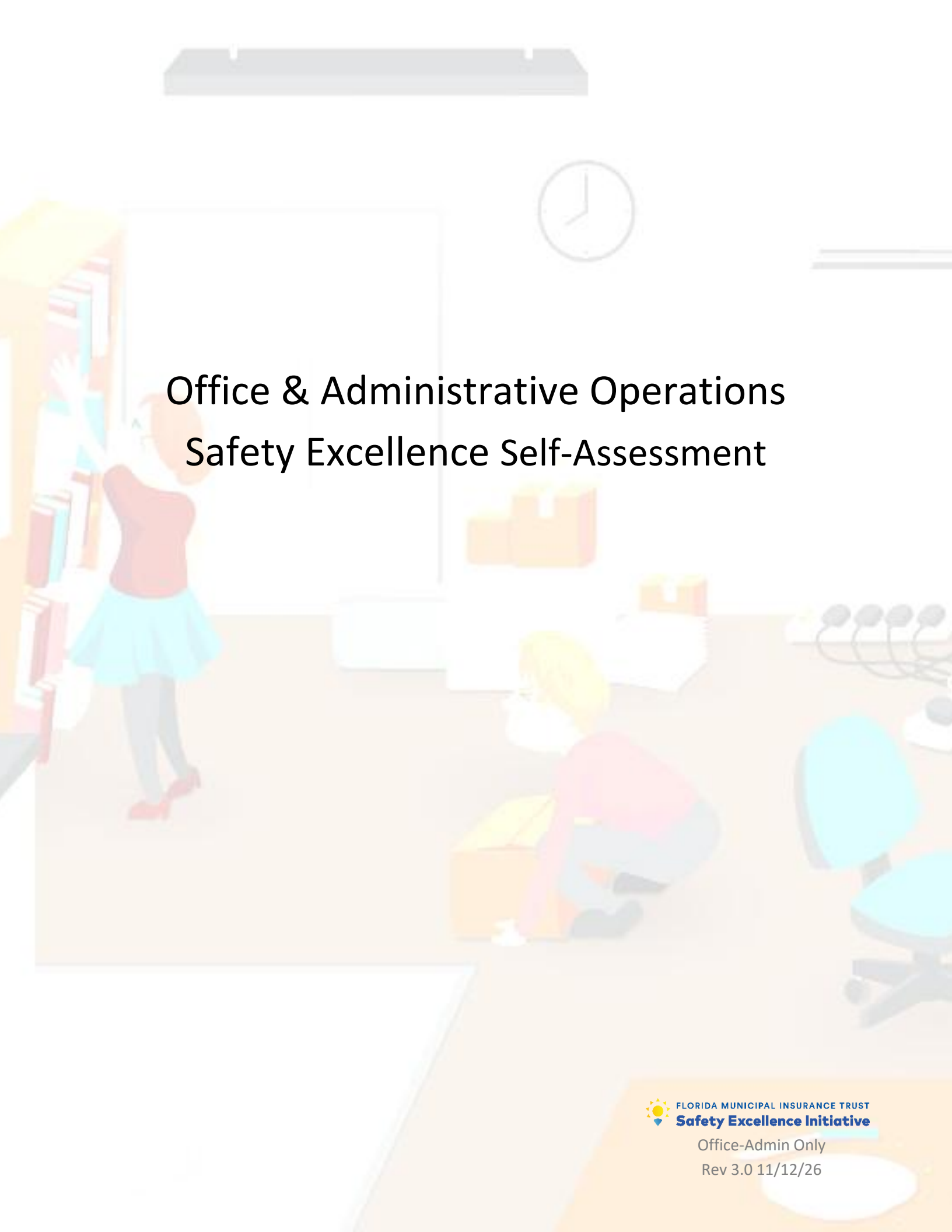


Office & Administrative Operations Safety Excellence Self-Assessment

FLORIDA MUNICIPAL INSURANCE TRUST
Safety Excellence Initiative

Office-Admin Only

Rev 3.0 11/12/26

Table of Contents

FMIT Safety Excellence Initiative 3
Voluntary Safety Accreditation Program 3
Self-Assessment Instructions 3
Step 1: Complete the Self-Assessment 3
Step 2: Complete the Scoring Summary 3
Next Steps 4
Self-Assessment Score Summary: 4
Section Scoring Summary 4
Overall Score Calculation 4
Section 1: Leadership and Risk Management: 5
Section 2: Office & Employee Safety: 6
Section 3: Hazard, Incident & Corrective-Action Management 7
Section 4: Contract & Vendor Risk Management: 8
Section 5: Emergency Planning & Continuity of Operations 9
Section 6: Employment Practices Risk Management: 10
Section 7: Cybersecurity & Information Protection 11
Section 8: Public Entity Governance & Operational Risk 12

Disclaimer and Limitation of Liability

The Florida Municipal Insurance Trust (FMIT) Safety Excellence Initiative (SEI) Assessment is intended solely as a voluntary risk management and continuous improvement tool. The assessment evaluates selected safety management practices, policies, procedures, documentation, and operational controls that were available and observed at the time of the review. The results, recommendations, scores, and accreditation status are based upon information provided by the participating organization and do not constitute a guarantee of compliance with any federal, state, or local law, regulation, standard, accreditation requirement, or industry best practice.

Participation in the SEI program and successful completion of an assessment do not guarantee the absence of injuries, illnesses, claims, losses, liability exposures, regulatory violations, or other adverse events. The assessment is not a comprehensive audit of all operations, hazards, or management practices and should not be relied upon as legal, regulatory, engineering, or professional advice.

The participating organization retains sole responsibility for maintaining a safe work environment, complying with applicable laws and regulations, implementing corrective actions, and managing its operations. FMIT reserves the right to modify assessment criteria, scoring methodologies, accreditation requirements, and program benefits at any time.

SEI accreditation signifies that the organization demonstrated implementation of applicable safety management elements at the time of assessment and is intended to recognize commitment to safety excellence and continual improvement. Accreditation does not constitute certification of regulatory compliance, operational safety, or freedom from risk.

FMIT Safety Excellence Initiative

The Florida Municipal Insurance Trust (FMIT) Safety Excellence Initiative (SEI) is a voluntary accreditation program designed to help FMIT Members develop, implement, and sustain effective safety and risk management systems. The program is founded on the principle that organizations that proactively identify hazards, manage risk, train employees, investigate incidents, and promote leadership accountability experience fewer injuries, illnesses, vehicle crashes, workers' compensation claims, liability exposures, and other preventable losses. The purpose of the FMIT Safety Excellence Initiative is to provide participating organizations with practical guidance, assessment tools, sample resources, and best practices that support continuous improvement in safety, organizational readiness, and risk management. By participating in the program, organizations can strengthen their safety culture, improve operational performance, reduce losses, and better protect both employees and the communities they serve.

Voluntary Safety Accreditation Program

Participation in the FMIT Safety Excellence Initiative is completely voluntary and available to all eligible FMIT members. Organizations that successfully demonstrate implementation of the safety and risk management practices outlined in this assessment may earn a Certificate of Safety Excellence. Accreditation is based on demonstrated implementation and effectiveness, not simply the existence of policies or stated intentions. During the assessment process, organizations are evaluated on documented evidence of safety management practices, leadership involvement, employee participation, training programs, operational controls, inspections, corrective action processes, and continuous improvement efforts.

Self-Assessment Instructions

Step 1: Complete the Self-Assessment

Conduct a thorough assessment of your safety and risk management system using the questions contained in this document. The assessment is organized into eight (8) sections covering critical areas of risk management, employee safety, training, health and wellness, and emergency preparedness. Each question is worth one point. A point should only be awarded when objective, observable, and measurable evidence demonstrates that the requirement has been implemented.

Important: Credit should not be awarded based solely on verbal confirmation that a process exists or is being performed.

Not Applicable (N/A) Questions

Certain questions may not apply to every organization. If a question is determined to be Not Applicable (N/A):

- Do not award the point.
- Remove the question from the section's total possible points.
- Recalculate the section score using only applicable questions.

This approach ensures organizations are evaluated fairly based on the services, programs, and operations they perform.

Step 2: Complete the Scoring Summary

After completing all eleven sections, transfer the results to the Scoring Summary below and calculate:

1. Total points earned for each section.

2. Total applicable points for each section.
3. Individual section percentages.
4. Overall assessment percentage.

Once the calculations are complete, compare the results to the accreditation requirements for Levels 1, 2, and 3.

Next Steps

If your department meets or exceeds the requirements for the desired level, contact the FMIT to schedule a formal Safety Improvement Assessment and verification review. If your department does not meet the minimum accreditation requirements, use the recommendations, sample policies, forms, procedures, checklists, and other resources referenced throughout this document to address identified gaps.

Self-Assessment Score Summary:

Section Scoring Summary

Section	Points Earned	Applicable Points	Section %
Section 1: Leadership & Risk Management			%
Section 2: Office & Employee Safety			%
Section 3: Hazard, Incident & Corrective-Action Management			%
Section 4: Contract & Vendor Risk Management			%
Section 5: Emergency Planning & Continuity of Operations			%
Section 6: Employment Practices Risk Management			%
Section 7: Cybersecurity & Information Protection			%
Section 8: Public Entity Governance & Operational Risk			%

Overall Score Calculation

Calculation Item	Score
Total Points Earned	
Total Applicable Points	
Overall Percentage (Points Earned ÷ Applicable Points × 100)	%
Level 1: Safety and Risk Foundations (70%–79%) | Level 2: Advanced Safety and Risk Management (80%–89%) |Level 3: Safety and Risk Excellence (90%+)	

Section 1: Leadership and Risk Management:

	Criteria	Score	Objective Verification	Notes:
1.	Has the organization established a written commitment to employee safety and organizational risk management?		• Current safety or risk-management policy, handbook language, board-approved statement, or signed management commitment. • Evidence the commitment was communicated or made available to employees.	
2.	Has responsibility for coordinating safety and risk-management activities been assigned to an employee, manager, contractor, or other designated individual?		• Job description, organizational chart, written designation, board minutes, management contract, or service agreement. • Interview confirms the responsible person understands the role.	
3.	Are new employees provided with basic information about workplace safety, emergency procedures, incident reporting, and applicable organizational policies?		• Completed orientation checklist, handbook acknowledgment, onboarding agenda, training record, or new-hire materials. • Content addresses emergency actions, incident reporting, hazards, and key contacts.	
4.	Does the organization periodically communicate safety, risk-management, or loss-prevention information to employees?		• Staff meeting agendas, safety emails, newsletters, brief training records, posters, or FMIT resource distribution. • Examples from the current assessment period.	
5.	Are employees provided with a method for reporting unsafe conditions, hazards, incidents, or near misses?		• Reporting form, designated email, hotline, intranet process, handbook instructions, or documented verbal process. • Employee interviews confirm awareness.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 2: Office & Employee Safety:

	Criteria	Score	Objective Verification	Evidence, Observations and Recommendations
6.	Are office areas periodically reviewed for common safety hazards?		• Completed inspection checklist, property inspection, photographs, work orders, or landlord/property-manager report. • Documented correction of significant findings.	
7.	Are applicable fire extinguishers, alarms, emergency lighting, exit signs, and other life-safety systems inspected or maintained?		• Current extinguisher tags, fire inspection, alarm/service documentation, landlord confirmation, or maintenance agreement. • Visual observation of clear exits and visible signage.	
8.	Are appropriate first-aid supplies readily available and periodically checked? If AEDs are present, are they maintained in operable condition and checked at least monthly?		• First-aid kit inventory/check record and replenishment receipts. • AED monthly checklist, status indicator check, pad expiration dates, battery status, and service records, if applicable.	
9.	Are employees provided information or assistance for properly arranging computer workstations and addressing ergonomic concerns?		• Ergonomic self-assessment, workstation checklist, training material, accommodation record, or equipment request process. • Observation of representative workstations.	
10.	Does the organization have a policy or procedure addressing threats, workplace violence, and concerning behavior, including how employees should report an immediate or developing concern?		• Workplace violence policy, security procedure, employee handbook, emergency contacts, or training records. • Instructions distinguish immediate emergencies from developing concerns.	
11.	If employees drive while conducting organizational business, has the organization established basic driver requirements and collision-reporting procedures?		• Driver authorization, license/MVR review where appropriate, personal-auto insurance requirement, distracted-driving policy, vehicle-use rules, and collision-reporting instructions. • Sample documentation for active drivers.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 3: Hazard, Incident & Corrective-Action Management

	Criteria	Score	Objective Verification	Notes:
12.	Does the organization have a procedure for reporting employee injuries, vehicle collisions, property damage, liability incidents, and other potentially covered losses?		• Incident-reporting procedure, flowchart, claim contact sheet, forms, handbook instructions, or intranet page. • Procedure addresses after-hours or urgent events where applicable.	
13.	Has responsibility for reporting and coordinating insurance claims been assigned to a specific employee or position to ensure incidents and potential claims are reported promptly to FMIT?		• Written designation, job duty, contact list, organizational chart, or management agreement. • Interview confirms access to reporting systems and FMIT contacts.	
14.	Are incidents appropriately documented and investigated?		• Incident report, photographs, witness information, police report, supervisor notes, invoices, video preservation record, or claim confirmation. • Samples are complete, timely, and retained securely.	
15.	Has the organization identified responsibility for inspecting and maintaining the buildings, facilities, infrastructure, or other property under its control?		• Property inventory, maintenance matrix, contract, job description, inspection schedule, interlocal agreement, lease, or board designation. • Responsibility gaps and shared obligations are identified.	
16.	Does the organization provide a method for employees, contractors, residents, or members of the public to report unsafe conditions involving property under the organization's control?		• Website form, phone line, email, mobile app, work-order portal, posted contact, call log, or complaint procedure. • Reports can be tracked and acknowledged.	
17.	Does the organization have a process for evaluating reported property hazards, prioritizing corrective action based on potential risk, and documenting the response?		• Work-order system, hazard log, inspection record, photographs, barricade notice, contractor request, repair invoice, or closure verification. • Priority reflects severity, exposure, and urgency.	
18.	Are significant corrective actions identified following incidents or inspections tracked through completion?		• Corrective-action log, work order, project tracker, meeting minutes, email follow-up, or closure photograph. • Overdue items are escalated.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 4: Contract & Vendor Risk Management:

Criteria		Score	Objective Verification	Notes:
19.	Does the organization establish appropriate insurance requirements for vendors and contractors when their activities create a significant exposure?		• Contract insurance schedule, procurement template, risk review, or counsel-approved requirements. • Requirements may include general liability, auto, workers' compensation, professional, pollution, or cyber coverage as applicable.	
20.	When insurance is required by contract, does the organization obtain and review evidence of the required coverage?		• Current certificate of insurance, additional insured endorsement where required, workers' compensation evidence, expiration tracking, or renewal request. • Named insured, insurer, limits, dates, and operations align with the contract.	
21.	When appropriate, do contracts include provisions addressing responsibility for injuries, property damage, professional errors, data incidents, or other losses?		• Indemnification/hold-harmless language, additional insured requirement, waiver provisions, professional liability, cyber/data clauses, or counsel review. • Provisions are appropriate to Florida public-entity operations and the specific scope.	
22.	When contractors maintain facilities, infrastructure, landscaping, recreation areas, roadways, stormwater systems, or other organizational property, does the organization confirm that key safety, inspection, maintenance, insurance, and reporting duties are performed?		• Service reports, inspection logs, maintenance schedules, work orders, performance meetings, complaint records, insurance tracking, or renewal evaluation. • Deficiencies are documented and escalated.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 5: Emergency Planning & Continuity of Operations

Criteria		Score	Objective Verification	Notes:
23.	Does the organization maintain emergency procedures appropriate to the hazards and operations of its office?		• Emergency action plan, handbook section, building procedures, one-page emergency guide, or landlord plan supplemented by member instructions. • Roles, contacts, evacuation/shelter actions, and accountability are addressed.	
24.	Has the organization identified the functions that must continue or be restored promptly following a significant disruption?		• Essential-functions worksheet, continuity plan, business-impact discussion, departmental list, or management/board approval. • Each function has an owner and target restoration timeframe where practical.	
25.	Has the organization established reasonable backup arrangements for essential personnel, records, technology, facilities, or services?		• Alternate staff assignments, remote-work capability, alternate workspace, cloud access, succession list, vendor recovery terms, backup contacts, or manual workarounds. • Arrangements are feasible and accessible during disruption.	
26.	Are emergency and continuity procedures periodically reviewed, discussed, tested, or exercised?		• Annual review record, tabletop exercise, hurricane meeting, evacuation drill, notification test, after-action notes, or updated plan. • Identified improvements are assigned and tracked.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 6: Employment Practices Risk Management:

Criteria		Score	Objective Verification	Notes:
27.	Does the organization maintain written personnel policies appropriate to its workforce and operations?		• Employee handbook, personnel policy manual, adopted policies, acknowledgment forms, and revision/approval record. • Policies address key employment practices and identify responsible contacts.	
28.	Do organizational policies prohibit discrimination, harassment, and retaliation and establish a method for employees to report concerns?		• Policy language, reporting procedure, complaint form, acknowledgment, posting, or training record. • Alternative contact exists when the supervisor is involved.	
29.	Does the organization appropriately document significant employment actions and personnel decisions?		• Applications, interview records, performance documentation, counseling/discipline, accommodation or leave records, promotion/transfer decisions, and termination approvals. • Records are stored securely and access is limited.	
30.	Does the organization seek appropriate human resources or legal guidance before taking significant or potentially high-risk employment actions?		• HR/legal consultation record, FMIT ELA contact information, supervisor guidance, counsel invoice, email, or decision checklist. • Examples involving termination, discipline, accommodation, leave, discrimination, harassment, or retaliation.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 7: Cybersecurity & Information Protection

Criteria		Score	Objective Verification	Notes:
31.	Has responsibility for managing the organization's information technology and cybersecurity risks been assigned to an employee, contractor, managed service provider, or other appropriate party?		• Job duty, IT service agreement, managed service provider scope, organizational chart, board designation, or contact list. • Primary and backup contacts are known.	
32.	Does the organization use reasonable controls to protect access to email, financial systems, cloud services, and other important technology?		• Individual accounts, MFA settings, password standard, screen-lock setting, privileged-access list, onboarding/offboarding checklist, and access review. • Former users are promptly disabled.	
33.	Are employees periodically provided cybersecurity awareness information or training?		• Completion report, attendance record, simulated phishing results, training email, onboarding material, or annual acknowledgment. • Training includes how to report suspicious activity.	
34.	Are important electronic information and records appropriately backed up or maintained in systems that provide reasonable backup and recovery capabilities?		• Backup configuration, cloud retention settings, vendor report, restore-test record, recovery documentation, and identification of critical systems. • Backups are separated or protected from ordinary user alteration where feasible.	
35.	When vendors host important systems, maintain sensitive information, or provide technology services, does the organization consider cybersecurity, privacy, backup, incident notification, and data-protection requirements?		• Security questionnaire, contract clauses, service-level agreement, backup terms, breach-notification requirement, data return/destruction terms, cyber insurance, or independent assurance report. • Critical vendor list and renewal review.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%

Section 8: Public Entity Governance & Operational Risk

	Criteria	Score	Objective Verification	Notes:
36.	Does the organization have a process for receiving, routing, retaining, and responding to public records requests and maintaining public records?		• Public records policy, custodian designation, request log, retention schedule, website instructions, contract terms, training, or counsel guidance. • Employees know where to route requests.	
37.	Does the organization maintain procedures to support applicable public-meeting requirements, including notices, agendas, minutes, and preservation of meeting records?		• Meeting calendar, notice checklist, agenda/minute templates, posting records, approved minutes, accessibility process, or counsel guidance. • Roles and deadlines are assigned.	
38.	Does the organization maintain a system for identifying and monitoring important statutory, financial, insurance, contractual, and administrative deadlines?		• Compliance calendar, spreadsheet, task system, board calendar, recurring reminders, filing confirmations, or management report. • Includes entity-specific filings, renewals, reporting, meetings, contracts, and insurance dates.	
39.	Does the organization maintain reasonable controls governing access to organizational funds, purchases, payments, credit cards, bank accounts, and electronic financial transactions?		• Purchasing policy, approval matrix, bank reconciliation, dual-approval record, credit-card log, invoice support, user-access list, vendor change callback, or board review. • Exceptions are documented and reviewed.	
40.	Does the organization have a process for transferring important responsibilities, records, system access, financial authority, contracts, and other critical information when key employees, board members, managers, or contractors change?		• Transition checklist, offboarding record, password/account transfer process, bank-signature update, records inventory, contract list, pending-matter summary, or board orientation. • Access removal and authority changes occur promptly.	

(1) Total Points Possible for Section	*(2) Points Not Applicable (NA)*	*(3) Applicable Points For section: Subtract (2) from (1)*	*(4) Total Points Scored: Add All*	*(5) Section Percentage: Divide (4) from (3) = %*
				%