AI Review

Monday, October 28, 2024 8:13 AM

. Establish AI Usage Policy and Scope

- **1.1 Define an AI Usage Policy**: Develop and document a formal AI usage policy outlining acceptable AI tools, purposes for their use, prohibited uses, and risk considerations, aligning with 12 CFR Part 748.
- **1.2 Establish Scope of AI Applications**: Identify all AI tools currently in use or planned for implementation across the organization, including AI models, machine learning algorithms, and decision-making systems that impact data management, cybersecurity, and member services.

2. Conduct a Risk Assessment for AI Applications

- **2.1 Identify AI-Related Risks**: Evaluate risks related to data privacy, cybersecurity, operational integrity, model bias, and legal compliance associated with AI tools.
- **2.2 Document and Rank Risks**: Rank risks based on potential impact and likelihood, documenting mitigative controls or compensating measures for each risk identified.
- **2.3 Review and Update Regularly**: Regularly assess and update risk analysis as AI tools evolve, accounting for new or altered regulations, technological advances, and organizational changes.

3. Implement Governance and Oversight

- **3.1 Define Roles and Responsibilities**: Assign a governance structure, identifying stakeholders responsible for AI oversight, including board members, compliance officers, data scientists, and IT security.
- **3.2 Establish an AI Oversight Committee**: Form an AI Oversight Committee responsible for reviewing AI risk assessments, compliance reports, model performance, and ongoing regulatory adherence.
- **3.3 Schedule Regular Governance Meetings**: Require regular meetings (quarterly or semi-annually) to review AI-related activities, compliance status, risk assessments, and any corrective actions or updates to the AI program.

4. Ensure Data Privacy and Protection

- **4.1 Define Data Access and Use Controls**: Limit access to data used by AI tools based on employee roles, ensuring only authorized personnel handle sensitive information.
- **4.2 Enforce Data Anonymization and Masking**: Where possible, use anonymization and masking techniques to protect personally identifiable information (PII) within datasets processed by AI.
- **4.3 Monitor Data Protection Standards**: Implement continuous monitoring of AI systems for adherence to data protection standards, using automated tools to flag any deviations.

5. Maintain Model Transparency and Explainability

- **5.1 Develop Explainable Models**: Ensure AI models are interpretable and that decision-making processes can be clearly explained to relevant stakeholders, including regulators and members if needed.
- **5.2 Document Model Logic and Parameters**: Keep detailed documentation on model parameters, algorithms used, and training data sources for transparency.
- **5.3 Provide Member Explanation**: Offer members a simple, understandable explanation of how AI-driven decisions may affect them, especially if decisions impact financial products, credit scores, or service availability.

6. Establish Robust Model Validation and Monitoring

- **6.1 Conduct Pre-Deployment Testing**: Validate AI models through testing on varied datasets, assessing accuracy, bias, and predictive validity before full-scale deployment.
- **6.2 Implement Continuous Monitoring**: Deploy monitoring systems to detect model drift, degradation in accuracy, and deviations from expected outcomes, including bias checks.
- **6.3 Require Regular Revalidation**: Revalidate AI models on an established schedule, documenting changes and conducting bias testing and performance benchmarking as part of each revalidation.

7. Implement Cybersecurity Controls for AI Systems

- **7.1 Assess AI Vulnerabilities**: Regularly conduct penetration testing and vulnerability assessments of AI infrastructure, considering AI-specific risks like adversarial attacks and data poisoning.
- **7.2 Enforce Access Control for AI Systems**: Restrict access to AI models, datasets, and production environments using multi-factor authentication (MFA) and role-based access controls (RBAC).
- **7.3 Maintain Incident Response Plans for AI Breaches**: Integrate AI-related scenarios into the incident response plan, establishing protocols for data breaches, unauthorized model access, and cybersecurity threats targeting AI.

8. Validate Compliance with Regulatory Requirements

- **8.1 Align with Appendix A Requirements**: Ensure that the AI systems support compliance with Appendix A to Part 748, emphasizing data security, confidentiality, and integrity.
- **8.2 Integrate AI into Compliance Reviews**: Include AI activities in regular compliance audits, focusing on data protection, cybersecurity measures, model transparency, and risk mitigation strategies.
- **8.3 Report to the Board of Directors**: Provide an annual AI compliance report to the board, detailing the use of AI tools, their impact on member information security, and compliance status with 12 CFR Part 748.

9. Implement Continuous Improvement and Training

- **9.1 Establish Training Programs**: Educate staff on AI compliance requirements, ethical considerations, and security practices, tailoring content to roles such as IT, compliance, and operations.
- **9.2 Foster a Culture of Responsible AI Use**: Encourage responsible and ethical AI use across the organization by embedding AI ethics into the organizational culture.
- **9.3 Document Lessons Learned**: Document outcomes from audits, incident responses, and periodic reviews, identifying areas for improvement and updating AI policies and procedures accordingly.

10. Develop Key Performance Indicators (KPIs) and Reporting Mechanisms

- **10.1 Define Compliance KPIs**: Set KPIs that track adherence to AI risk management and compliance, such as the number of models reviewed, revalidated models, identified biases, and mitigated risks.
- **10.2 Create Reporting Templates**: Develop standardized reports that track AI compliance status, incidents, and model performance, including summaries for regulatory bodies or internal audit.
- **10.3 Schedule Regular Board Reporting**: Regularly report AI compliance metrics, incident summaries, and regulatory alignment status to the board, ensuring ongoing oversight and transparency.

11. Audit AI Processes for Regulatory Adherence

- **11.1 Conduct Independent Audits**: Arrange for independent audits to assess AI practices, model accuracy, data security, and compliance with Part 748.
- **11.2 Address and Document Findings**: Document audit findings, initiate corrective actions, and track remediation progress, ensuring continuous compliance improvement.
- **11.3 Establish a Compliance Feedback Loop**: Use audit findings to refine AI governance, model validation, data security, and incident response measures, aligning AI program development with evolving regulatory standards.

Questions

Monday, October 28, 2024 8:14 AM

Section 1: AI Usage Policy and Scope

1.1 **Is there a documented policy that defines the acceptable use of AI within the organization?**

- ☐ Yes ☐ No ☐ Other (explain): __________

1.2 **Are the purposes and limitations of AI tools clearly outlined in the policy?**

- ☐ Yes ☐ No ☐ Other (explain): __________

1.3 **Has the credit union identified all AI tools currently in use or planned for future deployment?**

- ☐ Yes ☐ No ☐ Other (explain): __________

1.4 **How frequently is the AI usage policy reviewed and updated?**

- Answer: __________

Section 2: AI Risk Assessment

2.1 **Has the credit union conducted a risk assessment specific to the use of AI tools?**

- ☐ Yes ☐ No ☐ Other (explain): __________

2.2 **Are the potential risks of AI, such as data privacy, model bias, and cybersecurity, documented and ranked?**

- ☐ Yes ☐ No ☐ Other (explain): __________

2.3 **Is there a process to update the AI risk assessment as new risks or changes in AI usage emerge?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 3: Governance and Oversight

3.1 **Are roles and responsibilities for AI governance clearly defined?**

- ☐ Yes ☐ No ☐ Other (explain): __________

3.2 **Is there an established AI Oversight Committee?**

- ☐ Yes ☐ No ☐ Other (explain): __________

3.3 **How often does the AI Oversight Committee meet to review AI compliance and risk management?**

- Answer: __________

Section 4: Data Privacy and Protection

4.1 **Are access controls in place to restrict unauthorized access to data used by AI tools?**

- ☐ Yes ☐ No ☐ Other (explain): __________

4.2 **Is data anonymization or masking applied to sensitive information used in AI models?**

- ☐ Yes ☐ No ☐ Other (explain): __________

4.3 **Are data protection standards for AI models monitored continuously?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 5: Model Transparency and Explainability

5.1 **Are AI models designed to ensure transparency in decision-making processes?**

- ☐ Yes ☐ No ☐ Other (explain): __________

5.2 **Is model documentation maintained with details on logic, parameters, and training data sources?**

- ☐ Yes ☐ No ☐ Other (explain): __________

5.3 **Are members provided with an explanation of how AI-driven decisions may affect them?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 6: Model Validation and Monitoring

6.1 **Are AI models validated before deployment to assess accuracy, bias, and predictive validity?**

- ☐ Yes ☐ No ☐ Other (explain): __________

6.2 **Is there continuous monitoring of AI models to detect accuracy drift and biases?**

- ☐ Yes ☐ No ☐ Other (explain): __________

6.3 **Is there a process in place for regular revalidation of AI models?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 7: Cybersecurity for AI Systems

7.1 **Are penetration testing and vulnerability assessments conducted on AI infrastructure?**

- ☐ Yes ☐ No ☐ Other (explain): __________

7.2 **Is access to AI systems restricted using multi-factor authentication and role-based access control?**

- ☐ Yes ☐ No ☐ Other (explain): __________

7.3 **Is the incident response plan updated to address AI-specific cybersecurity risks?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 8: Regulatory Compliance

8.1 **Are AI activities reviewed to ensure compliance with Appendix A to Part 748?**

- ☐ Yes ☐ No ☐ Other (explain): __________

8.2 **Are AI applications included in compliance audits?**

- ☐ Yes ☐ No ☐ Other (explain): __________

8.3 **Does the board receive regular reports on AI compliance, including risk management and regulatory adherence?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 9: Continuous Improvement and Training

9.1 **Are staff members trained on AI compliance requirements, security, and ethical considerations?**

- ☐ Yes ☐ No ☐ Other (explain): __________

9.2 **Does the organization document lessons learned from AI incidents or audits for continuous improvement?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Section 10: KPIs and Reporting

10.1 **Are key performance indicators (KPIs) established for monitoring AI compliance and effectiveness?**

- ☐ Yes ☐ No ☐ Other (explain): __________

10.2 **Are standardized reports generated to track AI compliance, incidents, and model performance?**

- ☐ Yes ☐ No ☐ Other (explain): __________

10.3 **How frequently is AI compliance status reported to the board?**

- Answer: __________

Section 11: Audit and Regulatory Adherence

11.1 **Are independent audits conducted to assess AI systems' compliance and risk management?**

- ☐ Yes ☐ No ☐ Other (explain): __________

11.2 **Are audit findings documented, and are corrective actions tracked?**

- ☐ Yes ☐ No ☐ Other (explain): __________

11.3 **Is there a feedback loop from audit results to continuously refine AI practices?**

- ☐ Yes ☐ No ☐ Other (explain): __________

Answers

Monday, October 28, 2024 8:14 AM

Section 1: AI Usage Policy and Scope

Positive Responses:

- "Yes, we have a comprehensive, documented AI usage policy outlining the acceptable uses of AI, specifying prohibited applications, and the risks involved."
- "Our policy explicitly defines the limitations on AI applications and is reviewed annually to ensure alignment with regulatory requirements and evolving technology."
- "We conduct an annual inventory of all AI tools used across departments, ensuring all are registered and authorized."

Negative Responses:

- "No, we currently lack a documented AI usage policy, though we are working to establish one."
- "Our AI usage is loosely defined, with no formalized limitations or prohibited applications documented."
- "We have not conducted an AI inventory recently, so we may not have a complete list of AI tools currently in use."

Section 2: AI Risk Assessment

Positive Responses:

- "Yes, our risk assessment process specifically includes identifying and documenting risks associated with AI, such as data privacy concerns, cybersecurity risks, and model bias."
- "Risks are ranked and documented with detailed mitigation plans, and the assessment is reviewed every six months."
- "We have a formal process for updating risk analysis when new AI tools are implemented or when risks evolve."

Negative Responses:

- "No, we have not conducted a formal risk assessment specific to AI use, although we are in the initial planning stages."
- "Risks associated with AI tools are documented informally, without structured ranking or mitigation plans."
- "There is no established process for updating AI risk assessments; any changes are made on an as-needed basis."

Section 3: Governance and Oversight

Positive Responses:

- "Yes, we have clearly defined roles and responsibilities for AI governance, including a dedicated AI Oversight Committee that meets quarterly."
- "The board and key stakeholders are informed regularly about AI use, and an AI Oversight Committee is established to review AI activities."
- "Our committee meets biannually to discuss AI risk, model performance, and compliance updates."

Negative Responses:

- "No formal roles or responsibilities have been defined for AI governance; oversight is managed by individual departments."
- "We lack an AI Oversight Committee, and AI-related issues are discussed on an ad-hoc basis with minimal documentation."
- "Committee meetings are irregular, and there's no consistent reporting on AI risk or compliance."

Section 4: Data Privacy and Protection

Positive Responses:

- "Yes, we enforce access controls that limit sensitive data access to authorized personnel only, with regular audits."
- "Data used in AI models is anonymized and masked to minimize the risk of exposure of personally identifiable information (PII)."
- "Our data protection standards are monitored continuously with automated tools to detect and respond to deviations."

Negative Responses:

- "Access controls for AI data are limited, and sensitive information may be accessible to unauthorized staff."
- "Anonymization and masking are applied inconsistently, increasing the risk of exposure for sensitive data."
- "We do not monitor data protection standards continuously, and issues are identified only during periodic audits."

Section 5: Model Transparency and Explainability

Positive Responses:

- "Yes, all AI models are developed with transparency in mind, ensuring that decision-making processes are explainable to stakeholders."
- "Detailed documentation is maintained on model logic, parameters, and training datasets, accessible to authorized personnel."
- "Members are informed through clear, concise communications about how AI decisions may impact them."

Negative Responses:

- "Models are designed for performance rather than transparency, making explanations of decision-making processes difficult."
- "Documentation on model logic and parameters is incomplete or inaccessible to non-technical stakeholders."
- "No formal process exists for communicating the impact of AI-driven decisions to members."

Section 6: Model Validation and Monitoring

Positive Responses:

- "Yes, we conduct thorough pre-deployment validation, including accuracy, bias, and predictive performance tests, on all models."
- "Continuous monitoring systems are in place to track model performance, detect drift, and identify biases in real time."
- "Models are revalidated every six months to ensure ongoing compliance, accuracy, and fairness."

Negative Responses:

- "Pre-deployment testing for models is minimal, with little emphasis on bias or predictive validity."
- "Continuous monitoring of models is not established, leading to delays in detecting performance degradation."
- "Models are only revalidated if specific issues arise; there is no routine schedule for revalidation."

Section 7: Cybersecurity for AI Systems

Positive Responses:

- "Yes, we conduct regular penetration testing and vulnerability assessments specific to AI infrastructure."
- "Multi-factor authentication and role-based access control are enforced across all AI systems to prevent unauthorized access."
- "Our incident response plan includes protocols for AI-specific risks, such as adversarial attacks and data poisoning."

Negative Responses:

- "No AI-specific vulnerability assessments are conducted, and standard cybersecurity measures are applied."
- "Access controls are minimal, and multi-factor authentication is not enforced for AI system access."
- "Our incident response plan lacks provisions for AI-related risks, which would delay response to AI-specific incidents."

Section 8: Regulatory Compliance

Positive Responses:

- "Yes, our AI tools are reviewed to ensure they comply with Appendix A to Part 748, with a focus on confidentiality and integrity of member information."
- "Compliance audits for AI use are scheduled annually, and the board receives a detailed report on AI risk management."
- "The board is updated semi-annually on AI risk, including compliance, regulatory status, and any relevant changes."

Negative Responses:

- "No formal process exists to assess AI compliance with Appendix A to Part 748; compliance is inferred from general IT practices."
- "AI compliance is not included in audits, and there is no formal report on AI risk management presented to the board."
- "AI risk and compliance updates are only provided upon request, with no regular reporting schedule in place."

Section 9: Continuous Improvement and Training

Positive Responses:

- "Yes, staff across departments are regularly trained on AI compliance, data privacy, and ethical use of AI tools."
- "Documentation is maintained on lessons learned from AI-related incidents and audits, and practices are updated as a result."
- "We foster a culture of responsible AI use through awareness programs and training on responsible AI practices."

Negative Responses:

- "No specific training is provided for AI compliance; employees learn on an as-needed basis."
- "Documentation of lessons learned from AI audits or incidents is inconsistent, and improvements are not systematically applied."
- "There is limited emphasis on responsible AI use, and awareness programs are not in place."

Section 10: KPIs and Reporting

Positive Responses:

- "Yes, key performance indicators are defined to track the effectiveness of AI compliance, such as model accuracy and bias rates."
- "Standardized reports are generated quarterly, summarizing AI compliance, risk, and model performance for management."
- "The board receives regular updates on KPIs related to AI compliance and performance at least semi-annually."

Negative Responses:

- "No KPIs are defined specifically for AI compliance; tracking is limited to general performance metrics."
- "Reports on AI compliance are generated inconsistently and lack standardized formats, making trends hard to track."
- "The board is rarely updated on AI performance and compliance metrics, resulting in limited oversight."

Section 11: Audit and Regulatory Adherence

Positive Responses:

- "Yes, independent audits of AI use are conducted annually to assess compliance with regulatory requirements and risk management practices."
- "Audit findings are documented, and corrective actions are tracked and completed within set deadlines."
- "A feedback loop is established from audit results, with findings used to refine AI governance and compliance practices."

Negative Responses:

- "No independent audits have been conducted specific to AI; compliance is assumed from general IT audits."
- "Audit findings for AI are inconsistently documented, and corrective actions are rarely followed up on systematically."
- "There is no structured process to use audit results for continuous improvement; findings are noted but not formally acted upon."

Compliance

Monday, October 28, 2024 8:15 AM

1. Develop and Implement Clear Policies

- **Establish an AI Usage Policy**: Create a documented AI policy specifying acceptable AI applications, prohibited uses, and compliance requirements. Outline the roles and responsibilities for AI governance, including data privacy, cybersecurity, model transparency, and incident response requirements.
- **Regularly Update Policies**: Set an annual review schedule for AI-related policies to address emerging risks, evolving technologies, and regulatory changes.

2. Conduct Thorough Risk Assessments

- **Perform Initial Risk Assessments**: Evaluate each AI tool's potential risks, including data privacy concerns, model bias, cybersecurity vulnerabilities, and impacts on decision-making processes. Document these risks and rank them based on likelihood and impact.
- **Mitigate Identified Risks**: Develop risk mitigation strategies, such as implementing data anonymization, strengthening access controls, and enhancing model transparency.
- **Reassess Periodically**: Schedule periodic risk assessments, particularly when deploying new AI tools or updating existing models, to ensure any emerging risks are addressed.

3. Ensure Strong Data Privacy and Protection

- **Apply Data Access Controls**: Limit access to data used in AI models to authorized personnel only, using role-based access and multi-factor authentication (MFA).
- **Enforce Data Anonymization and Masking**: Use anonymization, masking, or encryption for personally identifiable information (PII) in datasets to protect member privacy.
- **Monitor Compliance with Data Protection Standards**: Implement automated monitoring tools that ensure continuous compliance with data privacy regulations.

4. Enhance Model Transparency and Explainability

- **Develop Explainable AI Models**: Design models that allow stakeholders to understand and interpret AI decisions, ensuring decisions can be communicated clearly to members.
- **Document Model Logic and Parameters**: Keep comprehensive documentation for each AI model, including training data sources, parameters, and decision-making logic.
- **Communicate AI Decisions to Members**: Clearly communicate how AI decisions affect members, especially in areas impacting financial products, credit scores, and loan approvals.

5. Implement Robust Model Validation and Monitoring

- **Validate Models Before Deployment**: Conduct bias, accuracy, and predictive validity tests on each model before deploying it in a live environment.
- **Monitor for Model Drift and Bias**: Establish a continuous monitoring process to detect and address model drift, bias, or deviations from expected performance.
- **Schedule Regular Revalidation**: Set revalidation intervals (e.g., quarterly or semi-annually) to ensure AI models remain compliant and effective over time.

6. Apply Cybersecurity Controls Specific to AI

- **Conduct Vulnerability Assessments**: Regularly test AI tools and infrastructure for vulnerabilities, including threats unique to AI, such as adversarial attacks and data poisoning.
- **Use Access Controls and MFA for AI Systems**: Limit access to AI models and systems with strong access controls and multi-factor authentication, especially for models containing sensitive data.
- **Update Incident Response Plans for AI**: Include AI-related scenarios in the incident response plan to ensure rapid response to AI-related breaches or security threats.

7. Establish Ongoing Training and Awareness Programs

- **Train Staff on AI Compliance**: Provide ongoing training for staff on AI-related risks, security practices, compliance requirements, and ethical use of AI tools.
- **Promote AI Awareness**: Create awareness programs to foster a responsible AI culture across the organization, reinforcing regulatory compliance and ethical considerations.

8. Implement Continuous Monitoring and KPI Tracking

- **Define Key Performance Indicators (KPIs)**: Establish KPIs to measure AI compliance effectiveness, such as the number of models revalidated, accuracy rates, bias levels, and incident frequency.
- **Automate Monitoring and Alerts**: Use monitoring tools to detect compliance deviations in real-time, sending alerts to relevant personnel if issues arise.
- **Review KPIs Regularly**: Set a regular schedule to review KPIs, assess trends, and use findings to improve compliance processes.

9. Conduct Regular Audits and Reviews

- **Schedule Independent AI Audits**: Arrange for third-party audits to review AI systems and processes for compliance, data security, and model integrity. This helps ensure objectivity and regulatory alignment.
- **Document Findings and Track Remediation**: Record audit findings and establish corrective action plans with deadlines. Assign responsibilities for addressing each finding and follow up on remediation.
- **Create a Compliance Feedback Loop**: Use audit and monitoring results to refine policies, risk assessments, and AI practices continuously. Adjust strategies based on audit outcomes and regulatory updates.

10. Ensure Governance and Board Oversight

- **Create an AI Oversight Committee**: Establish a committee to oversee AI compliance, risk management, and policy updates. This committee should include board members, compliance officers, IT security, and relevant stakeholders.
- **Provide Regular Compliance Updates to the Board**: Submit detailed AI compliance and risk management reports to the board at least semi-annually, including metrics, incidents, and compliance status with 12 CFR Part 748.
- **Integrate AI Governance into Broader Compliance Frameworks**: Ensure that AI compliance activities are incorporated into broader organizational compliance frameworks and audits to maintain consistent oversight.

1. Data Privacy and Protection

- **748.0(b) – Security Program Requirement**: Credit unions must implement a security program to protect member information, which includes appropriate safeguards for data privacy.
- **Appendix A to Part 748, Section II(A) – Security Program Objectives**: Emphasizes data confidentiality and integrity, especially in the context of AI data handling.
- **Appendix A to Part 748, Section III(C) – Information Safeguards**: Outlines specific controls for protecting member information, such as access restrictions and the safeguarding of information systems.

2. Compliance with Regulatory Requirements

- **748.1 – Filing Requirements for Security Program**: Requires credit unions to certify compliance with security program guidelines, including safeguarding sensitive information that may be handled by AI tools.
- **Appendix A, Section III(A) – Development and Implementation of an Information Security Program**: Mandates that credit unions establish an information security program addressing specific regulatory and privacy concerns applicable to AI usage.
- **Appendix A, Section III(D) – Overseeing Service Provider Arrangements**: Requires due diligence on third-party service providers, including AI vendors, ensuring they meet regulatory standards.

3. AI Model Transparency and Explainability

- **Appendix A, Section III(B) – Assessing Risk**: Requires identifying and controlling risks to member information, which includes the need for transparent, explainable AI systems where models impact member decisions.
- **Appendix B to Part 748, Section II – Governance and Management Oversight**: Emphasizes accountability and transparency, which are essential in managing AI models, explaining decision logic, and reporting to stakeholders.

4. Model Bias and Fairness

- **Appendix A, Section II(A) – Security Program Objectives**: Focuses on the integrity of member information, which includes ensuring unbiased and fair treatment in decisions affecting members.
- **Appendix B, Section II(B) – Protecting Member Information**: Calls for programs to protect information equitably and reliably, supporting the need to review AI models for biases that could impact members' access to services.

5. Cybersecurity and Access Control

- **Appendix A, Section III(C)(3) – Information Safeguards**: Specifies access control measures for systems processing member information, aligning with AI model protections.
- **748.0(b) – Security Program Requirement**: Requires credit unions to implement cybersecurity measures, applicable to AI systems processing member data.
- **Appendix A, Section III(C)(2) – Security Controls**: Includes guidance on access controls, encryption, and cybersecurity safeguards for systems with sensitive data, relevant to AI infrastructure.

6. Data Handling and Retention Policies

- **Appendix A, Section III(C)(4) – Information Disposal**: Mandates secure disposal of member information, which extends to data retained or used by AI vendors.
- **748.0(b) – Security Program Requirement**: Emphasizes the need for data retention policies that ensure member data is appropriately handled and disposed of when no longer necessary.

7. Audit and Monitoring Capabilities

- **Appendix A, Section III(C)(1) – Internal Controls, Testing, and Monitoring**: Outlines the need for internal monitoring and testing of security controls, relevant to tracking AI model usage and access.
- **Appendix B, Section II(C) – Security Testing and Monitoring**: Recommends frequent auditing and monitoring of systems that access or process member information, including third-party AI systems.

8. Vendor's Internal Compliance and Training

- **Appendix A, Section III(D) – Overseeing Service Provider Arrangements**: Requires credit unions to ensure that service providers have robust training programs and policies for handling member data securely.
- **748.1 – Filing Requirements**: Calls for certification of compliance, indirectly requiring vendors to be educated and trained on compliance standards, especially those handling sensitive data.

9. Incident Response and Business Continuity

- **Appendix B, Section III(B) – Incident Response Program**: Specifies requirements for an incident response program to address security breaches, relevant to vendors processing sensitive information.
- **Appendix A, Section III(E) – Implementing the Security Program**: Requires procedures for responding to security incidents, breaches, and other disruptions, which would apply to third-party vendors' AI systems.

10. Ethical Use and AI Governance

- **Appendix A, Section II – Objectives**: Calls for programs that protect the integrity of member information, indirectly supporting ethical use by avoiding biases and maintaining data security.
- **Appendix B, Section II(B) – Protecting Member Information**: Reinforces the importance of ethical practices in handling member information, which applies to AI vendor governance and bias prevention.

11. Third-Party and Subcontractor Compliance

- **Appendix A, Section III(D) – Overseeing Service Provider Arrangements**: Requires credit unions to conduct due diligence on third-party providers, ensuring their compliance with security and data protection standards.
- **Appendix B, Section II(D) – Due Diligence in Selecting Service Providers**: Stresses the need for thorough reviews and compliance checks for vendors handling sensitive data.

12. Service-Level Agreements (SLAs) and Reporting

- **Appendix A, Section III(D) – Overseeing Service Provider Arrangements**: Directs credit unions to establish SLAs with vendors that clearly outline compliance responsibilities, data security expectations, and reporting requirements.
- **Appendix B, Section II(D) – Establishing and Monitoring Service Level**

Agreements: Recommends SLAs with compliance terms and regular reporting to ensure that vendors meet the credit union's data protection standards.

13. Continuous Improvement and Updates

- **Appendix A, Section III(C)(1) – Internal Controls and Continuous Monitoring**: Requires credit unions to have a feedback loop for continuously improving security programs, applicable to updates in AI systems or vendor practices.
- **Appendix A, Section III(E) – Implementing the Security Program**: Stresses the need for updates and improvements to the security program as new risks emerge, aligning with the need for AI system reviews and updates.

Third Party

Monday, October 28, 2024 8:15 AM

1. AI Model Validation and Bias Audits

- **Purpose**: Evaluate AI models for fairness, accuracy, and potential bias, ensuring models do not unintentionally disadvantage any group.
- **Scope**: Include an assessment of training data quality, model logic, decision-making processes, and outcome consistency. Validate models for regulatory compliance, ethical considerations, and industry standards.
- **Frequency**: Annually or upon significant model changes.
- **Outcome**: An independent report identifying model biases, transparency issues, and areas for improvement with recommendations for mitigation.

2. Data Privacy and Protection Compliance Assessment

- **Purpose**: Ensure the credit union's data management practices comply with data privacy regulations, focusing on safeguarding member data used in AI systems.
- **Scope**: Assess data collection, access controls, anonymization, encryption, and data sharing protocols. Evaluate adherence to privacy regulations such as GLBA and, where applicable, the GDPR or CCPA.
- **Frequency**: Annually, with periodic reviews if new AI applications or data sources are introduced.
- **Outcome**: A report on data privacy controls, compliance gaps, and suggestions for strengthening data protection practices.

3. Cybersecurity Penetration Testing and Vulnerability Assessment

- **Purpose**: Test the security resilience of AI systems and supporting IT infrastructure against cyber threats.
- **Scope**: Perform penetration testing on AI systems, assess for vulnerabilities in data pipelines, models, and storage, and evaluate protections against data poisoning, adversarial attacks, and unauthorized access.
- **Frequency**: Biannually or after major system updates.
- **Outcome**: Identification of security vulnerabilities, risk assessment, and prioritized remediation recommendations.

4. IT and System Control Review

- **Purpose**: Review IT systems and controls to ensure they support AI applications securely and maintain proper access and data integrity controls.
- **Scope**: Assess role-based access controls, multi-factor authentication, logging, and monitoring specific to AI-related infrastructure. Confirm that access to sensitive data and models is restricted based on job roles and subject to regular review.
- **Frequency**: Annually, with follow-up reviews after significant infrastructure or policy changes.
- **Outcome**: A detailed report on control effectiveness, identified weaknesses, and recommendations for enhancing access management and system security.

5. Independent Compliance Audit of AI Practices

- **Purpose**: Validate the credit union's AI activities for compliance with Appendix A to Part 748, focusing on confidentiality, integrity, and security.
- **Scope**: Include a thorough examination of AI governance, risk management practices, model transparency, and documentation. Assess alignment with internal policies, regulatory requirements, and industry best practices.
- **Frequency**: Annually or upon substantial changes in AI tools or compliance policies.
- **Outcome**: An independent review that outlines compliance status, identifies gaps, and offers corrective actions to align with regulatory requirements.

6. Third-Party Vendor Security Review

- **Purpose**: Assess the compliance and security practices of third-party vendors, particularly those involved in data processing, model hosting, or AI service provision.
- **Scope**: Review vendor compliance with credit union's data privacy and security standards, focusing on data handling, contractual obligations, incident response capabilities, and security controls.
- **Frequency**: Annually or upon new vendor engagement.
- **Outcome**: A report on vendor security and compliance, along with risk ratings and recommendations for mitigating third-party risks.

7. Incident Response Readiness and Post-Incident Review

- **Purpose**: Test and validate the credit union's incident response plan for AI and data privacy-related incidents.
- **Scope**: Include simulated incidents or tabletop exercises to evaluate readiness for responding to AI-specific breaches or security incidents, such as unauthorized data access or data breaches involving AI systems.
- **Frequency**: Annually, with additional reviews following any actual incident.
- **Outcome**: Recommendations for strengthening response capabilities, documentation improvements, and refinement of incident handling protocols.

8. Internal Audit Review of Compliance with AI and Data Management Policies

- **Purpose**: Ensure internal audit processes cover compliance with AI-related policies, data handling, cybersecurity, and access control procedures.
- **Scope**: Review the effectiveness of internal audits in evaluating AI policy adherence, data protection practices, and control effectiveness across departments.
- **Frequency**: Quarterly or biannually, depending on internal audit cycles.
- **Outcome**: A review confirming the adequacy of internal audits in ensuring compliance with AI and data management policies, along with areas for process improvement.

9. Ethics and Responsible AI Use Review

- **Purpose**: Ensure AI applications align with ethical standards, emphasizing responsible AI use and minimizing unintended consequences.
- **Scope**: Evaluate AI models for ethical risks, such as potential biases or unintended harm.

Review documentation for transparency, accountability, and fairness practices.

- **Frequency**: Annually or when implementing new AI models.
- **Outcome**: A report on ethical considerations, with recommendations for addressing any identified biases or ethical risks.

10. Board and Executive Oversight Review

- **Purpose**: Assess the board's involvement in overseeing AI compliance, policy approvals, risk management, and strategy.
- **Scope**: Review board meeting minutes, reports presented to the board, and board discussions related to AI compliance and risk. Evaluate the adequacy of board reporting and executive understanding of AI compliance requirements.
- **Frequency**: Annually.
- **Outcome**: A review highlighting areas where board oversight can be strengthened, ensuring executive and board alignment on AI compliance and risk management.

Questions for Vendors

Monday, October 28, 2024 8:15 AM

1. Data Privacy and Protection

- **How do you ensure that member data remains private and secure in your AI models and systems?**
- **What data anonymization, encryption, or pseudonymization methods do you employ to protect sensitive data?**
- **Can you provide a list of data access controls and safeguards you have in place to prevent unauthorized access to member data?**
- **Do you have mechanisms for securely sharing data with us, and do you comply with data protection regulations such as GDPR or CCPA where applicable?**
- **Can you provide a data flow diagram that details how data is processed, stored, and transmitted across your systems?**

2. Compliance with Regulatory Requirements

- **How do you ensure your AI tools and processes align with the requirements of 12 CFR Part 748 and other relevant financial regulations?**
- **Do you conduct regular compliance audits and risk assessments, and can you share the results or provide compliance certifications?**
- **How do you manage compliance with data privacy laws across different regions, especially if data is stored or processed outside the United States?**
- **Are your services independently audited for compliance with industry standards (e.g., SOC 2, ISO 27001)?**

3. AI Model Transparency and Explainability

- **How do you ensure transparency in the decision-making processes of your AI models, especially in areas like lending or credit risk assessments?**
- **Can you provide documentation explaining how your models work, including the logic, algorithms, and data sources used?**
- **How do you address interpretability issues to ensure that our team can understand, monitor, and audit the model's decisions?**
- **Are explanations provided for AI-driven decisions that can be shared with our members if needed?**

4. Model Bias and Fairness

- **What steps do you take to prevent bias in your AI models, and how do you ensure fairness in outcomes for all member demographics?**
- **Do you conduct regular bias and fairness audits, and can you provide documentation on these assessments?**
- **How do you handle and mitigate unintended biases if they are discovered within your models?**
- **Can you share case studies or examples of how your AI models have been tested for**

fairness and ethical compliance?

5. Cybersecurity and Access Control

- **What cybersecurity measures are in place to protect your AI systems, data, and member information from unauthorized access and attacks?**
- **Do you conduct regular penetration testing and vulnerability assessments, and how often are they performed?**
- **Can you provide details about your access control policies, including role-based access and multi-factor authentication, for individuals who interact with or manage our data?**
- **How are security incidents handled, and do you have an incident response plan specific to AI-related breaches or risks?**

6. Data Handling and Retention Policies

- **What is your data retention policy, and how long do you retain our members' data?**
- **Do you have a data deletion or erasure policy that aligns with regulatory standards, and can data be securely deleted upon request?**
- **How is data backed up, and what controls are in place to protect backup copies from unauthorized access?**
- **Can you restrict data access only to specific authorized users within your organization?**

7. Audit and Monitoring Capabilities

- **Can we audit your systems and processes to verify compliance with our data protection and security requirements?**
- **Do you have tools in place for real-time monitoring of data usage, and can we receive alerts or notifications for any unusual activity involving our data?**
- **How frequently do you conduct internal audits, and are these available for review by our compliance team?**
- **Can you provide detailed logs of data access and changes made to the AI model or data pipelines?**

8. Vendor’s Internal Compliance and Training

- **What kind of compliance training do your employees receive, especially those who handle sensitive financial data or develop AI models?**
- **How do you ensure that your team is up-to-date on industry best practices, regulatory changes, and data privacy laws?**
- **Are your employees subject to background checks or other vetting processes before accessing our data?**
- **How is adherence to compliance policies enforced and monitored within your organization?**

9. Incident Response and Business Continuity

- **What is your incident response process in the event of a data breach or AI model failure?**

- **Can you detail your business continuity plan and how it ensures uninterrupted service and protection of our data in the event of an incident?**
- **How will you communicate with us in the event of a security incident, and what is the expected response time?**
- **Can you provide examples of previous incidents and the corrective actions taken to prevent recurrence?**

10. Ethical Use and AI Governance

- **Do you have a documented policy on ethical AI use, and can you provide details?**
- **How does your organization handle ethical considerations in AI development, including fairness, accountability, and transparency?**
- **Can you provide case studies or examples demonstrating your commitment to responsible and ethical AI practices?**
- **How is governance structured around AI practices, and who is responsible for ensuring compliance with ethical guidelines?**

11. Third-Party and Subcontractor Compliance

- **Do you use any third-party vendors or subcontractors to support your AI systems or data processing, and are they subject to the same compliance standards?**
- **Can you provide documentation verifying that third-party vendors meet our data protection and security requirements?**
- **How do you monitor third-party compliance, and are their security practices reviewed regularly?**
- **What is your policy for informing us if a third-party vendor experiences a data breach involving our information?**

12. Service-Level Agreements (SLAs) and Reporting

- **Do your SLAs include specific clauses on data privacy, security, and compliance with 12 CFR Part 748?**
- **How often will you report on compliance status, audit findings, and any issues impacting our data or AI models?**
- **Are there penalties or remediation processes outlined in the SLA if there is a breach of data privacy or security standards?**
- **Can we request customized reports or metrics to monitor compliance with our standards and requirements?**

13. Continuous Improvement and Updates

- **How do you stay current with evolving AI regulations and industry best practices?**
- **Do you have a formal process to update and improve your AI models and processes in response to new regulatory guidelines or discovered vulnerabilities?**
- **Will we be notified of any changes to the model's underlying algorithms or data processing practices that could impact compliance?**
- **How do you incorporate feedback from clients like us to improve compliance and risk**

management processes?

Lending compliance

Monday, October 28, 2024 8:24 AM

1. Data Protection and Security (12 CFR Part 748)

- **748.0(b) – Security Program Requirement**: Requires credit unions to implement a comprehensive security program to protect member information, which applies to data used in AI-driven credit decisioning.
- **Appendix A to Part 748, Section II(A) – Security Program Objectives**: Mandates that credit unions develop safeguards to ensure the confidentiality, integrity, and security of sensitive information, including data processed by AI in credit decisions.
- **Appendix A, Section III(C) – Information Safeguards**: Specifies controls for protecting member data used in automated decision-making, such as encryption, access restrictions, and data masking, to prevent unauthorized access and misuse.

2. Fair Lending and Equal Credit Opportunity (12 CFR Part 1002, Regulation B)

- **1002.4 – Prohibited Basis**: Under the Equal Credit Opportunity Act (ECOA), it is unlawful to discriminate on the basis of race, color, religion, national origin, sex, marital status, age, or income derived from public assistance. AI models used in credit decisions must be designed and validated to ensure they do not produce discriminatory outcomes based on these factors.
- **1002.6 – Rules Concerning Evaluation of Applications**: Prohibits credit decisions based on factors that are statistically unsupported or discriminatory. AI models used in credit decisions must use valid and legally compliant data inputs and methodologies.
- **1002.9 – Notifications**: Requires credit unions to notify applicants of action taken on credit applications within specified time frames, including adverse actions. If AI is used in decision-making, the credit union must provide an adverse action notice that includes the specific reasons for the denial, which can require explainable AI models.
- **1002.14 – Rules on Providing Appraisal Reports**: If an AI model is used to assess property value for credit decisions, the credit union must provide applicants with copies of appraisal reports and valuations, ensuring transparency.

3. Truth in Lending Act (12 CFR Part 1026, Regulation Z)

- **1026.4 – Finance Charge**: Defines finance charges and requires accurate disclosure of all costs associated with a loan. AI-driven credit decision tools must calculate finance charges in compliance with these regulations.
- **1026.17 – General Disclosure Requirements**: Requires clear and accurate disclosures in credit transactions. If AI is used to determine loan terms or pricing, the resulting disclosures must comply with these requirements.
- **1026.18 – Content of Disclosures**: Mandates detailed disclosures for open-end and closed-end credit, which AI systems must generate accurately to ensure members receive all required information regarding rates, fees, and terms.
- **1026.22 – Determination of Annual Percentage Rate**: AI models used to assess credit risk or determine loan pricing must comply with APR calculation guidelines, ensuring accuracy and consistency.

4. Consumer Privacy and Data Usage (Gramm-Leach-Bliley Act, 12 CFR Part 1016)

- **1016.10 – Limits on Disclosure of Nonpublic Personal Information**: Requires credit unions to limit the disclosure of member information to third parties. AI-driven systems must have safeguards to protect member privacy and ensure data is not shared in violation of these rules.
- **1016.13 – Opt-Out Rights**: Grants consumers the right to opt out of certain information sharing. AI systems must respect these opt-out preferences and avoid using data in ways that contravene privacy rules.
- **1016.12 – Notice and Disclosure Requirements**: AI systems should support transparency by helping credit unions meet notice and disclosure requirements for information collection and usage.

5. Transparency and Explainability in Automated Credit Decisions (Additional Guidance)

- **Appendix A to Part 748, Section III(C)(1) – Internal Controls, Testing, and Monitoring**: Recommends continuous monitoring and testing of automated decision-making models, such as AI, to ensure they operate accurately, equitably, and consistently with credit union policies.
- **1002.9(b)(2) – Adverse Action Notice Specificity (Regulation B)**: When AI denies credit, the adverse action notice must list specific factors contributing to the decision. AI models must be interpretable to ensure compliance with this notice requirement.
- **1002.6(b)(1) – Use of Empirically Derived, Demonstrably and Statistically Sound Credit Scoring Systems (Regulation B)**: AI-based credit scoring models must use empirically derived, statistically sound methodologies. This mandates testing for accuracy, fairness, and predictive reliability.

6. Vendor and Service Provider Oversight (12 CFR Part 748)

- **Appendix A, Section III(D) – Overseeing Service Provider Arrangements**: Requires due diligence for third-party AI vendors, ensuring they meet compliance standards for data privacy, model transparency, and non-discriminatory credit decisioning.
- **Appendix B, Section II(D) – Due Diligence in Selecting Service Providers**: Credit unions are responsible for ensuring that AI service providers adhere to all relevant regulations and best practices in fair lending and data protection.

7. Incident Response and Model Monitoring (12 CFR Part 748 and Appendices)

- **Appendix A, Section III(E) – Implementing the Security Program**: Requires procedures for monitoring and mitigating risks in automated systems, including real-time monitoring and corrective actions for AI models used in credit decisions.
- **Appendix B, Section III(B) – Incident Response Program**: Specifies the need for an incident response program, particularly if an AI model malfunctions, produces inaccurate credit assessments, or experiences a data breach.

Notes

Wednesday, March 26, 2025 3:05 PM