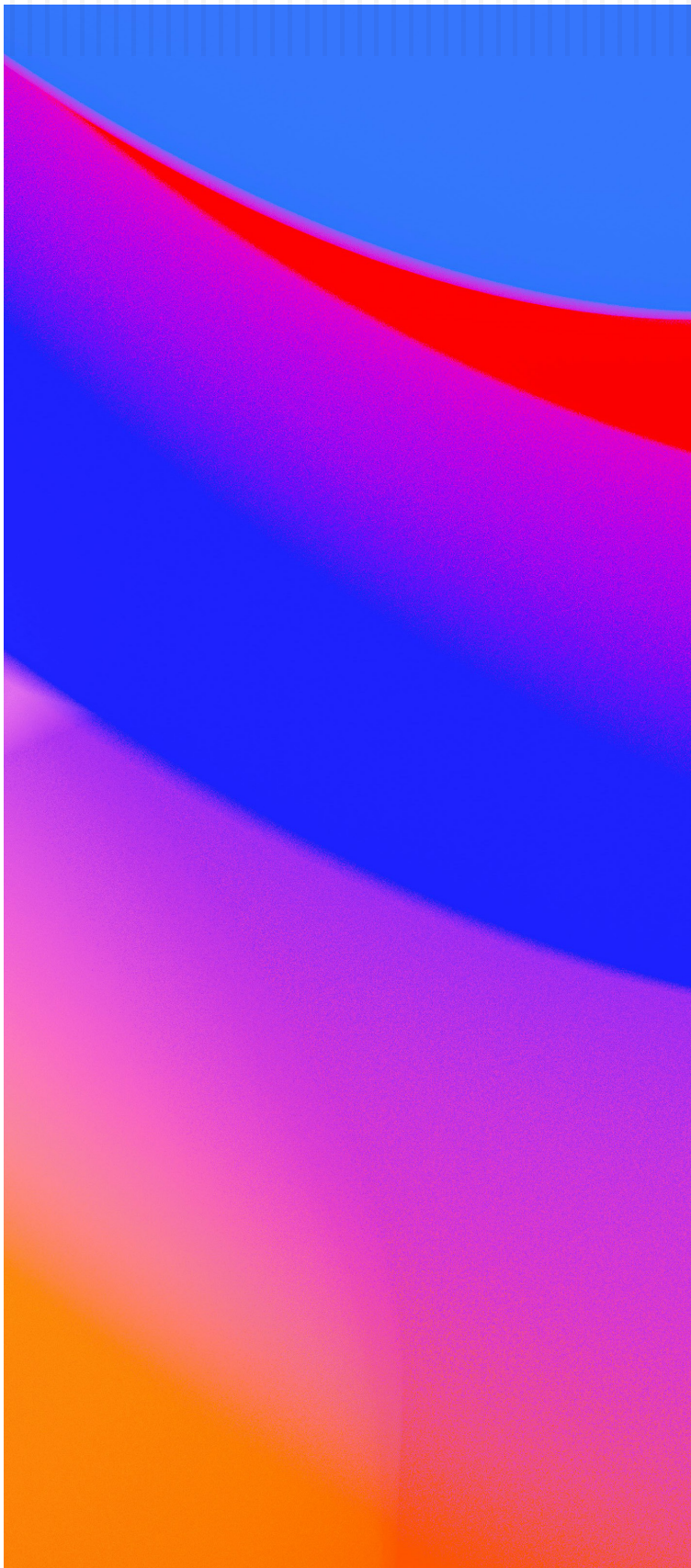
2025 Checklist

Enterprise Checklist for AI Governance, Security, and Privacy

Ensuring proper governance, security, and privacy for enterprise AI systems is critical to mitigate risks, maintain compliance, and build trust. This comprehensive checklist provides organizations with actionable steps to establish robust AI governance, security, and privacy controls across the enterprise.



2025 Checklist Enterprise Checklist for AI Governance, Security, and Privacy

2025 Checklist

Checklist for AI Governance, Security, and Privacy

The following checklist outlines the key steps and considerations for organizations aiming to meet AI compliance:

AI Governance

AI Policy and Strategy

- ❒ Define an enterprise-wide AI governance policy addressing ethical, legal, and operational requirements.
- ❒ Perform a gap analysis to manage AI systems' strategy, technical, regulatory, and operational risks to determine which are "high-risk" or "banned."
- ❒ Align the AI strategy with business objectives, industry-standard frameworks, and regulations.
- ❒ Assign ownership and accountability by designating an AI Governance Committee consisting of Security, Privacy, and Compliance professionals
- ❒ (D&A, Engineering, IT Architecture, Privacy, IT Security)

Regulatory Compliance

- ❒ Identify applicable laws, regulations, and standards (e.g., EU AI Act, GDPR, CCPA, ISO 27001, NIST AI RMF).
- ❒ Conduct a regulatory impact assessment for AI models to understand compliance risks.
- ❒ Regularly monitor and adapt to evolving AI regulations globally.

AI Ethics

- ❒ Establish an AI ethics framework to guide AI systems' design, development, and deployment.
- ❒ Integrate fairness, accountability, and transparency principles into all AI lifecycle stages.
- ❒ Perform bias assessments to ensure equitable outcomes across diverse user groups.

Model Governance

- ❒ Document the lifecycle of all AI models, including versioning, retraining, and retirement plans.
- ❒ Maintain a model inventory with details like model purpose, input data, and ownership.
- ❒ Establish audit trails for decision-making processes to ensure explainability.

AI Risk Management

- ❒ Conduct AI risk assessments to identify and mitigate potential impacts (e.g., bias, privacy violations, cybersecurity threats).
- ❒ Integrate AI risks into the enterprise's overall risk management framework.
- ❒ Monitor the performance and impact of AI models continuously.

AI Security

Data Security

- ❒ Implement encryption for data at rest and in transit to safeguard sensitive information.
- ❒ Utilize access controls to restrict data usage based on roles and responsibilities.
- ❒ Adopt data anonymization techniques to protect personally identifiable information (PII).

Model Security

- ❒ Secure AI models against cyberattacks (e.g., model inversion, evasion, poisoning).
- ❒ Deploy secure model hosting environments with runtime protections.
- ❒ Ensure robust change management for model updates to prevent unauthorized changes.

Incident Response

- ❒ Develop a cybersecurity incident response plan tailored for AI systems.
- ❒ Enable real-time monitoring to detect breaches or unauthorized access to AI systems.
- ❒ Conduct post-incident reviews to strengthen defenses and prevent recurrence.

Data Privacy for AI

Data Collecting and Processing

- ❒ Implement encryption for data at rest and in transit to safeguard sensitive information.
- ❒ Utilize access controls to restrict data usage based on roles and responsibilities.
- ❒ Adopt data anonymization techniques to protect personally identifiable information (PII).

Data Privacy by Design

- ❒ Secure AI models against cyberattacks (e.g., model inversion, evasion, poisoning).
- ❒ Deploy secure model hosting environments with runtime protections.
- ❒ Ensure robust change management for model updates to prevent unauthorized changes.

Data Rights Management

- ❒ Develop a cybersecurity incident response plan tailored for AI systems.
- ❒ Enable real-time monitoring to detect breaches or unauthorized access to AI systems.
- ❒ Conduct post-incident reviews to strengthen defenses and prevent recurrence.

Third Party Privacy

- ❒ Audit third-party datasets and vendors for compliance with privacy policies.
- ❒ Ensure contractual agreements include privacy and security clauses.
- ❒ Conduct regular reviews of external datasets for quality and legal compliance.

AI Operation Oversight

Training and Awareness

- ❒ Provide regular training programs on AI governance, security, and privacy for all employees.
- ❒ Educate stakeholders on the implications of AI risks and compliance requirements.
- ❒ Maintain a culture of ethical AI development through awareness campaigns

Monitor and Evaluate

- ❒ Continuously monitor AI systems for performance drift, bias, or data inaccuracies.
- ❒ Set up real-time dashboards to track key security, compliance, and impact metrics.
- ❒ Conduct periodic audits of AI models to ensure continued alignment with governance policies.

Vendor and Partner Management

- ❒ Vet AI vendors for compliance with privacy and security requirements.
- ❒ Require vendors to disclose information about their model development practices.
- ❒ Ensure partners adhere to shared AI governance frameworks.

Tools and Technologies

Privacy and Security Tools

- ❒ Deploy data discovery and classification tools to identify sensitive data in use. Use privacy-preserving AI tools for secure data sharing and processing.
- ❒ Implement data access monitoring tools to track who is accessing sensitive information.

Governance Platforms

- ❒ Invest in AI model governance platforms to manage the data lifecycle, compliance, and performance.
- ❒ Leverage GRC (Governance, Risk, and Compliance) tools for regulatory alignment.
- ❒ Automate audits with compliance management systems to streamline processes.

Threat Detection and Prevention

- ❒ Integrate AI-powered threat detection tools for cybersecurity.
- ❒ Utilize automated incident response systems for quick containment of breaches.
- ❒ Employ log management and monitoring tools to analyze anomalies in real time.

Continuous Improvement

Adaptation and Collaboration

- ❒ Gather feedback from users and stakeholders to improve AI governance processes.
- ❒ Regularly update AI policies to address emerging risks and regulatory changes.
- ❒ Benchmark performance against industry best practices for governance, security, and privacy.
- ❒ Join industry consortia or working groups to stay ahead of AI trends.
- ❒ Collaborate with regulators and policymakers to shape AI standards.

How BigID Addresses AI Governance, Security And Privacy

BigID is the first and only DSPM to give your GenAI strategy the upgrade it needs to bring you best-in-class results without compromising data security or privacy. BigID enables organizations to better govern, protect, and secure AI data and systems.

With BigID, organizations can:

- **Discover Data:** Automatically find, classify, and tag all structured and unstructured data sources across the cloud and on-prem, with more granularity, context, and accuracy than anyone else.
- **Enforce Policies:** Enforce and manage policies to monitor data location and movement and trigger controls for compliance with AI mandates and regulatory requirements, including GDPR, CCPA, LGPD, and more.
- **Customize Regulatory Policies:** Leverage OOB policies or configure their own based on their unique AI, business, regulatory, security, privacy, and management needs.
- **Conduct Privacy Impact Assessments:** Conduct PIAs quickly using industry-standard templates and create data flow maps from an active inventory to fulfill compliance requirements for GDPR Article 30, CCPA, LGPD, and more.
- **Automate Inventory of AI Assets:** Automatically inventory AI assets, models, and data for training AI models, including datasets and files, models, and vector databases.
- **Track AI Policies & Violations:** Automate policies and enforcement of data usage during the training process for AI and LLMs across the organization to gain critical insights into data security and compliance.
- **Jump Start AI Initiatives:** Prepare secure data sets for use in AI and minimize the risk of sensitive data overexposure, leaks, or breaches.
- **Enable Zero Trust & Model Access:** Reduce the overexposure of sensitive, personal, regulated, at-risk, and training data and manage AI model access to ensure zero trust.
- **Assess Data Risk:** Automatically generate comprehensive and actionable reports on data risk posture, governance, and compliance. Tailor the reports to address the specific areas of importance for your organization.
- **Investigate & Respond to Incidents:** Seamlessly map and inventory data to determine impacted users and personal data. Generate automated reports for regulators and auditors and identify users' residency to easily tailor the response to specific requirements.

About BigID

BigID enables security, compliance, privacy, & AI data management for all data, everywhere. BigID is enterprise-ready and built to scale: enabling a data-centric approach to comprehensive cloud data security & DSPM, accelerating compliance, automating privacy, and streamlining governance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

BigID has been recognized for innovation as a World Economic Forum Technology Pioneer; named to the Forbes Cloud 100; the Inc 5000 for 4 consecutive years; the Deloitte 500 for 4 consecutive years; Market Leader in Data Security Posture Management (DSPM); Leader in Privacy Management in the Forrester Wave; and an RSA Innovation Sandbox winner.

Find out more at https://bigid.com.

Know Your Data, Control Your Data.

Data Security • Compliance • Privacy • AI Data Management

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

> **Tools like BigID are the future.**
> Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.
>
> IDC
> Ryan O'Leary
> Future of Trust: Battling Data Discovery Confusion