIF which secures insurance protection through the New Jersey Municipal Excess Liability Joint Insurance Fund (NJ MEL); and

Whereas, through its membership in the BURLCO JIF, the City of Xyz enjoys cyber liability insurance coverage to protect the City of Xyz from the potential devastating costs associated with a cyber related claim; and

Whereas, in an attempt to prevent as many cyber related claims as possible, the NJ MEL developed and released to its members the NJ MEL Cyber Risk Management Plan; and

Whereas, the NJ MEL Cyber Risk Management Plan outlines a set of best practices and standards broken out into Tier 1, Tier 2, and Tier 3 standards that if adopted and followed will reduce many of the risks associated with the use of technology by the City of Xyz; and

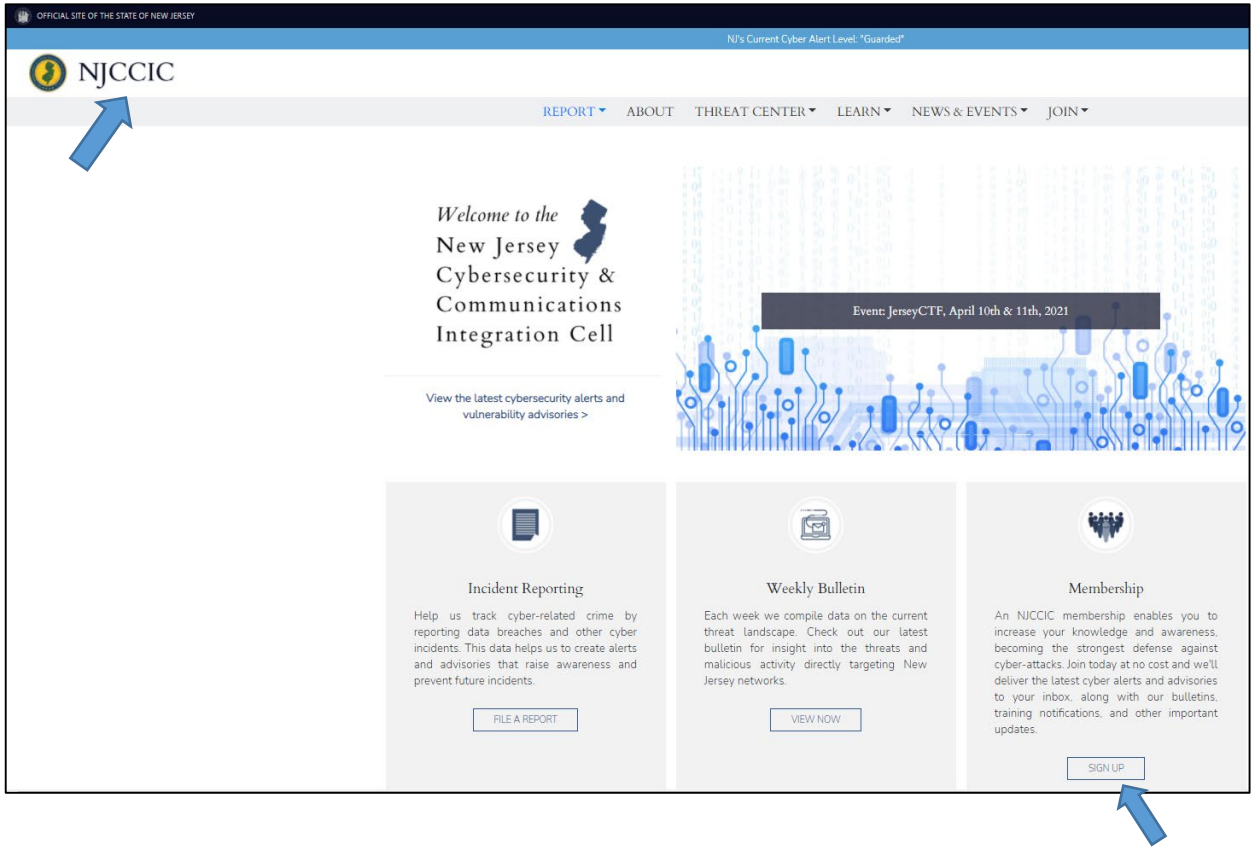
Whereas, in addition to the reduction of potential claims, implementing the following best practices and standards will enable the City of Xyz to claim a reimbursement of a paid insurance deductible in the event the member files a claim against City of Xyz's cyber insurance policy, administered through the BURLCO JIF and the Municipal Excess Liability Joint Insurance Fund;

Now Therefore Be It Resolved that the City of Xyz does hereby adopt the following best practices and standards, a copy of which is attached hereto and incorporated herein by reference, in accordance with Tier 1 of the NJ MEL Cyber Risk Management Plan;

Information Backup	**Password Management**
Security Patches and Updates	**Email Warning**
Defensive Software	**Incident Response Plan**
Security Awareness Training	**Technology Practice Policy**
	Government Cyber Membership

Differences –
Government Cyber Membership

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future



Free & Easy!!

NJCCIC
https://www.cyber.nj.gov/

Ensures that member stays current with cyber threat notifications and relevant information.

Differences –
Government Cyber Membership

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

Free & Easy!!

MS-ISAC
https://www.cisecurity.org/ms-isac/

Ensures that member stays current with cyber threat notifications and relevant information.

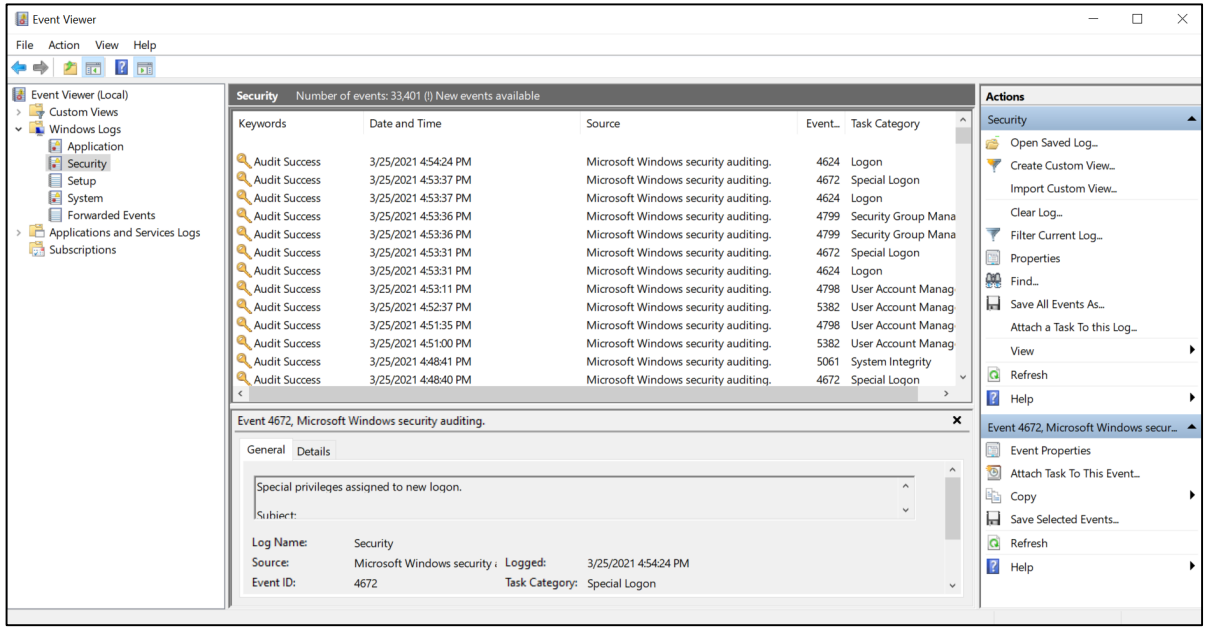
Differences – Tier 2

	Tier 2	
	Server Security	Same
	Access Privilege Controls	Same
	Technology Support	Same
New	System and Event Logging	System activities, information security events, and system utilization and performance need to be monitored. Microsoft natively maintains three logs; System, Application, & Security
	Protected Information	Same
New	Remote Access - VPN	Use a VPN connection when remotely connecting to the municipal network.
	Leadership Expertise	Same
New	IT Business Continuity Planning	Use the Business Continuity Guidelines to develop a Business Continuity Plan suited for your operations.
New	Banking Controls	Implement internal controls to minimize fraudulent banking transactions.
	Technology Practice Policy	Adoption of Tier 2 Technology Policy

Differences –
System & Event Logging

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

The purpose of System and Event Logging is to capture system activities, information security events, system utilization and performance in a pre-emptive manner.



In Windows 10, The Event Viewer helps you monitor apps and system components as well as troubleshoot problems.

There are various logs, but the primary ones are:

- ✓Application
- ✓Security
- ✓Systems

Your Technology Professional should review these logs quarterly.

https://www.windowscentral.com/how-use-event-viewer-windows-10

Differences –
Remote Access - VPN

The purpose of the Remote Access Policy is to secure remote access connectivity into the member's network using a Virtual Private Network (VPN).

Consult with your Technology Professional and use the guidelines in the Master Technology Policy when implementing a VPN solution.

The VPN connection will encrypt your data traffic, making it much more difficult for hackers and other parties to intercept and view your information.

1. The VPN software on your computer encrypts your data traffic and sends it (via your Internet Service Provider) to the VPN server through a secure connection.

2. The encrypted data from your computer is decrypted by the VPN server.

3. The VPN server will send your data on to the internet and receive a reply, which is meant for you.

4. The traffic is then encrypted again by the VPN-server and is sent back to you.

5. The VPN-software on your device will decrypt the data so you can understand and use it.

Differences –
IT Business Continuity Planning

The purpose of the IT Business Continuity Plan is to ensure the member is prepared and can effectively recover from a disruption in service, including cyber breaches, denial of service or ransomware attacks, and be able to restore continuity of operations.

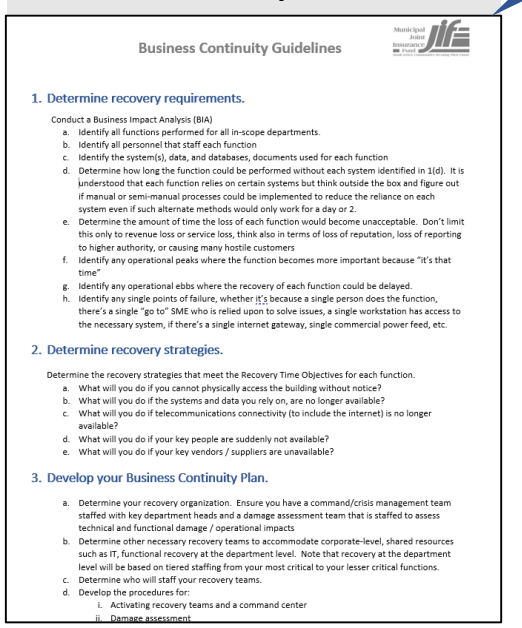
When developing an IT Business Continuity Plan you need to consider the following:

Recovery Strategies

1. Identify all operational functions
2. Identify key support personnel and communications plan
3. Prioritize based on Recovery Time Objectives (RTOs)
4. Consider and accommodate the following impacts:
   - ✓ Loss of Computing (Systems and Data)
   - ✓ Loss of Telecommunications
   - ✓ Loss of Personnel
   - ✓ Denial of Physical Access
   - ✓ Critical vendors' services

Use the Business Continuity Planning Guidelines as reference to help you develop your Business Continuity Plan

This can be found on the JIF website



Business Continuity Guidelines

1. Determine recovery requirements.

Conduct a Business Impact Analysis (BIA)

a. Identify all functions performed for all in-scope departments.
b. Identify all personnel that staff each function
c. Identify the system(s), data, and databases, documents used for each function
d. Determine how long the function could be performed without each system identified in 1(d). It is understood that each function relies on certain systems but think outside the box and figure out if manual or semi-manual processes could be implemented to reduce the reliance on each system even if such alternate methods would only work for a day or 2.
e. Determine the amount of time the loss of each function would become unacceptable. Don't limit this only to revenue loss or service loss, think also in terms of loss of reputation, loss of reporting to higher authority, or causing many hostile customers
f. Identify any operational peaks where the function becomes more important because "it's that time"
g. Identify any operational ebbs where the recovery of each function could be delayed.
h. Identify any single points of failure, whether it's because a single person does the function, there's a single "go to" SME who is relied upon to solve issues, a single workstation has access to the necessary system, if there's a single internet gateway, single commercial power feed, etc.

2. Determine recovery strategies.

Determine the recovery strategies that meet the Recovery Time Objectives for each function.

a. What will you do if you cannot physically access the building without notice?
b. What will you do if the systems and data you rely on, are no longer available?
c. What will you do if telecommunications connectivity (to include the internet) is no longer available?
d. What will you do if your key people are suddenly not available?
e. What will you do if your key vendors / suppliers are unavailable?

3. Develop your Business Continuity Plan.

a. Determine your recovery organization. Ensure you have a command/crisis management team staffed with key department heads and a damage assessment team that is staffed to assess technical and functional damage / operational impacts
b. Determine other necessary recovery teams to accommodate corporate-level, shared resources such as IT, functional recovery at the department level. Note that recovery at the department level will be based on tiered staffing from your most critical to your lesser critical functions.
c. Determine who will staff your recovery teams.
d. Develop the procedures for:
   i. Activating recovery teams and a command center
   ii. Damage assessment

Differences – Banking Controls

The purpose of implementing internal Banking Controls is to prevent or reduce fraudulent banking transactions.

When implementing the internal banking controls, use the following guidelines:

- Use Multi-Factor Authentication when accessing the bank's system and making financial transactions, where available.
- Establish procedures requiring multiple approvals for request to change banking information.
- Establish procedures requiring multiple approvals and source verification for financial transaction requests over $5,000.
- Ensure that relevant personnel know and understand these procedures.

Easy and cheap to implement – No Brainer !

Differences – Tier 3

Tier 3	
Network Segmentation	Divide the network into multiple zones or sub-networks and apply security protocols to each zone. The member shall consider isolating the network by key business units or sensitive departments, such as finance and human resources.
Remote Access – MFA (Multi Factor Authentication)	Enhance the security level by adding a second layer of authentication when remotely accessing the member's network
Password Integrity	Frequently validate users' emails and passwords to ensure they have not been compromised. This can be done by checking your credentials against an email breach service, such as HaveIBeenPwned. https://haveibeenpwned.com/
System and Event logging - Review	Ensure there is a process in place to review the system logs quarterly.
Third Party Risk Management	Perform a vendor review for all vendors that access, hold or transmit Personally Identifiable Information, Protected Health information Financial information, credit card information or have access to the member's system/computer network.

New

New

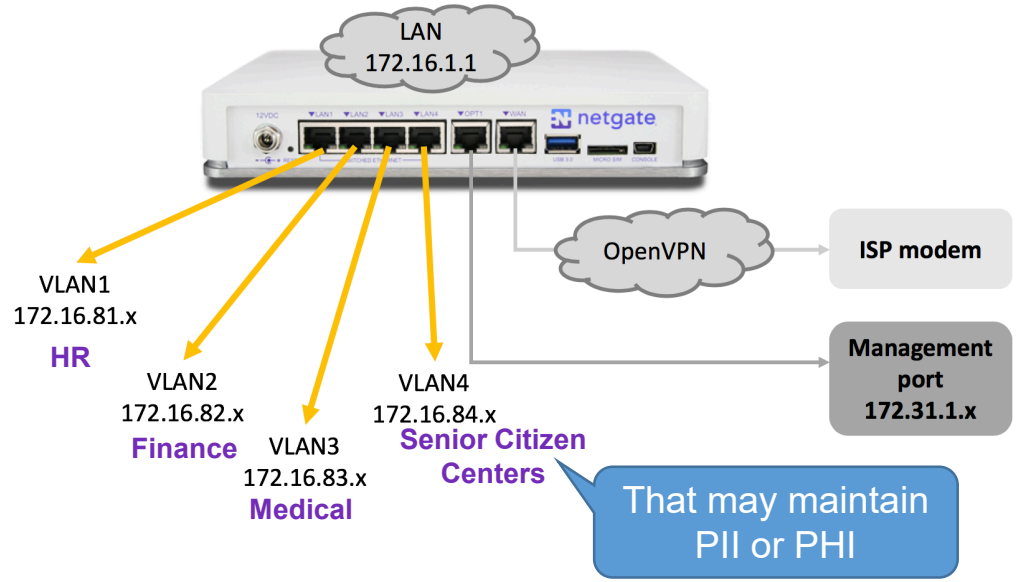
New

New

New

Differences –
Network Segmentation

The purpose of segmenting your network is to reduce the spread of a cyber-attack by dividing the network into multiple zones or sub-networks and applying security protocols to each zone. You should consider isolating key business units or sensitive departments, such as finance and human resources.



PII – Personally Identifiable Information
PHI – Protected Health Information

Network segmentation (often referred to as network isolation) is the concept of taking your network and creating silos within it called **VLANs**

(Virtual Local Area Networks)

✓Consult with your Technology Professional to plan a network segmentation initiative.

Differences –
Remote Access - MFA

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN and decreases the likelihood of a successful cyber attack.

1st Type your usual Username & Password.

2nd System sends you a verification code to your phone or email.

3rd System access is granted after security code is entered and is validated.

✓ **This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.).**

MFA shall be enabled for the following remote connections:

- Member's network if remote access is allowed.
- Email service (if cloud based)
- Third-Party applications that store or transmit PII or PHI information.

Differences –
Password Integrity

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

The purpose of the Password Integrity initiative is to frequently validate users' emails and passwords to ensure they have not been compromised.

Initiate a policy that users check their password or emails against an email breach service, such as HaveIBeenPwned, to determine if any email addresses have been compromised.

Users whose credentials have been compromised must take necessary action to ensure integrity of any emails or passwords found on the breach database.

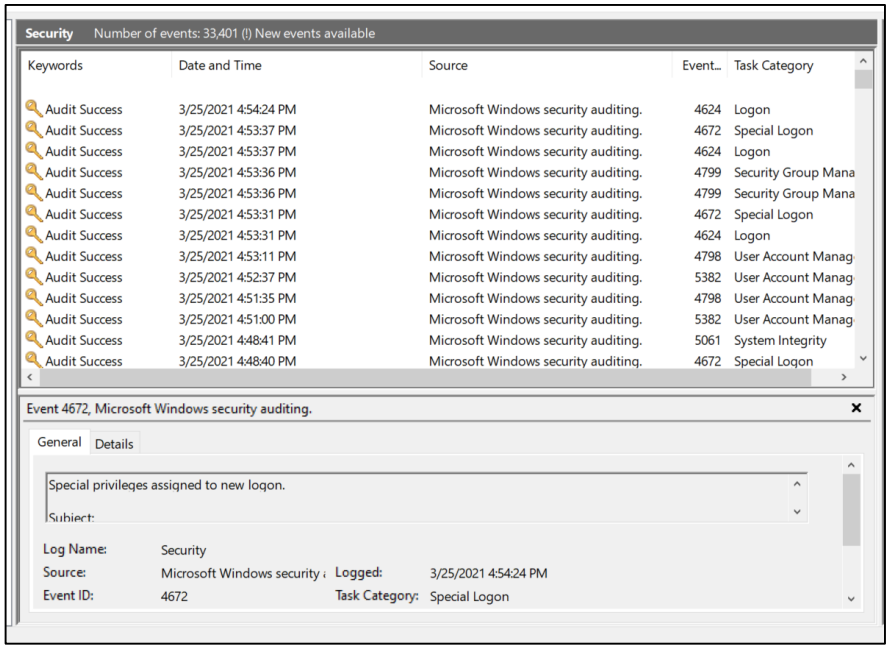
Quick Tip – What to do if your credentials have been compromised?

- ✓ Update your security software and delete any malware
- ✓ Change your passwords
- ✓ Check your account settings
- ✓ Tell your friends & financial institutions
- ✓ Frequently monitor your credit reports
- ✓ Turn on two-factor authentication if your service provider offers it

Differences –
System & Event Log Review

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

The purpose of the System and Event Log review initiative is to ensure that systems logs that are captured as part of the System & Event Logging process are reviewed quarterly to capture system activities, information security events, system utilization and performance in a pre-emptive manner.



✓Consult with your Technology Professional to build a quarterly system & log review process as part of the maintenance and support program.

Differences –
Third-Party Risk Management

The purpose of the Third-Party Risk Management (TPRM) initiative is to ensure the protection of information that is accessible to outside vendors.

Use the Third-Party Security Questionnaire when vendors or partners who store, handle, access, and or transmit any of the following sensitive data:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial information
- Credit card information
- Access to the member's information system and/or computer network
- Any asset deemed sensitive and/or of value

✓ **If your medical insurance carrier were to be breached, would your employee's PHI be exposed?**

✓ **If your payroll service provider were to be breached, would your employee's PII be exposed?**

✓ **If your Technology Professional were to be breached, would access to your network be compromised?**

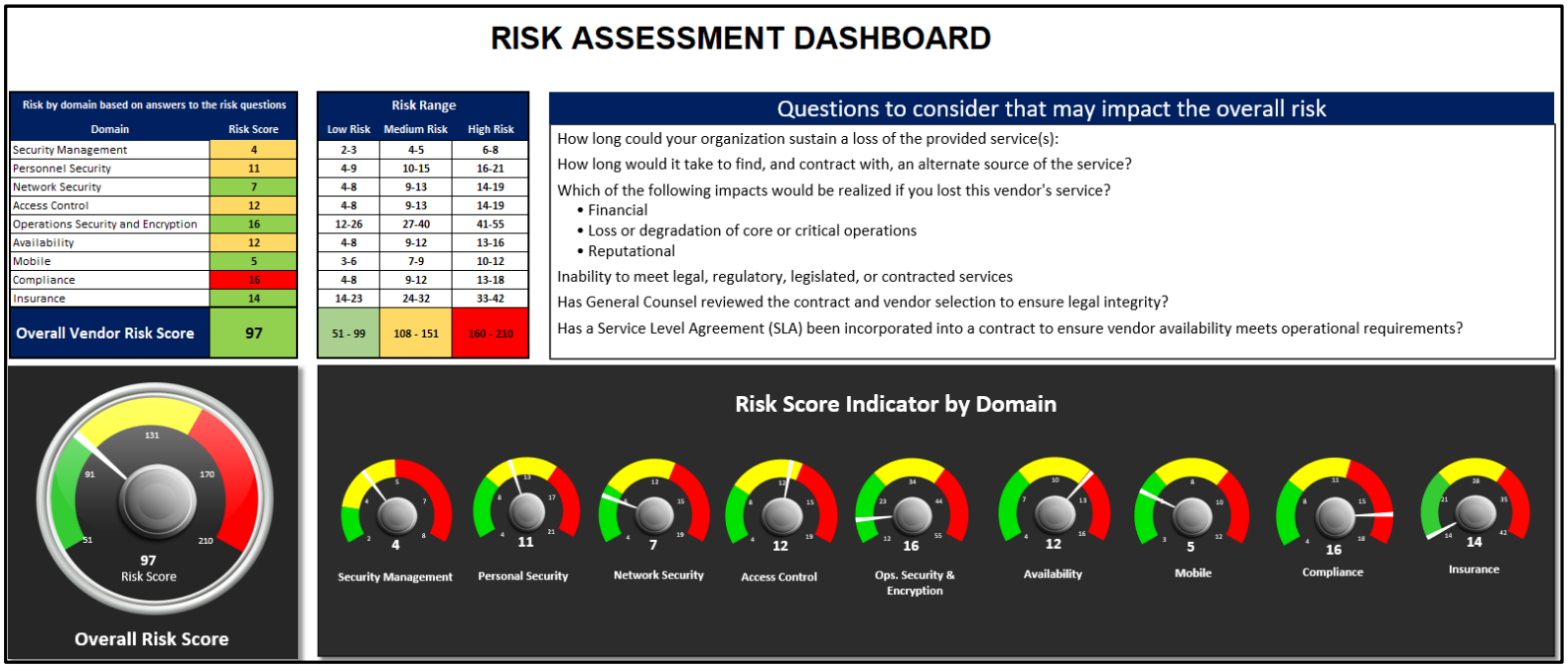
We will work with common vendors

No sense sending the same questionnaire to the same vendor multiple times.

Differences –
Third-Party Security Questionnaire

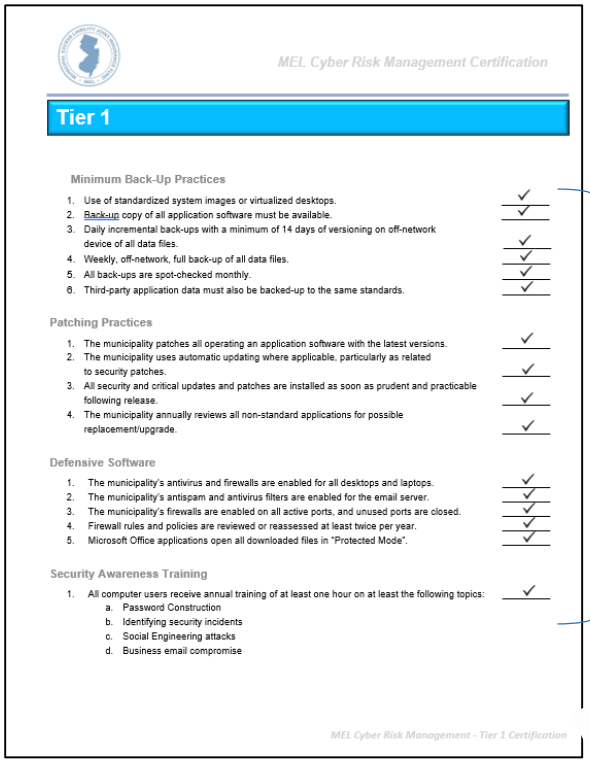
Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

The Third-Party Security Questionnaire consists of 52 questions and is to be used as part of the vendor selection process when evaluating vendors / contractors who store, handle, access, and or transmit sensitive information.



Certification

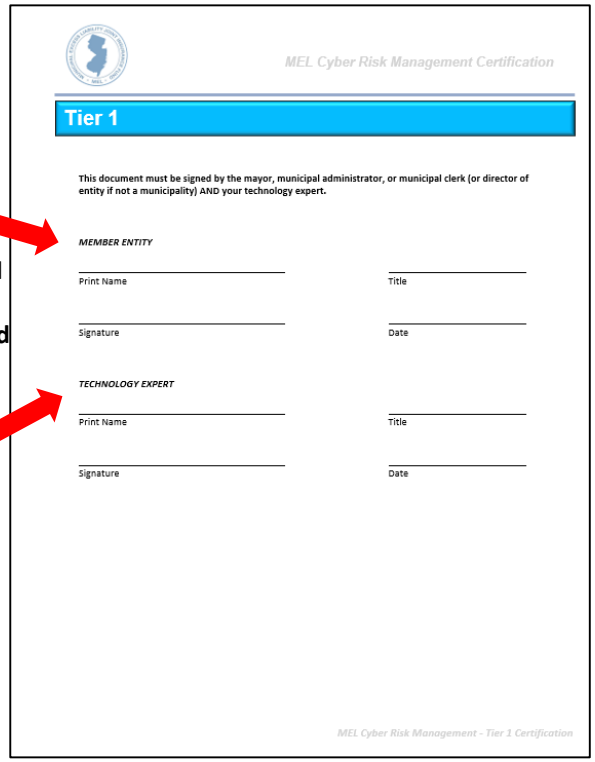
There are three Certification Checklists: Tier 1, Tier 2, Tier 3. Each Tier Certification Checklist need to be completed and executed by the member and their Technology Professional.



Tier 1 Certification Checklist Sample

All line items that apply and are in place need to be checked.

The Member and Technology Professional need to execute the Certification Checklist.



No checkmarks, no signatures, no certification!!

Certification

- ✓ **Tier 1, 2 and 3 Compliance Target date is <u>October 1, 2021</u>.**
  - To ensure eligibility for deductible reimbursement
- ✓ **Submit Certification Checklist as soon as you are compliant – don't wait.**
  - Example: Don't wait to submit Tier 2 Certification Checklist to submit Tier 1 if you meet the criteria
- ✓ **Work with your IT Professionals to implement the required controls**

Financial Impact

JERRY – SHOW ME THE MONEY !!!

Financial Impact

1. Reimbursements

The following are the amounts that will be reimbursed to the member by the MEL if found to be in compliance at the time of a claim.

2. Reimbursement Policy

The MEL Cyber Deductible Reimbursement program is a *reimbursement* program whereby the member is reimbursed for deductible amounts actually spent up to the maximum limit shown below.

3. Grandfather

All members in compliance with version 1 of the MEL Cyber Risk Management Program as of 3/5/2021 will receive grandfathered status until January 1, 2022. At such point in time, those grandfathered members will need to recertify. Any members not grandfathered must comply with version 2 as of 3/8/2021.

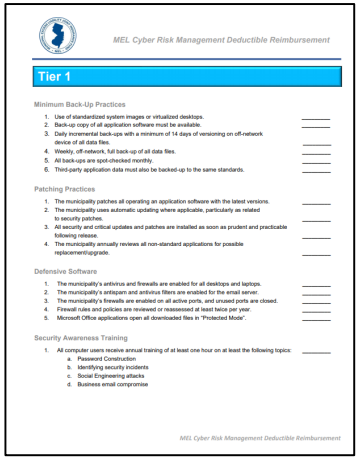
Year	Member Deductible	Reimbursement		
		Tier 1	Tier 2	Tier 3
2021	$25,000	$20,000	$22,500	$25,000
2022	$25,000	$10,000	$20,000	$25,000

JERRY – SHOW ME THE MONEY !!!

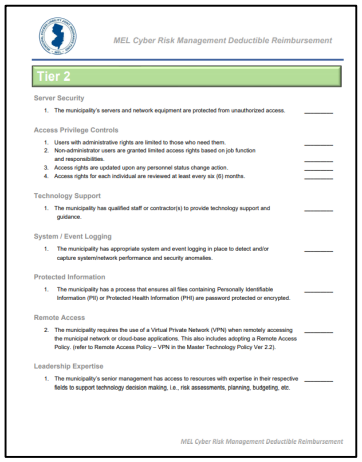
Deductible Reimbursement Certification

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

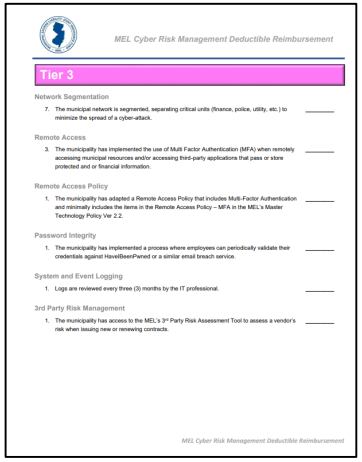
Upon a claim, you will need to submit all three Tier Reimbursement sheets along with the required documents as proof of compliance.



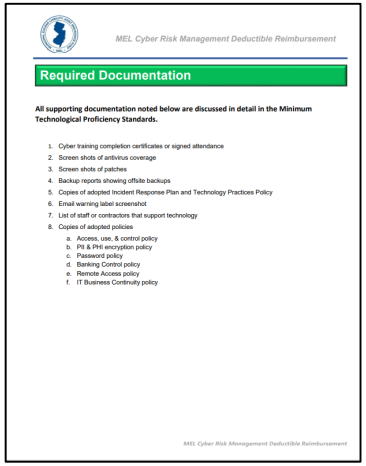
Tier 1



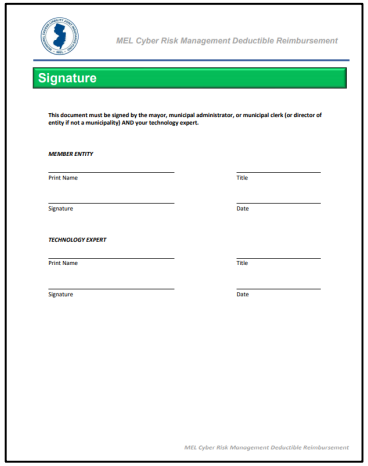
Tier 2



Tier 3



List of items to submit as Proof of Compliance



Signature Page

Program Rollout

The 1st part is understanding the documents associated with the program:

Document	Description
Master Technology Policy	The Master Technology Policy defines the information security practices that are governed by the MEL's Cyber Risk Management Program. It details the requirements and controls to comply with the three tiers of the program.
MEL Certification Checklist	The MEL Certification Checklist consists of three Certification Checklist for each respective Tier. The Certification Checklist need to be completed and executed by the member and their technology professional.
Incident Response Plan	The Incident Response Plan defines the methods for identifying, tracking, and responding to technology security incidents. This also has a table to identify your response team and contact information.
MEL Cyber Risk Management Deductible Reimbursement Checklist	The MEL Cyber Risk Management Deductible Reimbursement Checklist consists of three checklist for each respective Tier. The Deductible Reimbursement Checklist shall be completed and executed by the member and their technology professional along with the required documents as proof of compliance.
Third Party Security Questionnaire	Third Party Security Questionnaire is to be used as part of the vendor selection process when evaluating vendors / contractors who store, handle, access, and or transmit sensitive information.
MEL Cyber Task Force Memorandum	The MEL Cyber Task Force Memorandum is a one-page memorandum highlighting the program.
Business Continuity Planning Guidelines	The Business Continuity Planning Guidelines serves as a basic guideline for best practices and outlines the items to consider when developing a Business Continuity Plan.

Program Rollout

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

Step 1
Share the Master Technology Policy with your Technology Professional in effort to understand the requirements.

Step 2
The Technology Risk Service Director shall coordinate and schedule a conference call between the Technology Professional and the member to assess the current controls.

Step 3
The Technology Risk Service Director shall perform a Gap Assessment and provide the member an actionable report with findings, recommendations, and task ownership.

Step 4
The Technology Professional shall work with the member to incorporate the required changes to become compliant. The Technology Risk Service Director will provide support and guidance as needed.

Step 5
After the requirements have been met for each individual tier, the member can submit the Certification Checklist for validation and final approval to the MEL.

Program Rollout

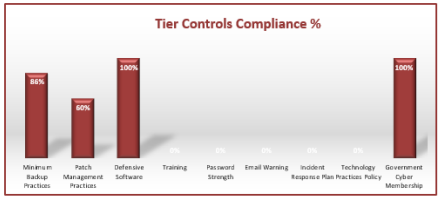
Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

Gap Assessment & Actionable Report

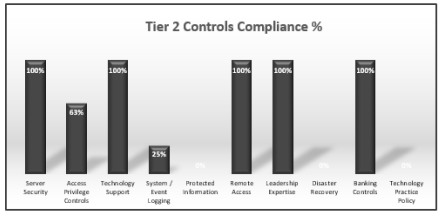
MEL's Minimum Technology Proficiency Standard Assessment - 2nd Edition

Tier	Control Requirement	Interpretive Statement	Findings	Recommendations	Task Owner	Status
1	**Minimum Backup Practices**	**Interpretive Statement**				
	1- Use of standardized system images or virtualized desktops.	PC configurations should be standardized, e.g. same version of Windows, Microsoft Offices, and other commonly used applications. This level of standardization should be imaged to simplify rebuilding or restoring a PC to it's original state in the event of a major incident.	The municipality uses Veeam as their backup platform to perform full image weekly backups and nightly file backups, local files are stored in One Drive. The municipality maintains an image of their Domain Controller server. It was noted that the municipality has 7 desktops which are currently different models.	No action required. The municipality should consider purchasing the same model desktops at the next technology refresh cycle to simplify imaging and support efforts.	None at this time	Fully implemented
	2- Application Software: Back-up copy of application software must always be available.	A copy of applications used, e.g. Windows, Microsoft Office, financial applications, dog license, code, construction, and other essential and mission critical software shall be available in effort to rebuild a PC.	The municipality maintain hard copies of required software to rebuild local desktops.	No action required.	None at this time	Fully implemented
	3a- Daily incremental back-ups with a minimum of 14 days of versioning on off-network device of all data files.	A daily incremental backup, copies data that has been changed or created since the previous backup. A 14 day versioning period referrers to the number of copies or days that you can revert to. In the event a backup becomes corrupted, you can go to a previous copy that is intact. Being a government entity, cloud backups should be hosted by a FedRamp certified service provider, e.g. Google, Amazon, Microsoft, IBM, etc.	The municipality's backup retains a 30 day versioning schedule.	No action required.	None at this time	Fully implemented
	3b- Weekly, off-network, full back-up of all data files.	The backup methodology or practice requires a weekly full backup that is stored off site and that is not part of or connected to the network.	The municipality uses Veeam as their backup platform to do full image weekly backups that is also maintained off site.	No action required.	None at this time	Fully implemented
	3c- All backups are spot-checked monthly.	A log is to be maintained to ensure that the backup is validated and tested monthly. Testing the backup requires restoring a file from the backup and noting it on a log. Backup software can also provide reporting status of the backup activity.	The backup software provides nightly status reporting; however, the municipality does not routinely spot check the backups.	The municipality shall develop a policy to effectively spot check the backups monthly. This can be accomplished by restoring a test file and maintaining a log. Testing and validating backups are crucial practices that ensure backups are functioning as designed and intended to.	IT - Christopher Alworth	Not implemented
	4- Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data.	Being a government entity, cloud backups should be hosted by a FedRamp certified service provider, e.g., Google, Amazon, Microsoft, IBM, etc.	The municipality uses Datto's Backupify which is a SOC 2 Type II compliance cloud base backup solution.	No action required.	None at this time	Fully implemented
	5- Third-party application data must also be backed-up to the same standards.	All mission critical, essential files, and 3rd party applications must be part of the backup scheme and follow the same policy. (e.g. construction, code enforcement, financial, animal license, etc.)	The municipality's Edmunds financial data is part of the nightly and weekly backup. However, it was noted that the municipality's construction, zoning, and engineering services are supported by the Borough of Rumson in a shared service agreement.	No action required.	None at this time	Fully implemented
1	**Patch Management Practices**	**Interpretive Statement**				
	1- Keep all operating and application software current with latest versions.	All software that have applicable updates need to be updated or patched regularly. This includes security, and operational enhancement updates. If a software vendor does not provide updates, then there are no patches to implement.	The municipality has automatic desktop update enabled; however it is not controlled by the IT vendor nor is it know if an end-user turns off the automatic function.	The IT vendor shall deploy the automatic update function via a group policy where the end-user cannot turn off the automatic update feature.	IT - Christopher Alworth	Partially implemented
	2- Use automatic updating where practicable, particularly as related to security patches.	Ensure that all software products (where applicable) can automatically perform security updates as required by the vendor. However, server security updates may be scheduled and performed manually to ensure there are no adverse effects on other applications.	The municipality has automatic desktop update enabled; however it is not controlled by the IT vendor nor is it know if an end-user turns off the automatic function.	The IT vendor shall deploy the automatic update function via a group policy where the end-user cannot turn off the automatic update feature.	IT - Christopher Alworth	Partially implemented
	3- Install all security and critical updates and patches as soon as prudent and practicable following release.	Security and critical patches need to be implemented as soon as possible; however it's negative impact on the operations, or compromising other software needs to be evaluated.	The municipality has automatic desktop update enabled; however it is not controlled by the IT vendor nor is it know if an end-user turns off the automatic function.	The IT vendor shall deploy the automatic update function via a group policy where the end-user cannot turn off the automatic update feature.	IT - Christopher Alworth	Partially implemented
	4- Annually review all non standard applications for possible replacement/upgrade.	Outdated or non-supported operating systems and software shall not be used unless there is no practical alternative available. PCs using unsupported or outdated software should be replaced/upgraded or must be isolated from the main network.	Though the municipality uses Office 365, it does not perform an annual review of other applications.	Mission critical and non-standard applications shall be reviewed annually to ensure they are kept current and supported by the vendor. PCs with unpatched or unsecure applications must be isolated from the network.	IT - Christopher Alworth	Partially implemented
	5- Regularly review MS-ISAC alerts on newly discovered software vulnerabilities and act accordingly to minimize risks until software patches are available.	Both MS-ISAC and NJCIC provide routine alerts on newly discovered software vulnerabilities. Ensure that recommended patches and updates are applied when applicable to your environment. EIO ISAC - https://www.cisecurity.org/ei-isac/	The municipality is a member of NJCCIC and MS-ISAC.	No action required.	None at this time	Fully implemented

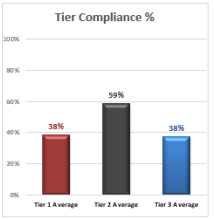
Tier 1 Controls	
Minimum Backup Practices	86%
Patch Management Practices	60%
Defensive Software	100%
Training	0%
Password Strength	0%
Email Warning	0%
Incident Response Plan	0%
Technology Practices Policy	0%
Government Cyber Membership	100%
Tier 1 Average	38%



Tier 2 Controls	
Server Security	100%
Access Privilege Controls	63%
Technology Support	100%
System / Event Logging	25%
Protected Information	0%
Remote Access	100%
Leadership Expertise	100%
Disaster Recovery	0%
Banking Controls	100%
Technology Practice Policy	0%
Tier 2 Average	59%



Tier 3 Controls	
Segmentation	50%
Remote Access Control - MFA	0%
Password Integrity	0%
Third Party Risk Management	100%
Tier 3 Average	38%



Program Rollout - Financial Assistance

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

You can use your allotted Cyber EPL budget amount to offset the cost of implementing any of the requirements to become compliant with the program.

Secure Data Consulting Services

About Lou Romero

Lou Romero has over 40 years of IT experience, works with local and municipal governments and private entities to help improve and manage their information security posture. Lou works closely with clients to develop a customized Cyber Risk Loss Control Program designed to identify cyber vulnerabilities, risks and provide actionable recommendations based on best practices and international standards.

Lou attends various cybersecurity symposiums, and summits. He has also been a keynote and panel speaker in Washington DC at the annual National Symposium on Cyber Security and Government.

Lou currently works with various Joint Insurance Funds / Government Risk Pools and is the Technology Risk Services Director for 66 municipalities in New Jersey. Lou is an ISO 27001 internal auditor with over 260 cyber risk assessments conducted throughout the State and attained his Certified Government Chief Information Officer (CGCIO) certification from Rutgers University.

Lromero@SecureDataCS.com
www.SecureDataCS.com
(732) 690-4057

Secure Data Consulting Services