AI Power vs. Protection Gap – IT Audit & Compliance Checklist (2026)

Mapped to NIST AI Risk Management Framework (NIST 600-1)

Use this checklist as a practical tool to identify risks, assess current maturity, and take action to close the gap between AI capabilities and governance in your organization.

How to Use This Checklist

- Start with **Visibility & Inventory** — you can't manage what you don't know
- Focus first on **high-risk AI use cases**
- Tackle gaps incrementally (don't try to fix everything at once)
- Integrate into existing **IT audit and compliance processes**

AI Power vs. Protection Gap – IT Audit & Compliance CHECKLIST

1. AI Visibility & Inventory

Goal: Know where and how AI is being used

- Maintain a centralized inventory of all AI tools and systems in use
- Identify both approved and "shadow AI" usage across departments
- Document business purpose for each AI use case
- Record system owners and accountable stakeholders
- Track whether AI tools are internally developed or third-party

NIST AI RMF Alignment:

- MAP 1.1: Identify AI systems and their context
- MAP 2.1: Document system purpose and stakeholders

Key NIST AI RMF Checklist Coverage:

- AI inventory
- Business purpose documentation
- Ownership identification
- Shadow AI discovery

2. Risk Classification

Goal: Prioritize what matters most

- Classify AI use cases (Low / Medium / High risk)
- Define clear criteria for each risk category
- Identify high-risk use cases (e.g., financial decisions, HR, legal, customer impact)
- Perform formal risk assessments for high-risk AI systems
- Reassess risk periodically or when use cases change

NIST AI RMF Alignment:

- MAP 3.1: Identify risks and impacts
- MEASURE 1.1: Assess risk levels

Key NIST AI RMF Checklist Coverage:

- Risk tiering (Low/Medium/High)
- Formal risk assessments
- Periodic reassessment

3. Data Protection & Privacy

Goal: Prevent sensitive data exposure

- Identify data types used in AI (PII, PHI, financial, confidential)
- Restrict sensitive data from public AI tools
- Implement data masking or anonymization where applicable
- Apply Data Loss Prevention (DLP) controls
- Verify data storage locations and cross-border data transfer risks

- Ensure compliance with applicable privacy regulations

NIST AI RMF Alignment:

- GOVERN 1.3: Data governance policies
- MANAGE 2.1: Risk mitigation controls

Key NIST AI RMF Checklist Coverage:

- Data classification
- DLP controls
- Data masking/anonymization
- Regulatory compliance

4. Model Governance & Accountability

Goal: Ensure AI decisions are controlled and explainable

- Assign clear ownership for each AI model/system
- Document model purpose, logic, and limitations
- Validate model accuracy and performance regularly
- Assess potential bias and fairness risks
- Ensure explainability for high-impact decisions
- Define escalation procedures for incorrect or harmful outputs

NIST AI RMF Alignment:

- GOVERN 2.2: Accountability structures
- MEASURE 2.1: Model evaluation and validation

Key NIST AI RMF Checklist Coverage:

- Model ownership
- Documentation of logic and limitations
- Bias and fairness assessments
- Explainability requirements

5. Logging, Monitoring & Auditability

Goal: Make AI activities traceable

- Enable logging of AI inputs and outputs
- Track user access and activity
- Maintain audit trails for decision-making processes
- Monitor for unusual or unauthorized AI usage
- Ensure logs are retained per policy and compliance requirements
- Test auditability during internal audits

NIST AI RMF Alignment:

- MEASURE 3.1: Ongoing monitoring
- MANAGE 3.2: Incident detection and response

Key NIST AI RMF Checklist Coverage:

- Input/output logging
- Audit trails
- Usage monitoring
- Log retention

6. Governance Framework & Policies

Goal: Establish clear rules for AI use

- Develop and publish an AI usage policy
- Define acceptable and prohibited use cases
- Establish approval processes for new AI tools
- Align AI governance with existing IT and risk frameworks
- Create an AI oversight committee or governance body (if applicable)
- Review and update policies regularly

NIST AI RMF Alignment:

- GOVERN 1.1: AI governance policies
- GOVERN 1.2: Organizational roles and responsibilities

Key NIST AI RMF Checklist Coverage:

- AI usage policy
- Approval workflows
- Governance structure
- Oversight committees

7. Third-Party & Vendor Risk Management

Goal: Control external AI risks

- Maintain a list of all third-party AI vendors
- Perform vendor risk assessments before onboarding
- Review vendor security certifications and compliance posture
- Understand how vendors store, use, and train on your data
- Ensure contracts include data protection and liability clauses
- Conduct periodic vendor reviews

NIST AI RMF Alignment:

- Vendor risk assessments
- Contractual protections
- Vendor monitoring

Key NIST AI RMF Checklist Coverage:

- Vendor risk assessments
- Contractual protections
- Vendor monitoring

8. Employee Awareness & Training

Goal: Reduce human-driven risk

- Provide training on approved AI tools and usage
- Educate employees on data handling risks with AI
- Share examples of AI misuse and consequences
- Communicate policies clearly and frequently
- Require acknowledgment of AI usage policies

NIST AI RMF Alignment:

- GOVERN 1.4: Workforce training and awareness

Key NIST AI RMF Checklist Coverage:

- AI training programs
- Policy communication
- Employee acknowledgment

9. Testing & Validation

Goal: Ensure AI systems work as intended

- Perform pre-deployment testing of AI systems
- Validate outputs against expected results
- Conduct scenario and edge-case testing
- Test for bias, fairness, and ethical concerns
- Re-test models after significant updates or retraining

NIST AI RMF Alignment:

- MEASURE 2.1: Model testing and validation
- MEASURE 2.2: Bias and performance evaluation

Key NIST AI RMF Checklist Coverage:

- Pre-deployment testing
- Output validation
- Bias/fairness testing
- Regression testing

10. Continuous Monitoring & Improvement

Goal: Keep up with evolving AI risks

- Continuously monitor AI system performance
- Track incidents and near-misses involving AI
- Perform periodic internal audits of AI systems
- Update controls based on new risks and regulations
- Benchmark against industry best practices
- Report AI risks to leadership regularly

NIST AI RMF Alignment:

- MANAGE 1.3: Continuous improvement
- MEASURE 3.1: Continuous monitoring

Key NIST AI RMF Checklist Coverage:

- Ongoing performance monitoring
- Incident tracking
- Periodic audits
- Control enhancements

———-