Administration and Management Standards

Risk Prevention and Management

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

Introduction

COA's Risk Prevention and Management standards require that organizations take a proactive approach to risk by continually improving systems and practices for identifying and mitigating potential risks and learning from adverse events and challenges when they occur. Proactive, systemic risk prevention and management requires a holistic approach that involves staff throughout the organization and considers all areas of potential risk, including, but not limited to: legal compliance, liability exposure, health and safety, human resources, contracting, technology, security of information, client rights and confidentiality, and finances. Such practices contribute to mission fulfillment by protecting the organization's long-term sustainability.

Note: *Please see the RPM Reference List and Artificial Intelligence Reference List for the research that informed the development of these standards.*

Table of Evidence

Self Study Evidence

No Self Study Evidence

Risk Prevention and Management

RPM 1: Legal and Regulatory Compliance

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The organization annually reviews compliance with applicable federal, state, and local laws, codes, and regulations, including those related to:

a. licensure;
b. facilities;
c. accessibility;
d. health and safety;
e. finances;
f. human resources;
g. contracting; and
h. technology.

Related Standards: AFM 11.04, AFM 4.01, AFM 8.02, AFM 8.04, ASE 4.02, CR 2, FIN 2.02, FIN 5.04, GOV 5.01, GOV 5.06, HR 2.02, HR 2.03, HR 2.04, HR 5.01, NET 3.01, TS 3.03

Interpretation: Regarding *element b, organizations that rent facilities should obtain relevant documentation from their landlord. If the organization cannot obtain access to the required documentation from its landlord or from relevant public or private health and safety authorities, the organization may also solicit a recognized expert to verify compliance with applicable laws and safety codes.*

Examples: *Regarding element b, examples of relevant regulations and codes can include: (a) certification of occupancy requirements; (b) zoning and building codes; (c) occupational safety and health administration codes; (d) health, sanitation, and fire codes; and (e) elevator inspections.*

Regarding element d, relevant requirements can include, for example, universal precautions for minimizing exposure to contagious and infectious disease; and storage, cleaning, and disposal of medical waste.

Regarding element f, it is recommended practice to conduct an annual review of human resource practices to ensure compliance with applicable employment and labor laws. The human resource management field refers to this annual review as an annual "audit." Examples of human resource laws and regulations include those pertaining to: (a) use of independent contractors; (b) use of contingent workers such as temporary employees, volunteers, and leased workers; (c) fair employment practices, including non-discrimination and harassment; (d) compensation and benefits; (e) maintenance of personnel records; (f) selection and retention practices, including retention of hiring records; and (g) background checks.

Regarding element h, applicable laws, codes, and regulations pertaining to the adoption and use of technology can include those related to: (a) cybersecurity; (b) electronic health records and HIPAA compliance; (c) data security; (d) intellectual property protections; (e) electronic communications and social media regulations; (f) AI adoption and use, including prohibited uses or what decisions can or cannot be aided by AI; and (g) any organizational functions in which AI or other technology has been embedded such as hiring or performance management (e.g., laws governing fair employment practices).

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement.
3	Practice requires significant improvement; e.g.,

- One of the elements has not been reviewed in more than two years; or
- The organization has been notified of compliance or licensure problems and is working with the relevant authority to remediate deficiencies.

4 Implementation of the standard is minimal or there is no evidence of implementation at all; e.g.,

- Two elements have not been reviewed in more than two years; or
- The organization is under sanction due to noncompliance with legal or regulatory requirements; or
- The letter certifying compliance with all applicable laws was not signed or was otherwise inadequate.

Table of Evidence

Self Study Evidence

* • Provide a letter signed by the Governing Body Chair and CEO certifying the organization is presently in compliance with applicable laws and regulations	
* • Procedures for reviewing compliance with applicable laws, codes, and regulations related to management, operations, and services delivered Networks Only • Procedures for ensuring provider compliance with licensure requirements and applicable laws and regulations for services provided by the network	

Site Visit Evidence

*
- Results of most recent annual, internal compliance reviews
- Governing Body minutes for most recent discussion of legal compliance
- Relevant licenses as applicable to the organization's programs and operations
- Reports from licensing/regulatory review that include adverse findings or loss of licensure, as applicable

Networks only

- Copies of relevant licenses and legal regulation documents, as applicable to the providers, made available at the office of the managing entity

On-Site Activities

*
- Interviews may include:

1. Governing body
2. CEO
3. Relevant personnel

RPM 2: Risk Prevention and Management

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The organization identifies and reduces potential loss and liability by:

a. conducting prevention and risk reduction activities; and
b. monitoring and evaluating risk prevention and management effectiveness.

Rating Indicators:

1	The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 2 Practice standards.
2	Practices are basically sound but there is room for improvement, as noted in the ratings for the RPM 2 Practice standards.
3	Practice requires significant improvement, as noted in the ratings for the RPM 2 Practice standards.
4	Implementation of the standard is minimal or there is no evidence of implementation at all, as noted in the ratings for the RPM 2 Practices standards.

Table of Evidence

Self Study Evidence

*	• Procedures for quarterly review of immediate and ongoing risks	
*	• Procedures for investigation and review of critical incidents	

Site Visit Evidence

*	• Quarterly risk management reports • Results of independent investigations of critical incidents • Governing body and management meeting minutes where risk prevention and management activities are reviewed

On-Site Activities

*	• Interviews may include: 1. Governing Body 2. CEO 3. Relevant personnel

RPM 2.01 (FP)

The organization conducts a quarterly review of immediate and ongoing risks that includes a review of incidents, critical incidents, accidents, and grievances related to the following, as appropriate to the program or service:

a. facility safety issues;
b. serious illness, injuries, and deaths;
c. situations where a person was determined to be a danger to himself/herself or others;
d. client rights and confidentiality violations;
e. technology use, including artificial intelligence (AI);
f. service modalities or therapeutic interventions; and
g. the use of restrictive behavior management interventions, such as seclusion and restraint.

Related Standards: ASE 4, ASE 5, ASE 5.01, CR 1.05

FEC Interpretation: *In credit counseling organizations, only elements (a) through (e) could potentially apply.*

EAP Interpretation: *In employee assistance programs, only elements (a) through (e) could potentially apply.*

Examples: *Regarding element b, serious illnesses can include those illnesses that pose a significant, widespread risk to public health or the health of the organization's staff and persons served.*

Example: *The organization can disaggregate critical incident data to identify trends, such as disproportionate use of restrictive interventions with specific populations.*

Note: *Results of the quarterly reviews may inform the annual insurance needs assessment in RPM 3.01.*

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Reviews are conducted quarterly but one of the elements is not fully addressed.
3	Practice requires significant improvement; e.g., • The organization conducts reviews less than quarterly; or • Two elements are not fully addressed; or • One element is not addressed at all.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 2.02 (FP)

The organization conducts a review of each incident, serious occurrence, accident, and grievance that involves the threat of or actual harm, serious injury, or death; and review procedures:

a. require that the investigation be initiated within 24 hours of the incident and/or accident being reported and establish timeframes for completing the review;
b. require solicitation of statements from all involved individuals;
c. ensure an independent review;
d. require timely implementation and documentation of all actions taken;
e. address ongoing monitoring if actions are required to determine their effectiveness; and
f. address applicable reporting requirements.

Examples: *Root cause analysis can be a useful approach to reviewing serious incidents and accidents. Root cause analysis is a term used to describe a variety of techniques used by organizations to identify the cause of a problem and determine how to prevent that problem from recurring.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,

- Review procedures need strengthening; or
- One of the elements is not fully addressed; or
- Documentation could be improved.

3 Practice requires significant improvement; e.g.,

- One of the elements is not addressed at all; or
- While reviews are generally conducted, documentation is consistently missing; or
- There is evidence that at least one serious incident was not reviewed.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

Risk Prevention and Management

RPM 3: Insurance Protection

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The organization is adequately insured.

Rating Indicators:

1 The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 3 Practice standards.

2 Practices are basically sound but there is room for improvement, as noted in the ratings for the RPM 3 Practice standards.

3 Practice requires significant improvement, as noted in the ratings for the RPM 3 Practice standards.

4 Implementation of the standard is minimal or there is no evidence of implementation at all, as noted in the RPM 3 Practice standards.

Table of Evidence

Self Study Evidence

*	• Written notification to staff and governing body describing insurance coverage including the extent and limits of such coverage	
*	• Policy for legal assistance to personnel against whom claims are made	
*	Networks Only • Procedures for identifying and verifying provider insurance	

Site Visit Evidence

*	• Current insurance policies with descriptions, amounts, and dates of coverage • Results of most recent annual assessment of insurance needs Networks Only • Documentation of insurance verification • Copy of written communication to providers regarding required insurance

On-Site Activities

*	• Interviews may include: 1. Governing Body 2. CEO/CFO 3. Relevant personnel

Networks Only

- Interviews may include:

1. Provider Representatives

RPM 3.01 (FP)

The organization annually assesses insurance needs in consultation with insurance professionals or experienced legal counsel, and obtains coverage commensurate with the scope and complexity of its services.

Related Standards: ASE 4.02, GOV 5.06

Examples: *Relevant types of insurance can include: (a) general liability; (b) worker's compensation; (c) disability; (d) fire and theft; (e) medical; (f) indemnification; (g) professional liability; (h) officer's or director's liability; (i) automobile liability; (j) property and casualty; (k) malpractice; (l) cybersecurity; and (m) bonding or other forms of employee theft insurance, for all staff and governing body members who sign checks, handle cash or contributions, or manage funds.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.
The organization obtains professional consultation about appropriate coverage.

2 Practices are basically sound but there is room for improvement; e.g.,
- Insurance needs are reviewed annually, however coverage may be insufficient in some areas.

3 Practice requires significant improvement; e.g.,
- Insurance needs have not been reviewed for more than two years; or
- Coverage is clearly inadequate in one key area.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 3.02

The organization:

a. provides written notification to the governing body and personnel of the amount and type of insurance coverage related to the scope of their activities performed on the organization's behalf;
b. advises the governing body and personnel of the extent and limits of liability coverage; and
c. provides and assumes the cost of legal assistance to personnel against whom claims are made related to lawful, authorized actions taken within the course and scope of their duties.

Interpretation: *All personnel and governing body members must receive this information at the initiation of their association with the organization and when any changes to the level and/or type of insurance coverage occur.*

Interpretation: *This standard does not require the organization to provide assistance to personnel who commit unlawful acts or acts that are not conducted in the course of, or in furtherance of, their employment. In addition, this standard does not require the organization to provide legal assistance to personnel if the organization's legal counsel determines that doing so would constitute a conflict of interest.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- The organization generally provides a written description but on occasion the disclosure is verbal and informal.

3 Practice requires significant improvement; e.g.,
- The organization provides information only upon request or provides partial disclosure.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 3.03

The network annually verifies that provider insurance coverage is current and meets the organization's requirements stated in the contract.
NA: The organization is not a network management entity and is not assigned the Network Administration (NET) standards.

Related Standards: GOV 5.06

Note: *See RPM 6.04 for more information on establishing and communicating insurance requirements to network service providers.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- Procedures for identifying/specifying level and type of insurance or for annually verifying coverage need strengthening.

3 Practice requires significant improvement; e.g.,
- Annual verification not documented for all providers; or
- Some providers did not meet insurance requirements yet continue to provide network services.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

Risk Prevention and Management

RPM 4: Technology and Information Management

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The organization's technology and information systems have sufficient capability to support operations, service delivery, strategic planning, and quality improvement activities.
Related Standards: NET 2.02, NET 7

Interpretation: *The standards in this section address the management of all types of paper and electronic information maintained by the organization, including:*

1. *case records and other information of persons served;*
2. *administrative, financial, and risk management records and reports;*
3. *personnel files and other human resources records or data; and*
4. *performance and quality improvement data and reports.*

Examples: *Implementing a controlled document system is one way an organization can organize, track, store, and ensure the use of the most current version of documents. These systems address processes for: (a) updating, creating, and deleting documents; (b) notifying users of changes; (c) identifying documents; and (d) maintaining an inventory of documents.*

Rating Indicators:

1	The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 4 Practice standards.
2	Practices are basically sound but there is room for improvement, as noted in the ratings for the RPM 4 Practice standards.
3	Practice requires significant improvement, as noted in the ratings for the RPM 4 Practice standards.
4	Implementation of the standard is minimal or there is no evidence of implementation at all, as noted in the ratings for the RPM 4 Practice standards.

Table of Evidence

Self Study Evidence

*	• Technology assessment	
*	• Information management procedures/guidelines	
*	• AI acceptable use policy	

Site Visit Evidence

*	• Documentation of the annual review of AI Acceptable Use Policy • Agreements with third parties (e.g., technology or information management vendors, business associates, etc.), when applicable

On-Site Activities

*

- Interviews may include:

1. Information Systems Manager
2. Relevant personnel

- Observe Information Systems

RPM 4.01

The organization assesses its technology and information management needs including a review of:

a. current technology and information systems in use by the organization;
b. short- and long-term goals for utilizing technology; and
c. current technical skills of staff and need for staff training.

Related Standards: AFM 2.03, GOV 2.04, GOV 5.06, TS 1.01

Interpretation: *The technology assessment should include artificial intelligence (AI) regardless of whether the organization is currently using it. This ensures preparedness for potential adoption and helps mitigate risks that may arise if staff are using AI without clear policies or guidance. See RPM 4.04 and RPM 8 for more information on ethical and responsible AI use.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- One of the standard's elements was not fully addressed.

3 Practice requires significant improvement; e.g.,
- The assessment is very basic and provides minimal guidance to staff; or
- One of the elements was not addressed at all.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 4.02

The organization has an information management system that:

a. gives personnel consistent, timely, and appropriate access to all types of electronic and paper records; and
b. supports continuity and integration of care across programs and services by giving timely access to information about persons served to practitioners across the organization, as appropriate.

Related Standards: NET 2.03

Interpretation: *Organizations moving to electronic systems may need to develop procedures for maintaining both electronic and paper records including procedures for maintaining consistency between the two file types and ensuring the electronic record is comprehensive and complete. If there are components of paper records that cannot be accommodated electronically, the organization should consider how it will retain and document the existence of supplemental, paper-based portions of records.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,

- A formal system is in place, but is not fully implemented so locating records may sometimes be time consuming or difficult.

3 Practice requires significant improvement; e.g.,
- The system is informal and unsystematic; or
- Records are occasionally misplaced.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 4.03

The organization's electronic information systems are capable of:

a. capturing, tracking, and reporting financial, compliance, and other business information;
b. longitudinal reporting and comparison of performance and outcomes over time; and
c. the use of clear and consistent formats and methods for reporting and disseminating data.

Related Standards: FIN 3.02, FIN 3.03, FIN 5.01, PQI 5.02

Interpretation: *"Electronic information systems" are used for collecting, storing, analyzing, and disseminating information electronically. An electronic information system may consist of a single desktop or larger network of computers, laptops, and/or devices. Organizations are not required to implement robust electronic information systems; rather they must have systems that are appropriate for supporting their administrative operations and service delivery.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- Some aspects of the system need further development.

3 Practice requires significant improvement; e.g.,
- The system is basic and minimally supports the organization's data needs.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 4.04 (FP)

The organization maintains an AI acceptable use policy that prioritizes the needs of people and communities and:

a. provides clear guidance on whether AI use is permitted, which applications are approved, their intended purpose, and guidelines for their responsible use;
b. reflects the organization's data security and confidentiality policies and procedures;
c. aligns with the organization's mission, vision, values, and strategic plan; and
d. is reviewed and updated annually.

Related Standards: CR 2, HR 2

Interpretation: *To avoid the need for frequent updates, the AI acceptable use policy can state that only AI applications that have been reviewed and approved may be used, and then refer to a separate list of approved tools that is maintained by the AI oversight group for more information.*

Examples: *Regarding element b, AI data security measures can include: (a) prohibiting personal information (e.g., personally identifiable information, financial information, and personal health information) about persons served, staff, volunteers, or contractors from being entered into unsecured AI tools; (b) limiting the collection and storage of data to only what is necessary for the AI's specific purpose; (c) requiring personal data be anonymized, whenever possible, before being entered into secured*

AI systems; (d) permitting the inclusion of confidential or sensitive information in AI outputs only when necessary for service delivery; and (e) protecting AI outputs that contain confidential or sensitive information from intentional or unintentional theft, unauthorized use or disclosure, damage, or destruction as outlined in RPM 5.

Examples: *Regarding element c, the organization can demonstrate that its AI acceptable use policy is aligned with its mission, vision, and values by, (a) referencing its mission statement in the policy and outlining how AI use is intended to support the delivery of human-centered, high-quality services; (b) defining acceptable and prohibited uses of AI within the context of the organization's vision and values, prohibiting uses of AI that directly conflict with these; and (c) tailoring the language in the AI policy to reflect the organization's stated mission, vision, and values rather than relying solely on technological jargon or generic language.*

Note: *Organizations may fully incorporate their AI acceptable use policy into their existing data security and confidentiality policies and procedures. When that is the case, evidence of implementation for this standard will overlap with evidence provided in RPM 5 and CR 2.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- An AI acceptable use policy is in place, but some aspect of the policy needs further development.

3

Practice requires significant improvement; e.g.,

- The policy is very basic and provides minimal guidance to staff; or
- The policy is not well-understood by staff, or is frequently not followed; or
- A policy is still under development.

4

Implementation of the standard is minimal or there is no evidence of implementation at all.

Risk Prevention and Management

RPM 5: Security of Information

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

Electronic and printed information is protected against intentional and unintentional destruction or modification and unauthorized disclosure or use.
Related Standards: CR 2

Interpretation:*The standards in this section address security of all types of paper and electronic information maintained by the organization, unless otherwise noted, including:*

1. *case records and other information of persons served;*
2. *administrative, financial, and risk management records and reports;*
3. *personnel files and other human resources records or data; and*
4. *performance and quality improvement data and reports.*

Rating Indicators:

1 The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 5 Practice standards.

2 Practices are basically sound but there is room for improvement, as noted in the ratings for the RPM 5 Practice standards.

3 Practice requires significant improvement, as noted in the ratings for the RPM 5 Practice standards.

4 Implementation of the standard is minimal or there is no evidence of implementation at all, as noted in the ratings for the RPM 5 Practice standards.

Table of Evidence

Self Study Evidence

*	• Data security policies	
*	• Data security procedures, including HIPAA compliance as applicable	
*	• Policies on the use of social media, electronic communications, and mobile devices	
*	• Procedures on the use of social media, electronic communications, and mobile devices	
*	• Procedures for managing data interruptions/disaster recovery plan	

Site Visit Evidence

*	• Agreements with third parties (e.g., information technology vendors, business associates, etc.), when applicable • Results of HIPAA compliance review

On-Site Activities

*

- Interviews may include:

1. Relevant personnel

- Observe case record room/files and information system accessibility

RPM 5.01

The organization protects confidential and other sensitive information from theft, unauthorized use or disclosure, damage, or destruction both on- and off-site by:

a. limiting access to authorized personnel on a need-to-know basis;
b. using firewalls, anti-virus and related software, and other appropriate safeguards;
c. monitoring security measures on an ongoing basis;
d. having the ability to remotely wipe or disable mobile devices when a device is lost, stolen, repurposed, or discarded, if applicable; and
e. maintaining paper records in a secure location when not in use by authorized staff.

Examples: Regarding *element a, the organization may limit access to authorized personnel by: (a) limiting access based on staff role within the organization; (b) using encryption; (c) ensuring the electronic system requires strong passwords/passcodes for access to confidential information, requires passwords/passcodes to be regularly changed, locks the user out of the system for incorrect login attempts, and automatically times out after a period of inactivity and prompts reauthentication; (d) disabling the equipment, passwords, and access of former employees; and (e) ensuring the system can track who accesses confidential information in the system and record when information is altered or deleted, also known as audit logs.*

Regarding element e, secure storage of paper records can include: (a) locked file cabinets; (b) a locked file room with limited access or a gatekeeper system whereby one person or a few people can unlock the file storage area or access the files themselves; or (c) a system using a keypad or keys, where only authorized individuals are given the keypad code or copies of the keys.

Note: *Please see the Facility Observation Checklist for additional guidance on this standard.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- Some aspect of the organization's data security procedures needs strengthening; or
- With few exceptions, procedures are understood by staff and are being used.

3 Practice requires significant improvement; e.g.,
- There is a major deficiency in at least one of the listed elements resulting in risk to the organization; or
- There have been instances of unauthorized access to confidential or sensitive information; or
- Procedures are not well-understood or used appropriately.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 5.02

Proper safeguards protect confidential information when transmitted electronically.

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement.
3	Practice requires significant improvement.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 5.03

The organization has policies and procedures addressing the use and monitoring of:

a. social media;
b. electronic communications; and
c. mobile devices, including staff-owned devices, if applicable.

Examples: *Risks associated with the use of social media and electronic communications may include: (a) unauthorized or prohibited contact between staff and service recipients; (b) unauthorized or inappropriate use of organization logos or trademarks; (c) personal comments or opinions that can be misconstrued as representing the views of the organization, or that present the organization in a negative light; (d) inadvertent or deliberate disclosure of confidential or proprietary business information; and (e) inadvertent or deliberate disclosure of confidential or protected information about service recipients.*

Examples: *A social media policy typically addresses: (a)*

the organization's definition of "social media"; (b) responsible parties (e.g., individuals responsible for setting up accounts, contributing content, monitoring content, etc.); (c) prohibited forms of communication; (d) the appropriate use of social media, including confidentiality and privacy considerations; and/or (e) consequences for failure to follow the policy and/or related guidelines.

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Some aspect of the procedures need further development.
3	Practice requires significant improvement; e.g., • Procedures are very basic and provide minimal guidance to staff; or • Procedures are not well-understood by staff or are frequently not being followed; or • Procedures are still under development and have only been partially implemented.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 5.04

The organization is prepared for planned and unplanned interruptions of data and limits the disruption to its operations and service delivery by:

a. maintaining procedures for managing data interruptions and resuming operations;
b. backing up electronic data regularly, with copies maintained off premises; and
c. regularly testing the organization’s back-up plan including data restoration processes.

Related Standards: ASE 6.01, ASE 6.02

Interpretation: *This standard applies to any instance of prolonged data disruption, regardless of whether there is a corresponding emergency.*

Examples: *A disaster recovery plan is a set of procedures put in place to protect and recover an organization's IT infrastructure to ensure the continuation of business in the event of a disaster. The plan clearly defines what disaster means for the organization's administrative operations and service delivery. It also includes specific guidance on when primary systems are considered nonfunctional/shut down, at what point secondary systems should be activated, who has the authority to make that determination, and how to inform staff and stakeholders that a disaster has occurred.*

Factors that increase the effectiveness of a disaster recovery plan include: (a) training staff on response procedures; (b) practicing procedures/conducting downtime drills; (c) testing disaster recovery systems on an ongoing basis; and (d) monitoring plan implementation.

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Some aspects of the procedures need further development.
3	Practice requires significant improvement; e.g., • Procedures are very basic and provide minimal guidance to staff; or • Procedures are still under development and have only been partially implemented.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 5.05

The organization ensures its electronic system for managing health records or protected health information limits access to information in accordance with confidentiality rules and the person's privacy preferences to the greatest extent possible.
NA: The organization does not electronically manage health records or protected health information.

Interpretation: *If the electronic health record system employed by the organization is not able to meet all client privacy preferences, the organization informs the service recipient of the system's limitations and obtains consent for the exchange of electronic health information based on those restrictions. If the organization cannot accommodate the client's preferences and their consent is not obtained, the organization should connect the person to another provider who can meet their needs and privacy preferences.*

Examples: *The HIPAA Security Rule and federal interoperability standards guide organizations regarding the technical capabilities and safeguards expected of electronic health record systems. Using Certified EHR Technology (CEHRT) supports compliance with HIPAA and federal interoperability requirements when paired with appropriate organizational safeguards.*

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Procedures for monitoring and maintaining legal compliance require greater clarity or specificity.
3	Practice requires significant improvement; e.g., • The organization is aware of compliance problems and is working to remediate deficiencies.
4	Implementation of the standard is minimal or there is no evidence of implementation at all; e.g., • The organization is aware of compliance problems and is not working to remediate deficiencies.

Risk Prevention and Management

RPM 6: Contracts and Service Agreements

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The pursuit of contracts and service agreements is:

a. consistent with the organization's mission and values;
b. aligned with, and supportive of, the organization's service array and resource development goals; and
c. responsive to the needs and desired outcomes of persons served.

Interpretation: *These standards apply to all contracts entered into by the organization in which it acts as a purchaser or vendor of social and human services, as well as to contracts for the purchase of support services, such as technology, maintenance, or transportation services. These standards do not apply to contracts with individual consultants and independent contractors, which are addressed in Human Resources Management (HR 7).*

Note: *See Applicability of COA Standards to Contracts and Non-contractual Service Agreements for additional guidance on this standard.*

Rating Indicators:

1	The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 6 Practice standards.
2	Practices are basically sound but there is room for improvement, as noted in the ratings for the RPM 6 Practice standards.
3	Practice requires significant improvement, as noted in the ratings for the RPM 6 Practice standards.
4	Implementation of the standard is minimal or there is no evidence of implementation at all, as noted in the ratings for the RPM 6 Practice standards.

Table of Evidence

Self Study Evidence

*	• Contracting procedures	
*	• List of contracts/service agreements/memoranda of understanding (MOU)	

Site Visit Evidence

*	• Contracts/service agreements/MOUs • Board meeting minutes of governing body review of significant contracts from the previous 12 months

On-Site Activities

*	• Interviews may include:

1. Governing Body
2. CEO/CFO
3. Contract manager(s)
4. Vendors

Networks Only:

- Interviews may include:

1. Provider CEO/CFO
2. Provider contract manager(s)

RPM 6.01

The organization:

a. establishes a system of standardized contracting practices;
b. pursues contracts that serve the best interests of persons served, the organization, and its workforce, not private interests;
c. seeks opportunities to source goods and services from a wide range of suppliers;
d. conducts due diligence in contracting activities, including review of risks;
e. uses competitive bidding, when applicable; and
f. ensures governing body review of significant contracts.

Related Standards: GOV 5.06

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • One of the elements needs strengthening.
3	Practice requires significant improvement; e.g., • Two of the elements need strengthening; or • One element is not addressed at all; or • The governing body does not review significant contracts.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 6.02 (FP)

Written contracts:

a. are reviewed by legal counsel or another qualified individual prior to signing; and
b. contain all significant terms and conditions in accordance with applicable law.

Interpretation: *"Significant terms" should include, as appropriate to the type of contract:*

1. *roles and responsibilities of participating organizations;*
2. *services to be provided;*
3. *clearly defined performance goals;*
4. *measurable outcomes;*
5. *service authorization, including eligibility criteria;*
6. *provisions for training and technical support, as necessary;*
7. *duration of contract, including delineation of follow-up services;*
8. *policies and procedures for sharing information;*
9. *confidentiality and privacy protections;*
10. *methods for resolving disputes;*

11. *a plan and procedure for timely payment, and consequences for failure to pay;*
12. *necessary documentation and means of reporting to funding or oversight bodies; and*
13. *conditions for termination of the contract.*

Interpretation: *When contracting with AI vendors or vendors whose products embed AI, significant terms should also include contract provisions on bias auditing, data usage and security, and notification procedures and liability in the event of a data breech.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- Though all contracts are reviewed, contracting procedures do not address the standard.

3 Practice requires significant improvement; e.g.,
- Terms and conditions of contracts are often general, nonspecific, or unclear; or
- There is evidence that some contracts have not been reviewed as required by the standard.

4 Implementation of the standard is minimal or there is no evidence of implementation at all; e.g.
- Contracts are totally inadequate in specification of terms and conditions; or
- Contracts are not routinely reviewed as required.

RPM 6.03

Non-contractual service agreements include, as appropriate:

a. services exchanged or provided, and/or the goals and objectives of such collaborations;
b. roles and responsibilities of each organization including reporting responsibilities;
c. procedures for sharing information;
d. confidentiality protections including signed written consent forms;
e. assignment of case coordination responsibilities;
f. service authorization procedures including accepting or rejecting cases; and
g. how to resolve communication difficulties.

NA: The organization does not enter into non-contractual service agreements.

Interpretation: *This standard applies to non-contractual arrangements, also known as Memorandums of Understanding (MOUs), in which organizations collaborate with service providers to deliver specific services to a person or persons. This could include, for example, a service in which a service provider voluntarily comes into the host organization's facility to provide weekly smoking cessation classes.*

Rating Indicators:

1 The organization's practices reflect full implementation of the standard.

2 Practices are basically sound but there is room for improvement; e.g.,
- Procedures need strengthening; or
- One element is not addressed at all.

3 Practice requires significant improvement; e.g.,
- Terms and conditions of service agreements are often general, nonspecific, or unclear; or
- At least two of the elements are not addressed at all.

4 Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 6.04 (FP)

Contracts for the provision of network services also include:

a. the network's requirements regarding provider participation in network quality improvement activities;
b. access to case record provisions;
c. utilization management protocols;
d. required levels and types of insurance; and
e. agreement to participate in network training.

NA: The organization is not a network management entity and is not assigned the Network Administration (NET) standards.

Related Standards: NET 11, NET 7

Examples: *Regarding element b, network management entities could require access to case information to conduct utilization management activities, verify billing, provide care coordination, and other network management activities.*

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Procedures need strengthening; or • One of the elements is not fully addressed.
3	Practice requires significant improvement; e.g., • The terms and conditions of contracts are often general, nonspecific, or unclear; or • At least two of the elements are not fully addressed; or • One element is not addressed at all.
4	Implementation of the standard is minimal or there is no evidence of implementation at all; e.g., • Contracts are totally inadequate in specification of terms and conditions.

RPM 6.05 (FP)

When organizations contract with artificial intelligence (AI) vendors, or vendors whose products embed AI, contracting procedures also require that prospective contractors disclose:

a. what data will be collected;
b. how long personally identifiable information (PII) or personal health information (PHI) will be stored, if applicable;
c. whether PII and PHI will be shared, how they will be shared, and for what purposes;
d. what precautions exist to protect collected data from intentional and unintentional destruction or modification and unauthorized disclosure or use;
e. who retains ownership and control of the data and any outputs derived from it;
f. information on the training data sets that were used and any known model limitations;
g. its processes for continuing to audit the model to ensure accurate, unbiased results; and
h. any third-party certifications they have.

NA: The organization does not have any contracts with AI vendors or vendors whose products embed AI.

Interpretation: *Regarding element g, external certification of AI products is not required to move forward with a particular vendor. However, if a vendor lacks third-party verification of its commitment to data security and privacy, it becomes even more important that it provides the organization with the information outlined in elements a through f of the standard.*

Interpretation: *When selecting commercially available AI tools, preference should be given to:*

1. *vendors that allow the organization to opt-out of its data being used to train the model;*
2. *vendors whose data handling practices comply with the organization's own privacy and data security policies;*
3. *vendors that have demonstrated experience working with similar types of organizations; and*
4. *paid versions of tools when licensed access provides improved privacy protections, accuracy, or data controls.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- Procedures need strengthening; or
- One of the elements is not fully addressed.

3

Practice requires significant improvement; e.g.,

- Three of the elements are not fully addressed; or
- Two elements are not addressed at all.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- Contracting procedures do not address contracting with AI vendors at all.

Risk Prevention and Management

RPM 7: Quality Monitoring of Contracted Social and Human Services

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The organization monitors and evaluates the quality and effectiveness of social and human services purchased from other provider organizations.
NA: The organization does not purchase social and human services from other organizations.

Interpretation: *These standards only apply to contracts entered into by the organization in which it purchases social and human services from another organization, such as when a shelter program purchases vocational rehabilitation services for its clients. They do not apply to contracts where the organization acts as a vendor of social and human services or to contracts for the purchase of support services, such as technology, maintenance, or transportation services. These types of contracts are addressed in RPM 6.*

The standards in this Core are also not applicable to contracts with individual consultants and independent contractors, which are addressed in Human Resources Management (HR 7).

Network Interpretation: *These standards apply to services purchased from all service providers, including owner and partner organizations, and individual practitioners, as applicable.*

Rating Indicators:

1	The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 7 Practice standards.
2	Practices are basically sound but there is room for improvement, as noted in the ratings for the RPM 7 Practice standards.
3	Practice requires significant improvement, as noted in the ratings for the RPM 7 Practice standards.
4	Implementation of the standard is minimal or there is no evidence of implementation at all, as noted in the ratings for the RPM 7 Practice standards.

Table of Evidence

Self Study Evidence

*

- Contract monitoring procedures

Site Visit Evidence

*

- Contracts
- Contractor progress reports
- Documentation of contract remediation as appropriate

On-Site Activities

*

- Interviews may include:

1. Governing Body
2. CEO/CFO
3. Contract manager(s)

Networks Only:

- Interviews may include:

1. Provider CEO/CFO
2. Provider contract manager(s)

RPM 7.01 (FP)

Contractors who provide human or social services:

a. have sufficient human and financial resources to fulfill the terms of the contract; and
b. are licensed or otherwise legally authorized to provide the contracted services.

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Procedures need strengthening.
3	Practice requires significant improvement; e.g., • Documentation is poorly maintained or some documentation is missing; or • The organization has not conducted the required due diligence in some instances.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 7.02

The organization routinely monitors contractor progress toward fulfilling the terms of the contract.

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Monitoring procedures need strengthening.
3	Practice requires significant improvement; e.g., • Monitoring is not consistently done.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

RPM 7.03

Contracts for social and human services include:

a. service quality, client satisfaction, and outcomes that accord with the organization’s expectations;
b. criteria for evaluating vendor performance;
c. a process for remediating performance issues; and
d. protocols for routine communication of related data.

Rating Indicators:

1	The organization's practices reflect full implementation of the standard.
2	Practices are basically sound but there is room for improvement; e.g., • Monitoring procedures need strengthening.
3	Practice requires significant improvement; e.g., • One of the elements has not been implemented.
4	Implementation of the standard is minimal or there is no evidence of implementation at all.

Risk Prevention and Management

RPM 8: Ethical and Responsible Use of Artificial Intelligence (AI)

Purpose

Comprehensive, systematic, and effective risk prevention and management practices sustain the organization's ability to positively impact the communities and people it serves by reducing its risk, loss, and liability exposure.

The organization’s use of AI is aligned with its mission and values, minimizes risk, and prioritizes the well-being of people and communities.

NA: The organization is not using AI systems of any kind in its operations, and its policies prohibit staff from using AI applications.

Rating Indicators:

1

The organization's practices fully meet the standard, as indicated by full implementation of the practices outlined in the RPM 8 Practice standards.

2

Practices are basically sound, but there is room for improvement, as noted in the ratings for the RPM 8 Practice standards.

3

Practice requires significant improvement, as noted in the ratings for the RPM 8 Practice standards.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all, as noted in the ratings for the RPM 6 Practice standards.

Table of Evidence

Self Study Evidence

*	• AI monitoring and accountability procedures	
*	• Job description and resume of qualified professional(s) responsible for AI model design, training, and maintenance, and/or formal agreement with an appropriate vendor, when applicable	

Site Visit Evidence

*	• Results of AI risk-benefit analysis • Informational materials and/or AI disclosure statement(s) provided to applicable stakeholder groups • Documentation of AI oversight activities (e.g., review and approval for AI tools/applications, bias reports and evidence of corrective action when indicated, impact reports and evidence of corrective action when indicated, etc.) • Documentation of stakeholder engagement in AI discussions and decision-making

On-Site Activities

*

- Interviews may include:

1. Relevant personnel
2. IT personnel responsible for AI model design, training, and maintenance, when applicable
3. Persons served
4. Personnel responsible for AI oversight
5. AI vendors, when applicable

- Observe AI applications currently in use
- Review AI Acceptable Use policy on the public website
- Review system for documenting AI-assisted decisions impacting rights or safety

RPM 8.01

Before implementing an AI strategy, the organization conducts a risk-benefit analysis that evaluates the potential impacts of AI on the organization and its stakeholders.

Examples: *Relevant stakeholders may include staff at all levels of the organization, persons served, community partners, funders, and others who may be impacted by the organization's AI use.*

Examples: *Relevant questions that can help organizations to evaluate potential impact include: what problem is this AI solution intended to address, who will benefit from this solution, do the potential beneficiaries want it, and what are the risks and how might they be mitigated?*

This evaluation can consider, for example, AI's potential impacts on: (a) client rights, dignity, and privacy; (b) professional roles, judgment, and workforce wellbeing; (c) service quality and access; (d) community relationships and stakeholder trust; and (e) the environment.

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- The risk/benefit analysis was somewhat informal but results clearly informed AI implementation at the organization; or
- Written evidence of the risk/benefit analysis could be strengthened but staff were able to describe how the analysis informed AI implementation.

3

Practice requires significant improvement; e.g.,

- There is evidence that a discussion of potential risks and benefits occurred, but it is not clear that impacts on both the organization and its stakeholders were considered; or
- Risks and benefits were discussed, but there is no evidence that this informed the adoption of AI strategies in any significant way; or
- Staff report that discussions around the potential benefits of AI adoption occurred, but risks were not considered.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- Little or no effort was made to consider the risks and benefits of AI adoption prior to implementation.

RPM 8.02

Organizations that are building or significantly customizing technology using coding methods ensure the availability of an appropriately qualified team that is responsible for:

a. training AI models using large, accurate, diverse, and representative datasets;
b. documenting model design, assumptions, limitations, and training data and maintaining version control;
c. regularly retraining and validating the model to reflect changes in real-world conditions or to address issues that arise through ongoing monitoring activities; and
d. providing technical assistance and maintenance.

NA: The organization is not building or significantly customizing technology using coding methods.

Interpretation: *Building or significantly customizing tools using coding methods includes activities such as software design and development, data architecture or infrastructure design, or creating digital platforms, applications, or tools that go beyond the basic customization of off-the-shelf products using non-coding methods.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- An appropriately qualified team is in place, but one of the elements is not fully implemented.

3

Practice requires significant improvement; e.g.,

- An appropriately qualified team is in place but two of the elements are not fully implemented; or
- An appropriately qualified team is in place but one of the elements is not addressed at all.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- The organization is building or significantly customizing AI tools without the support of an appropriately qualified team; or
- Staff responsible for building or customizing AI tools report feeling underqualified; or
- An appropriately qualified team is in place but two of the elements are not addressed at all.

RPM 8.03 (FP)

A copy of the AI acceptable use policy is available on the organization’s public website, and stakeholders are helped to understand:

a. why, when, and how AI is being used, including what data is being collected, stored, and/or shared;
b. the risks and ethical considerations of AI use;
c. what safeguards are in place to mitigate risk and unintended consequences of AI use;

d. how to provide feedback on AI use and report negative impacts for investigation and remediation; and
e. how to opt out of AI use, including data collection when applicable.

Related Standards: ASE 3.03, CR 1.05, CR 2

Interpretation: *When persons served refuse the use of AI technologies, the organization should provide services without it. If that is not possible, the individual must be connected with another provider that meets their needs.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

1. The acceptable use policy is available on the public website, but stakeholders report that one element is not fully understood; or
2. The AI acceptable use policy is difficult to find on the website and, as a result, is not likely to be accessed but all elements are well understood by stakeholders; or
3. Some minor aspect of the AI policy is difficult to understand.

3

Practice requires significant improvement; e.g.,

- Several aspects of the AI policy are difficult to understand; or
- The AI acceptable use policy is not available on the public website; or
- Two of the elements are not fully understood by stakeholders; or
- One element is not explained at all to stakeholders.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- There is little to no transparency regarding how the organization is using AI.

RPM 8.04

Client-facing, AI-enabled tools, such as FAQ chatbots, clearly inform users that they are interacting with an AI-powered system and provide a clear, accessible option for connecting with a human when desired.

NA: The organization does not use client-facing, AI-enabled tools (e.g., FAQ chatbots or virtual assistants).

Interpretation: *The use of conversational bots for talk therapy is an emerging practice and is not yet well established. There have been documented instances in which the use of such tools for behavioral health support has resulted in serious harm, particularly among vulnerable populations such as children and adolescents. The American Psychological Association has indicated that more evidence is needed to demonstrate the effectiveness and safety of these tools in behavioral health care. As such, the use of conversational AI chatbots as a substitute for a qualified mental health provider is not recommended. See RPM 8.05 for more information on maintaining human oversight and accountability of all AI-assisted processes and decision-making.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- The method for notifying users when they are interacting with AI is present but could be more prominently displayed; or
- Options for connecting with a human exist but could be more convenient or user-friendly.

3

Practice requires significant improvement; e.g.,

- The method for notifying users when they are interacting with AI is adequate, but options for connecting with a human are not present.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- There is little to no transparency for users interacting with client-facing, AI-enabled tools.

RPM 8.05 (FP)

The organization maintains human oversight and accountability of all AI-assisted processes by establishing mechanisms for:

a. conducting sufficient pre-deployment testing;
b. detecting and mitigating bias in AI inputs and outputs;
c. reporting, investigating, and remediating negative impacts of AI;
d. regularly reviewing what data is available to AI tools and ensuring that the level of sharing continues to be appropriate;
e. human review of AI outputs for quality, accuracy, compliance, respect, and fairness prior to inclusion in the case record, dissemination, or use in decision making; and
f. documenting all AI-assisted decisions that impact rights or safety or have the potential to impact rights or safety.

Related Standards: CR 1.05, HR 2, HR 3.04

Interpretation: *AI may supplement human judgment and critical thinking, but should never replace them. The AI acceptable use policy submitted in RPM 4 should ensure human involvement and accountability in any decision-making that has the potential to impact rights or safety.*

AI-assisted decisions that impact rights and safety include, but are not limited to, those related to diagnosis or treatment; hiring, performance evaluation, promotion, or termination; assessment of risk of harm to self or others; allocation of resources; eligibility, access to services, triaging cases, or balancing caseloads across workers; adoption matching and child custody; and protective actions for children, older adults, or adults with disabilities. Some AI uses have the potential to impact rights or safety if the decisions they inform lead to negative outcomes, misinformation, or create unnecessary barriers to accessing needed supports or services.

Systems for tracking these AI-assisted decisions may vary based on the organization's size, IT infrastructure, maturity of AI integration, and AI use cases. Organizations may choose to use existing systems for tracking these decisions, such as case record notations or tracking systems embedded in AI tools or applications, or they may maintain separate logs or other tracking systems specifically designed for this purpose. The chosen tracking method should allow for transparency, accountability, and effective monitoring of AI-assisted decisions over time.

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- Two of the elements are not fully addressed; or
- One element is not addressed at all.

3

Practice requires significant improvement; e.g.,

- Three of the elements are not fully addressed; or
- Two of the elements are not addressed at all.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- The organization has established very few mechanisms for human oversight and accountability, posing a significant risk to the organization and its stakeholders.

RPM 8.06

The organization designates a multidisciplinary AI oversight group that is responsible for:

a. establishing and reviewing the organization’s AI acceptable use policy and its monitoring and accountability procedures;
b. receiving and responding to stakeholder feedback and questions;
c. investigating and remediating reports of harmful AI outcomes;
d. approving and regularly reviewing AI technologies and use cases; and
e. monitoring the impact of AI on the organization’s capacity to deliver services and meet the needs of persons served.

Interpretation: *When approving and/or reviewing AI use cases, organizations should consider factors that may impact their reliability, associated risks, and potential value, such as: (a) how often the AI is likely to encounter new or unexpected situations in the use case, (b) whether sufficient, accurate data exists to inform reliable predictions, (c) how willing impacted staff are to adopt the AI solution, (d) what the cost or impact will be if the AI makes errors, (e) what risks already exist in the current process and how might those risks change with the assistance of AI, (f) how likely staff are to use the technology in a way that falls outside its intended purpose, (g) how aligned the potential use case is with organizational goals, (h) how urgent the need is that the AI is intended to address, and (i) how much staff time will be required to review AI outputs compared to the time saved by automation.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

- The organization has identified a multidisciplinary team responsible for AI oversight, and there is evidence that all elements of the standard are being implemented.

2

Practices are basically sound, but there is room for improvement; e.g.,

- The organization has identified a person or team responsible for AI oversight, but one element of the standard is not fully implemented

3

Practice requires significant improvement; e.g.,

- A person or team responsible for AI oversight has been identified, but their responsibilities are not well defined; or
- There is little evidence that AI oversight responsibilities have been officially delegated, but there is evidence that some oversight mechanisms have been initiated (e.g., there is an AI acceptable use policy in place).

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- There is no evidence that AI oversight responsibilities have been delegated, and little to no evidence that oversight mechanisms have been established.

RPM 8.07

The organization engages stakeholders in ongoing discussions about the impact of AI and provides affected people and communities with meaningful opportunities to influence how AI is used in the organization.

Examples: *Literature on successful AI deployment in the workplace points to the early engagement of staff as central to successful AI adoption. Asking staff to identify real problems they would like to see addressed, providing opportunities for staff to experiment with different AI applications that could resolve their identified concerns, collecting and responding to feedback on how things went, and then expanding solutions across departments, functions, or use cases are all ways that organizations can promote engagement and buy-in among their staff.*

Examples: *The organization can promote meaningful engagement of stakeholders by requesting feedback on the use of AI, training staff on meaningful engagement practices and how to discuss AI within the context of service delivery, and informing individuals of how the organization will use their input and notifying them of any changes that were made as a result.*

Rating Indicators:

1

The organization's practices reflect full implementation of the standard.

2

Practices are basically sound, but there is room for improvement; e.g.,

- There is evidence that stakeholders were meaningfully engaged in discussions early on in AI adoption, but ongoing methods of engagement could be further developed.

3

Practice requires significant improvement; e.g.,

- There is evidence that stakeholders have been engaged in some conversations regarding AI use, but it is not clear that their feedback has been used to inform the organization’s AI use; or
- The organization has received and acted on some stakeholder feedback, but mechanisms for engagement are too informal and sporadic to be meaningful.

4

Implementation of the standard is minimal, or there is no evidence of implementation at all; e.g.,

- Little or no effort is made to provide meaningful opportunities for stakeholders to influence how AI is used in the organization.