AI Risk and Implementation Assessment: Zapier

Research and Report by Tawana Townsend, AIGP ODCP

Executive Summary

This assessment evaluates AI governance risks associated with Zapier's AI-powered automation platform, applying the NIST AI Risk Management Framework and a proprietary Human Enablement and Exploitation Framework. The analysis identifies 27 potential risks across privacy, security, operational, compliance, and ethical categories, with five priority risks requiring immediate attention.

Key Finding: While Zapier demonstrates solid technical security and privacy practices with transparent compliance to US privacy laws and GDPR, the platform's governance approach creates a critical organizational challenge. Zapier's "Zapier-centered" governance model encourages organizations to delegate governance responsibility to the exact vendor providing the AI service (Zapier). This relationship creates a false sense of security and blurs accountability lines. **The greatest risks associated with Zapier adoption are not platform-level technical failures, but organizational implementation gaps.**

Critical Assessment of Zapier's Governance Posture

Strengths:

- Robust security infrastructure with demonstrated incident response capability
- Transparent compliance certifications and adherence to privacy regulations
- Clear documentation of data handling and security practices
- Enterprise features supporting technical controls

Concerns:

- Cavalier tone regarding organizational governance responsibility
- Limited guidance on safety risks, rogue system scenarios, and system shutdown protocols
- Unclear delineation of authority: Who can shut down automations in crisis scenarios (organization, Zapier, or third-party vendors)?
- Insufficient acknowledgment of risks beyond those explicitly tied to legal compliance
- Vendor-centric governance model that blurs accountability boundaries

The Accountability Gap: Zapier provides the tools for governance, but its stance on being both the service provider and governance advisor poses a conflict of interest that leaves organizations vulnerable. Organizations that "hand over governance" to Zapier abdicate responsibility while remaining legally and operationally accountable for outcomes.

Priority Risk Landscape

Of the 27 identified risks, **five require immediate organizational mitigation:**

R1 & R2: Data Flow, Contextual Integrity, and Data Exposure (CRITICAL)

- Employees create automations without understanding data classification
- Cross-application data flows bypass security controls and violate privacy laws
- Unclear data retention practices conflict with GDPR "right to be forgotten"
- Weak authentication practices (2FA optional, not required) create security vulnerabilities
- **Likelihood:** High | **Impact:** High | **Priority:** Critical

R3: System Reliability and Validity (HIGH)

- AI-suggested automations may be inaccurate or suboptimal
- System failures (API limits, authentication failures, app changes) cause operational disruption
- Over-reliance on automation erodes contingency planning and human judgment
- **Likelihood:** High | **Impact:** Medium-High | **Priority:** High

R4: Transparency, Explainability, Interpretability, and Accountability (HIGH)

- Zapier's AI agents operate as "black boxes" with opaque decision-making logic
- Organizations defend AI decisions without understanding underlying algorithms or training data
- Insufficient audit trails complicate incident investigation and compliance
- Unclear ownership when employees leave (orphaned automations)
- **Likelihood:** Medium | **Impact:** High | **Priority:** High

R5: Job Displacement and Workforce Impact (MEDIUM-HIGH)

- Automation adoption without change management disrupts organizational culture
- Employee fears about job security reduce engagement and productivity
- Potential ethical violation: Training AI on employee-derived data without compensation
- **Likelihood:** Medium | **Impact:** Medium-High | **Priority:** Medium-High

Mitigation Strategy: Governance Framework

The assessment provides 32 specific mitigation strategies organized across four control areas:

Technical Controls

- Data loss prevention, mandatory 2FA, API key management, automated monitoring
- Focus: Close technical security gaps that Zapier leaves to organizational discretion

Policy Controls

- Acceptable use policies, cross-border data governance, approval workflows
- Focus: Define boundaries for responsible automation use

Process Controls

- Mandatory training, regular audits, incident response plans, human-in-the-loop requirements
- Focus: Operationalize governance through repeatable workflows

Organizational Development Controls

- Change management, transparent communication, skills transition, psychological safety
- Focus: Address the human dimension of AI adoption

Cross-Cutting Governance

- Center of Excellence establishment, tiered risk classification, maturity assessment
- Focus: Create sustainable governance infrastructure

Implementation Approach: 12-Month Phased Rollout

Recognizing that governance implementation is fundamentally an organizational challenge, not a technical one, the assessment provides a comprehensive change management strategy:

Phase 1 (Months 1-2): Foundation & pilot **Phase 2 (Months 3-4):** Expanded pilot across additional departments, policy refinement **Phase 3 (Month 5):** Scaled rollout to multiple departments **Phase 4 (Month 6):** Enterprise-wide adoption with 180-day assessment **Phase 5 (Months 7-12):** Optimization and continuous improvement, 360-day assessment

Critical Success Factors:

- Executive sponsorship and sustained leadership commitment
- Stakeholder engagement: Meet early and often, co-design governance with users
- Comprehensive training: Enterprise-wide AI awareness + user-specific + specialist training
- Transparent communication addressing job security fears directly and honestly
- Cultural readiness: Psychological safety, employee autonomy within guardrails
- Continuous improvement: Quarterly reviews, annual maturity assessment

Zapier is a powerful automation platform with solid technical foundations, but it shifts governance responsibility to organizations without providing sufficient guidance on implementation. Organizations must proactively develop robust governance frameworks that address not only technical controls but also the organizational, cultural, and human dimensions of AI adoption.

The risks are manageable, but only through deliberate organizational action. Organizations that implement the mitigation strategies and change management approach outlined in this assessment can safely harness Zapier's capabilities while protecting data, maintaining compliance, preserving employee trust, and ensuring accountability.

Organizations that delegate governance to Zapier or adopt the platform without comprehensive internal governance structures and change management practices expose themselves to critical privacy, security, operational, compliance, and ethical risks.

Section 1: System Overview

1.1 Company Overview

Zapier is a private, U.S. software company, specializing in workflow automations and application integration through its AI powered platform. Its latest capability includes AI orchestration, a term

used to describe backend processes that connect AI tools, AI agents, and AI powered automation for advanced, seamless workflow integration. Established in 2011, Zapier is now the most recognized and used enterprise workflow automation platform for businesses. As of this assessment, Zapier averages 3.4 billion workflow automation tasks each month. Its simple, structured integrations allow users to connect multiple applications to produce workflow automations without Application Programming Interfaces (API). Zapier has multiple customer tiers: limited free tier, professional for $19 per month, and a team plan for $69 per month. They also offer customized pricing for enterprise contracts. Customer tiers are segmented by the users ability and desire to customize automations and integrations through the use of code or low/no code.

Notable Zapier Features

- Classified as a integration Platform as a Service (iPaaS)
- Utilizes serverless cloud through Amazon Web Services (AWS) Lambda, an event driven cloud service
- Uses Large Language Models (LLMs), through its Zapier Copilot, to assist users in building, modifying, and troubleshooting automations and integrations
- APIs provide seamless programming to its users
- Through Canvas, businesses can map processes and workflows on a virtual, user-friendly whiteboard to develop a strategic view of possible automations
- Zapier's Developer Platform allows customization of automations and integrations

Zapier brings in roughly $400M in annual revenue, providing iPaaS support to over 3M users. Mid and large sized companies make up 61% of its customer base, with the bulk of users residing in the US. Zapier offers roughly 8,000 applications to-date, such as Canva, Asana, Claude, Hubspot, Jira, and Google Suite. By creating *Zaps,* users are able to connect these previously stovepiped applications to streamline and automate tasks on a daily basis. Businesses have shown cost and time savings and significant reduction in errors through the use of automation tools and platforms like Zapier. Typical use cases include automations in data entry, e-commerce, marketing, engagement, IT helpdesk support, operations, sales, and client management.

As AI advances, so does Zapier's AI powered capabilities. AI-related tasks have grown sevenfold in the last two years. In fact, Zapier now provides AI powered workflows, chatbots, Model Context Protocol (MCP) servers, and Agentic AI. These AI-powered tools move beyond step-by-step instructions to platforms that can think, perform, and make decisions without explicit rules and programming.

AI Powered Zapier Uses

ZAPIER AGENTS	ZAPIER CHATBOTS	ZAPIER CANVAS	ZAPIER MCP
Moves beyond automation and integration by creating AI *team members*	Automates FAQs and tier 1 employee/ client engagements	Organizations and teams can conduct process mapping with Canvas to first understand and standardize current process	Allows developers to connect their AI tools to any commercial application
Allows for delegation of low priority or tedious and repetitive tasks	Learns to respond and engage based on shared organizational knowledge and alignment to an organization's style	Teams can receive AI powered optimization recommendations to improve their current processes	Handles authentication, rate limits, and retries
Notification of high-value leads for potential sales or senior leader requests for quick decisions		Teams can automatically create Zapier workflows and integrations aligned to the new processes	Connect AI tools to the business stack with minimal build and integration management

Table 1: Zapier AI-powered product offerings and uses

1.2 Technology Overview

Zapier in its simplest terms connects apps. It does not build or train AI models, but instead uses rules to trigger automatic actions, such as moving an organization's data between multiple applications (e.g. reviewing a customer's email, populating a spreadsheet with the information, and then building a dashboard at the end of the day to show customer inquiry trends). Through Zapier, businesses can connect multiple apps to automatically trigger multiple actions, including decision making.

Section 2: Current Governance State

Overall Zapier is fairly solid from a governance perspective. They thoroughly address security and privacy risks, are transparent about their compliance, and adhere to US privacy laws and the EU's General Data Protection Regulation (GDPR). One point of concern is Zapier's rather cavalier tone regarding risk and governance. The company's stance on governance for its users is a "Zapier-centered approach" that serves Zapier, not necessarily its customers. In fact, the company encourages organizations to "hand over their governance" to Zapier, the same vendor

providing the AI-powered service. This type of relationship creates a false sense of governance and blurs the lines of accountability.

Additionally, risk, outside of those easily tied to laws, are not discussed in great detail by Zapier. However, there are risks associated with automation tools and these risks are exactly why organizations should proceed with caution when giving Zapier authority to provide both the service and the oversight.

In terms of security, Zapier mentions their security breach process, which was recently tested in real time during a security breach. The company's subsequent incident response shows resiliency and robustness as the automations were not down long and the problem was quickly identified and fixed. However, Zapier does not address rogue systems nor does it share identified safety risks and potential for harm. Questions such as, "how quickly can the system shut down?" and "who has the authority to shut down the automations (the company, Zapier, or the third-party vendor)?" should be clear and understood between all parties.

Section 3: Risks

3.1 Risk Overview

This section identifies and analyzes key AI governance risks associated with Zapier's AI-powered automation platform. Risks are categorized using the NIST AI Risk Management Framework and evaluated through an ethical lens informed by several ethical AI frameworks, including a proprietary Human Enablement and Exploitation Framework. The analysis focuses on platform-level technical risks, but shines a critical lens on organizational adoption and implementation risks, addressing how organizations may deploy and govern Zapier.

The assessment identified five priority risks out of 27 across five categories: privacy, security, operational, compliance, and ethical. Each risk is evaluated for likelihood and impact, with particular attention to risks that emerge from the intersection of AI automation capabilities and organizational governance gaps.

Privacy (P): information or data privacy and the rules that govern the management of private information; it is the right of individuals and/or organizations to be the authority on how their information is used, stored, shared, and collected. (IAPP, Data Privacy

Security (S): protection of information to prevent loss, unauthorized access and/or misuse. It involves assessing threats and risks to information and the procedures and controls to preserve confidentiality, integrity and availability of information (IAPP)

Operational (O): summary of loss resulting from inadequate or failed internal processes, people and systems or from external events (IBM)

Compliance (C): the threat that an organization will fail to adhere to applicable laws, regulations, contractual obligations, and internal policies (Compliance Seminars.com)

Ethics (E): the design, development, and deployment of artificial intelligence systems that align with human values, fairness, transparency, and societal well-being. Ethical AI addresses concerns such as algorithmic bias, privacy protection, accountability for AI's decisions, and the potential negative impacts of AI on employment and society. (Stanford University Human-Centered Artificial Intelligence (HAI))

Organizations should assess, evaluate, and align their internal compliance management and governance culture prior to Zapier adoption. Though Zapier is relatively safe and secure, 27 risks were identified which should be considered from each organization's lens. Proactively addressing these risks involves developing or modifying governance and risk management plan for Zapier adoption and integration.

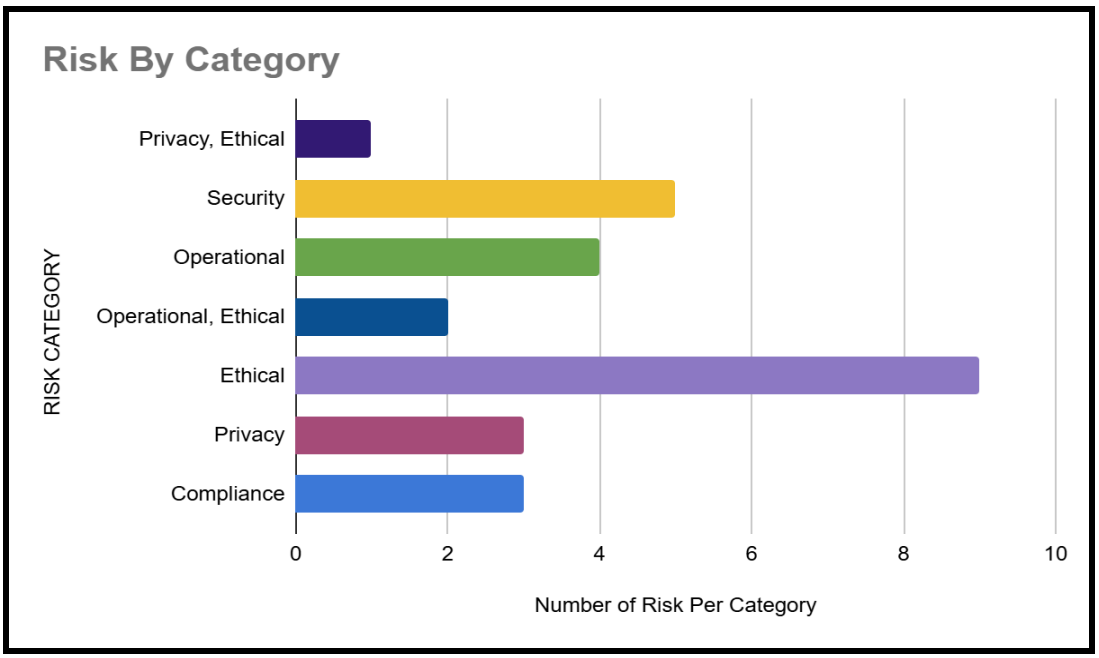


Figure 1 shows where the risks are categorized, highlighting the high level of ethical risks.

3.2 Critical Risk Assessment

3.2.1 Critical Risk Overview

27 risks were identified and aligned to Zapier's platform, implementation of automations or agents, or both. The top 5 risks focus on data transmission and storage, trustworthiness of the platform, and job displacement concerns.

RISK #	RISK CATEGORY	IDENTIFIED RISK	PROBABILITY	IMPACT	RISK RATING
R1	**Privacy, Ethical**	Data Flow and Contextual Integrity	High	High	3
R2	**Security**	Data Exposure and Storage	High	High	3
R3	**Operational**	System Reliability and Validity	High	High	3
R4	**Operational, Ethical**	Transparency, Explainability, & Interpretability and Socio-Technical Accountability	High	High	3
R5	**Ethical**	Job Displacement and Transparency	High	High	3

Top 5 Critical Risk of Zapier adoption. Rating schema 1=Low, 2=Med, 3=High

3.2.2
Risk 1 (R1) Data Flow and Contextual Integrity
Risk 2 (R2) Data Exposure and Storage

There is a high-probability for employees to create Zaps without a full understanding or appreciation for data classification, resulting in potential privacy and data protection law violations. Automation software inherently increases the probability of data exposure and leakage. This is due to the quantity and frequency of connections between various applications and platforms. For example, if an organization plans to use Zapier to create an agent that performs tasks using multiple apps (e.g. email, social media, Excel, and Notion), data privacy may be compromised by one or all of the applications, including Zapier. Using multiple applications makes it challenging to pinpoint the responsible party when an incident, such as data leakage, occurs. Furthermore, running multiple applications increases the likelihood of a customer or the organization's data being used outside of the original intent, thus potentially violating consent laws. Zapier's AI automation and agent tools empowers employees to execute

functions and tasks at higher speeds and greater scale. This ease of access and implementation of Zaps may allow employees to create automations and agents without IT/security approvals, often bypassing established security controls and change management practices.

Additionally, Zapier's storage practices may conflict with industry or country laws. Data is stored globally and without a clear indication of data retention rules. If an employee assumes the storage is account-based versus global, they may choose a weak key. This opens the user up to security issues related to authentication tokens, personally identifiable information (PII), and sensitive data.This poses a risk because if an employee chooses a weak key or if an employee stores API keys in Zaps, they could unintentionally allow unauthorized access to sensitive data, PII, or even authentication tokens. It also creates cascading security breach by compromising not just Zapier, but all connected applications. Organizations without robust data governance practices run the risk of violating data localization requirements found in industry and or country specific requirements. Common data retention policies have strict rules regarding the storage timeline and Zapier's policy fails to address it. There is inadequate information on how often data is stored in the Zaps and how employees or customers can purge data from Zaps, which explicitly violates the GDPR's stance on "the right to be forgotten".

To combat data security breaches, Zapier strongly recommends that users enable two-factor authentication (2FA) for security best practices; however, 2FA is only a suggestion, thus most users are using an outdated and unsecure credential method (username and password). Additionally, Zapier's March 2026 security breach can be traced back to a 2FA misconfiguration of an account. The ramifications of this data leakage is unknown, but typically organizations face financial losses, damaged reputations, and legal repercussions. Zapier has since modified its routine monitoring and auditing, but outdated authentication methods are still in place. It isn't clear if the recent updates to their monitoring/auditing are specific to data leakage, data flow and integrity.

Bottom Line: Organizations and teams must ensure that the use of Zapier doesn't "go against" the organization's internal privacy and data protection rules and industry or local compliance standards.

3.2.3 Risk 3 (R3): System Reliability and Validity

Automation software and AI agents are not infallible; Zapier users experience system failure due to issues with API rate limits, changes in connected apps, and authentication failures. Intermittent automation and agent failures are costly for organizations, as they may result in missed opportunities, competitive disadvantage, and decreased productivity. At times, Zapier automation tools may recommend inaccurate or incorrect automations as well, prompting the necessity for human oversight and routine monitoring to reduce the probability of faulty automations. Since system downtime and automation/agent mistakes are inevitable, it is important for organizations to identify and pilot low risk tasks to minimize any potential high risk and costly impacts. The path to over-reliance on AI-driven workflows is a slippery slope. It is easy for employees to trust AI-powered automation and agents without verification, especially

when the messaging around AI has been “increased accuracy and faster speed”. Employees must know that the system may produce suboptimal results, make recommendations that are inaccurate, or completely fail. Organizations must have contingency plans in place that address what to do when systems fail or produce unreliable outcomes.

Bottom Line: The mindset of blind trust has to be addressed early and continuously to avoid catastrophic impacts of system failures and decreased reliability.

3.2.4 Risk 4 (R4): Transparency, Explainability, & Interpretability; Socio-Technical Accountability

Many basic automations in Zapier, such as drafting an email at a specific time each day, are fairly straightforward. However, agents are not transparent, explainable, and interpretable. Zapier's AI automations and agents have black box capabilities, so the logic and reasoning used to execute agent functions is unknown. This means there is no clear path for how and why decisions were made or actions were performed. Organizations that use Zapier, and in some cases, individual employees in an organization are responsible for the outcomes, not the AI nor Zapier. This means organizations will have to defend decisions made by agents acting on their behalf without full knowledge, understanding, and agreement on the data the agent was trained on, its logic, nor its algorithms. Zapier's agents may make biased and discriminatory decisions, especially if they were trained on biased data. The automations and agents also neglect industry or sector-specific regulations (e.g. HIPPA, FINRA), meaning organizations must be diligent about applying these rules in an automated environment. Though the regulations exist outside of AI-powered tools, staff typically have a wide breadth of knowledge and experience to spot these violations fairly easy. By the time an organization realizes the Zapier agent’s outcomes are inaccurate, biased, or discriminatory, the damage has likely been done. Furthermore, without a sufficient audit trail, incident investigations are challenging and security compliance is often violated.

Organizations have to ensure accountability when using AI-powered automations and agents. Waiting to identify the accountable party until after a Zapier AI automation tool or agent causes harm, is simply too late. Accountability, transparency, and explainability should be addressed prior to Zapier deployment. Questions to consider:

1. Who is held accountable when automation or agents don't work?
2. If an agent executes a task incorrectly or inaccurately, what steps should the responsible party take?
3. What is the logic behind the agent’s decisions? What algorithms are used and why?
4. What type of data was used to train Zapier’s AI-powered platform?
5. Who should be responsible for monitoring and how often should it occur?
6. Will you allow for collaboration in agent creation/execution? If so, what will accountability look like with collaborative ownership?
7. What should we specifically monitor for that may indicate decreased trustworthiness in the automation or agent’s outputs?
8. How will you mitigate the risk of abandoned automations when employees leave?

Bottom Line: Organizations are solely responsible for the outcome of Zapier's AI-powered automations and agents; therefore, AI governance plans are necessary to ensure transparency, explainability, interpretability, and accountability.

3.2.5 Risk 5 (R5): Job Displacement and Transparency

There is inherent risk to organizational culture, operations, and the workforce when tasks are redistributed from employees to AI. While automation can free up cognitive space for innovation, automation has historically led to job loss and/or restructuring. When organizations begin to consider AI-integration or flat out adopt AI-powered automation and agents, such as Zapier, a shift occurs in the workforce. Some employees begin to fear job loss or job reassignment. Redistributing work from employees to AI and/or forcing employees to offload their tasks to AI, may result in disengaged, less productive employees and an unintended shift in the organizational culture. Psychological safety is disrupted when advanced AI tools, such as Zapier, are integrated without effective organizational development practices. Successful implementation of Zapier is not linear, but it does require effective change management, implemented early on and throughout.

Additionally, employees may also suffer a form of job displacement as models are trained using employee-derived data (their work products, communications, logic, templates, etc.). This results in a potential ethical risk of replacing employees without compensating them for their hours, data, ideas, solutions, and voice.

Bottom Line: Zapier, or any AI-powered tool should not be adopted until a thorough assessment and plan are established; this is more likely to result in adoption that enables versus exploits the existing workforce.

Section 4: Risk Mitigation

This risk mapping reveals that the greatest governance challenges in Zapier AI automation stem not from platform limitations but from organizational governance gaps. While Zapier provides tools for oversight and control, many organizations lack the policies, processes, and cultural norms to use these tools effectively.

Section 4.1
Risk 1(R1) Data Flow, Contextual Integrity
Risk 2 (R2) Data Exposure & Storage
Risk Rating: HIGH

R1/R2 Technical Controls

1. **Implement Data Loss Prevention (DLP) Rules**
    - Configure Zapier to restrict data flows to approved applications only

- Set up automated alerts for high-risk data transfers (PII, financial data, health data)
- Block connections to non-approved third-party apps

2. **Enforce Data Classification Tagging**
   - Tag data sensitivity level prior to Zapier adoption
   - Require employees to tag data sensitivity level before creating Zaps (requires training and change management)
   - Automate restrictions: Tier 1 data cannot flow through Zapier without explicit approval
3. **Mandatory Two-Factor Authentication (2FA)**
   - Require 2FA for all Zapier accounts (not optional)
   - Use hardware keys or authenticator apps (not SMS)
   - Audit monthly for non-compliant accounts
4. **API Key Management Protocol**
   - Centralized credential vault (e.g., HashiCorp Vault, AWS Secrets Manager)
   - Require API key rotation every 90 days
   - Never store keys directly in Zaps - use OAuth where possible
   - Automated scanning for exposed credentials in Zaps
5. **Data Retention & Deletion Controls**
   - Document Zapier's data retention practices clearly in organizational policy
   - Implement automated data purge workflows (quarterly reviews of stored data)
   - Ensure compliance with applicable laws and regulations; align deletion procedures to compliance

R1/R2 Policy Controls

1. **Zapier Acceptable Use Policy**
   - Define and share what data types are prohibited in automations
   - Specify approved applications for different data classifications
   - Include consequences for policy violations
2. **Cross-Border Data Transfer Governance**
   - Document where Zapier stores data (by region)
   - Maintain data processing agreements (DPAs) with Zapier
3. **Approval Workflow for High-Risk Automations**
   - Require Security approval for Zaps handling:
     - PII, Financial data, Health information, and Authentication credentials
   - Implement approval request system and process with built-in audits and defined SLA for approval turnaround

R1/R2 Process Controls

1. **Mandatory Zapier Governance Training**
   - Implement employee training before Zapier access is granted
   - Cover: Data classification, approved apps, security risks, approval process

- Refresher training required annually and after incidents
- Track completion in LMS

2. **Monthly Zap Audits**
   - IT reviews all active Zaps monthly
   - Flag high-risk data flows for review
   - Identify abandoned Zaps (Zap owner reassigned or left organization)
   - Document audit findings and remediation actions
3. **Incident Response Plan for Zapier Data Breaches**
   - Define roles: Who investigates? Who communicates?
   - Establish breach notification timeline
   - Document post-incident review process
   - Test incident response annually and as needed

Section 4.2
Risk 3 (R3): System Reliability and Validity
Risk Rating: HIGH

R3 Technical Controls:

1. **Automated Monitoring & Alerting**
   - Set up monitoring for Zap failures (alert after 3 consecutive failures)
   - Track API rate limit errors
   - Monitor authentication failures
   - Create and use automation health metrics dashboard
2. **Redundancy & Backup Workflows**
   - For critical automations, create manual backup procedures
   - Document rollback processes if automation fails
   - Maintain list of critical vs. non-critical Zaps

R3 Process Controls

1. **Pilot Program for New Automations**
   - Test all new Zaps in sandbox environment first
   - Start with low-risk, non-critical processes
   - Run parallel (manual + automated) for 30-45 days and assess
   - Document lessons learned from pilot
2. **Human-in-the-Loop for High-Stakes Decisions**
   - Require human approval for specific actions. Examples include: financial transactions above $X, customer-facing communications, data deletions, access provisioning/de-provisioning
   - Build approval steps into Zap workflows
3. **Contingency Planning**
   - Document what-if decision trees: "If Zapier fails, we will..."

- Maintain manual process documentation for critical workflows
- Define RTO (Recovery Time Objective) for each critical automation
- Test failover procedures quarterly

R3 Cultural/Training Controls

1. **"Trust but Verify" Culture**
   - Train users: AI/automation can fail - always verify outputs
   - Create all-access repository of automation failures
   - Reward employees who catch automation errors before impact
   - Leadership messaging: "Automation doesn't replace your judgment"

Section 4.3
Risk 4 (R4): Transparency, Explainability, Interpretability; Socio-Technical Accountability

Risk Rating: HIGH

R4 Governance Controls

1. **Zapier Accountability Matrix (RACI)**
   - Define for each automation prior to creation:
     - Responsible: Who created/maintains the Zap?
     - Accountable: Who is accountable for outcomes?
     - Consulted: Who must review before deployment?
     - Informed: Who gets notified of changes?
   - Document in centralized Zap registry
2. **Pre-Deployment AI Risk Assessment**
   - Before any automation goes live, complete risk assessment:
     - What decisions does this automation make?
     - What data does it use?
     - What could go wrong?
     - Who is accountable?
     - What regulatory requirements apply?
   - Require sign-off from business owner + IT + compliance at a minimum
3. **Create Audit Trail Environment**
   - Enable detailed logging for all Zaps
   - Retain logs for minimum 12 months (or per regulatory requirement)
   - Document: What triggered automation? What data was used? What action was taken?
   - Make logs accessible for incident investigation

R4 Process Controls

1. **Agent/Automation Ownership Lifecycle**
    - When employee leaves: Transfer Zap ownership within 5 business days
    - Monthly review: Identify ownerless Zaps, assign owners or deactivate
    - Maintain Zap inventory with owner contact info
    - Redundancy review: Identify and deactivate Zaps that produce the same output
2. **Bias Testing Protocol**
    - For automations involving decisions about people (hiring, lending, etc.):
        - Test outputs across demographic groups
        - Document disparate impact analysis
        - Review monthly for bias drift
    - Engage legal/compliance in review
3. **Regular Transparency Reviews**
    - Quarterly: Review list of all AI-powered automations
    - Can we explain to customers/regulators how each one works?
    - Document gaps in explainability
    - Remediate or decommission unexplainable high-risk automations

R4 Documentation Controls

1. **Zapier Governance Playbook**
    - Centralized documentation including: Approval workflows, Accountability assignments, Monitoring protocols, Incident response procedures, Regulatory compliance requirements by industry
    - Update quarterly, communicate changes

Section 4.4
Risk 5 (R5): Job Displacement and Transparency
Risk Rating: MEDIUM-HIGH

R5 Organizational Development Controls

1. **Change Management Plan for Zapier Adoption**
    - Phase 1: Communicate vision (why automation, what's the goal)
    - Phase 2: Stakeholder engagement (listen to concerns, co-design)
    - Phase 3: Pilot with champions (early adopters, success stories)
    - Phase 4: Gradual rollout with support
    - Phase 5: Continuous feedback loops
2. **Transparent Communication Strategy**
    - Leadership message that addresses workforce and stakeholder concerns
    - Share specific examples: "Zapier will handle X, freeing you to do Y"
    - Address job security concerns directly, honestly, and frequently
    - Commit: "No job losses due to automation without retraining opportunities"
3. **Skills Transition & Retraining Program**
    - Identify: What tasks are being automated?

    - Plan: What opportunities are created? What new skills will employees need?
    - Invest: Provide training for higher-value work
    - Track: Employee progression into new roles
4. **Employee Data Rights & Consent**
    - Transparent policy: How employee data is used to train/improve automations
    - Opt-in consent for using work products to train AI
    - Credit employees whose work/data improves AI systems
    - Consider: Profit-sharing or bonuses when AI trained on employee work increases efficiency

R5 Cultural Controls

1. **Psychological Safety Initiatives**
    - Create forums for employees to voice automation concerns without retaliation
    - Regular pulse surveys: How do employees feel about automation?
    - Leadership commitment: Address concerns raised, report back on actions taken
2. **Collaborative Automation Design**
    - Involve employees in designing automations for their own work
    - Ask: "What tasks would you like to automate? What concerns do you have?"
    - Co-create: Employees + IT + automation specialists
    - Result: Buy-in, better automations, reduced fear

Section 4.5
Cross Cutting Governance Strategies

1. Establish Zapier Center of Excellence (CoE)

Prior to adoption, the CoE develops and/or provides input to the governance strategy, implementation approach, and use case identification.

Recommended CoE Structure and Stakeholders

- Leadership: ISO/IT Director, Business Process Owner, Compliance Lead
- Members: Representatives from key business units, as well as security and legal
- Responsibilities:
    - Approve high-risk automations
    - Maintain governance policies
    - Develop and provide training and support
    - Monitor compliance
    - Share best practices

Meetings: Monthly governance reviews, quarterly planning

2. Establish Zapier Governance Operating Model

Recommended Guardrails

- Business units create automations with approved apps and for lower tier tasks
- IT identifies approved apps, data restrictions, conducts monitoring
- CoE provides oversight by approving high-risk categories, performing audits, and developing policies

Recommended Escalation Plan

- Low-risk automation: Self-service (user creates, IT monitors)
- Medium-risk: IT review required before activation
- High-risk: CoE approval required, documented risk assessment

3. Recommended Tiered Automation Guardrails

Risk Tier	Examples	Approval Required	Monitoring
Tier 1 (Low)	Email notifications, data syncs	None	quarterly
Tier 2 (Medium)	Customer data processing, multi-app workflows	IT review	monthly
Tier 3 (High)	Financial transactions, PII, decisions impacting people	CoE approval + documented risk	Real-time monitoring and weekly reviews

The mitigation strategies outlined in this assessment provide a comprehensive framework for governing Zapier's AI-powered automation platform. However, technical controls and governance policies must be embedded into organizational culture, processes, and daily operations. Successfully deploying these mitigations requires:

- Change management expertise to navigate the human dimensions of AI adoption
- Stakeholder alignment across IT, business units, legal, and compliance
- Cultural transformation that balances innovation with responsible governance
- Sustainable processes throughout implementation

Bridging the implementation gap between governance and operations requires expertise rooted in AI governance, organizational development, and change management. Organizations with limited internal AI governance expertise often benefit from partnerships with specialists who combine technical AI literacy with organizational change management capabilities. Whether

through fractional consulting arrangements, advisory relationships, or targeted implementation support, external expertise can accelerate governance maturity while building internal capacity.

Section 5: Change Management

This section addresses organizational change management approaches required to translate governance frameworks into sustainable practice. Drawing on organizational development principles and change management best practices, this implementation approach incorporates governance, people, processes, and culture.

5.1 Why Change Management

The emergence of more advanced AI-powered tools and agents does not negate the need for structured change management. It is essential to a successful and sustainable implementation. Research consistently shows that 70% of organizational change initiatives fail not due to poor strategy, but due to inadequate change management.

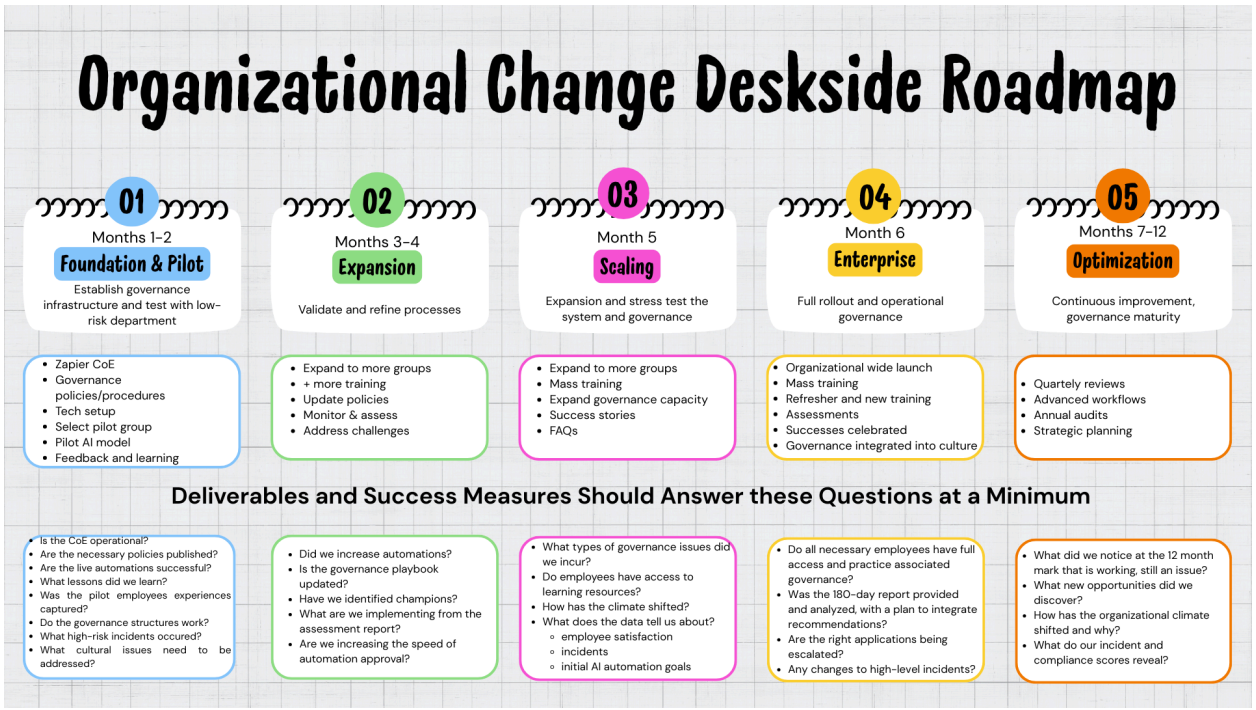
Process changes: New approval workflows, monitoring requirements, documentation standards
Behavioral changes: How employees create automations, seek approvals, think about risk
Cultural changes: From "move fast and automate" to "automate responsibly"
Role changes: New responsibilities for governance, new skills required
Psychological changes: Addressing fears about job security, control, and AI reliability

Integrating Zapier into an organization’s workflows requires a deliberate change management approach. The approach begins with recognizing that though the technology is ready, the people are likely not. Even the most enthusiastic or the change champions require time, support, and engagement to adopt any new practices. When these new tools impact not just the speed or accuracy of their work, but their sense of purpose, autonomy, and potentially their livelihood, a phased rollout strategy is a must. Below is an outline that balances the urgency of mitigating identified technical and implementation risks with sustainable organizational change.

5.2 Phased Zapier Rollout

The rollout is structured in five phases, each building organizational capability and governance maturity before expanding scope. It dedicates an entire year to adoption and integration, which is vital to sustainment. The full timeline can be found in the appendix, but a deskside roadmap is shown below. Each of the phases addresses people, processes, and tools. The length of each phase is a guideline and each organization should assess whether or not they need to increase

speed of implementation (rare), spend more time in a particular phase or pause implementation altogether.



5.3 Stakeholder Engagement

Stakeholder engagement is vital. Many organizations overlook this piece and move straight to communication and product launch. However, a great deal of time should be set aside to engage with key stakeholders early and often for several reasons.

- Stakeholders are the voice of the users and provide valuable insight into the needs, resistance, legal and regulatory requirements, use cases, and organizational climate
- Stakeholders advance adoption by often serving as champions or early adopters in a major organizational change
- Stakeholders work together to ensure required resources are available and in place to drive change from initial pilot to full scale adoption
- Stakeholders have their ear to the ground, often offering feedback and answering the "why" before an incident occurs

Stakeholder engagement ensures the approach is adopted across the enterprise versus stalling in one department. The implementation team or vendor cannot possibly conduct all of the organizational responsibilities associated with the adoption and that's where the key stakeholder groups shine.

5.3.1 Key Stakeholder Groups

Stakeholder Group	Role in Governance	Engagement Needs	Engagement Approach
Executive Leadership	Sponsor, resource allocation, culture setting	Understand business value, risk mitigation, ROI	Quarterly steering committee, executive briefings
IT Leadership	Technical implementation, security oversight	Detailed technical requirements, integration with IT processes	Weekly CoE meetings, technical working sessions
Business Unit Leaders	Department adoption, resource allocation, accountability	Balance governance with efficiency, department-specific guidance	Monthly governance roundtables, 1:1 consultations
Compliance/Legal	Regulatory interpretation, policy approval	Ensure governance meets regulatory requirements	Bi-weekly policy reviews, incident escalations

End Users	Day-to-day adoption, automation creation	Understand "why" governance matters, easy-to-follow processes	Training, office hours, user feedback sessions
IT/Security Team	Monitoring, approval workflow, technical support	Workload management, tools/training	Weekly standups, monthly retrospectives
HR/OD	Change management, training, culture	Support workforce through transition, address job security fears	Bi-weekly coordination, joint communication planning

5.3.2 Stakeholder Engagement Timeline

Pre-Launch (Month 0):

- Executive sponsor identified and committed
- CoE members recruited and onboarded
- Key stakeholder one-on-ones: "What are your concerns? What do you need?"

Phase 1-2 (Months 1-4):

- **Executive:** Monthly steering committee (30 min)
- **CoE:** Weekly meetings (1 hour)
- **Pilot users:** Weekly check-ins during pilot, bi-weekly after
- **Business unit leaders:** Monthly roundtable (1 hour)

Phase 3-5 (Months 5-12):

- **Executive:** Quarterly steering committee
- **CoE:** Bi-weekly meetings (as governance stabilizes)
- **All users:** Monthly office hours, quarterly town halls
- **Business unit leaders:** Quarterly governance reviews

5.3.3 Engagement Tactics

1. Meet Early and Often

- Launch with a feedback tour: this is an opportunity to listen to the employees about the challenges they face with the new system, what works, and discover new opportunities.
- Regular feedback loops: surveys, focus groups, office hours

- Transparent decision-making: **DO NOT HOLD ADDITIONAL INFORMATION GATHERING SESSIONS, WITHOUT ADDRESSING A PREVIOUSLY IDENTIFIED ISSUE FIRST.** "Here's what we heard, here's what we're doing"

2. Co-Design Approach

- Don't impose governance on users, design it WITH them
- Pilot feedback directly shapes policy
- User representatives in CoE meetings

3. Assign Meaningful Roles From your list of key tasks, assign ownership:

- **IT Director:** CoE chair, technical implementation lead
- **Compliance Lead:** Policy development, regulatory interpretation
- **Business Process Owner:** Approval workflow design, business impact assessment
- **Department Champions:** Training support, peer coaching, feedback gathering
- **Security Lead:** Monitoring strategy, incident response

4. Celebrate Contributions

- Recognize pilot participants publicly
- Highlight department champions in communications
- Executive thank-you notes to key contributors

5.3.4 Training & Development

Establish multiple training tiers to address the various roles and needs in your organization. Training should be innovative and engaging. Avoid sticking employees in an auditorium or tethering them to a computer for the full training. Provide multiple training methods and build-in opportunities for play, exploration, and experimentation for the best training results. The following are examples of training tiers that may work for Zapier implementation across a common organization, but the number of tiers and tier descriptions should be customized for each organization, use case, and tool.

Tier 1: Enterprise-Wide Foundation (All employees)

Learning Objectives:

- Understand what AI-powered automation is and isn’t (basic concepts)
- Recognize AI's role in the organization (why are we doing this)
- Understand why governance matters (safety, compliance, ethics)
- Know how to raise concerns or report issues (governance is everyone’s responsibility)

Tier 2: Zapier User Training (Automation creators, owners, managers)

Learning Objectives:

- Understand Zapier governance policies and procedures
- Navigate approval workflow
- Assess risk in automation scenarios
- Create automations that comply with governance
- Know when to escalate

Tier 3: Governance Specialist Training (CoE, approvers, champions)

Learning Objectives:

- Deep understanding of AI risk landscape
- Apply governance frameworks (NIST AI RMF)
- Make informed approval decisions
- Coach users through governance process
- Identify emerging risks

Training Innovation: Coaching Model

Coaching can complement traditional training structures, but providing support that addresses specific roadblocks and/or creates empowering environments and mindsets. Below are examples of coaching that could be offered to help ensure a successful AI adoption.

Innovation Coaching Sessions (Optional, for power users)

- 1:1 or small group sessions
- "I have a complex automation idea - help me design it within governance"
- CoE member coaches through risk assessment and design
- Builds capability while ensuring compliance
- Builds a governance culture that enables innovation and new ideas

5.6 Communication Strategy

The communication strategy will vary based on the organizational culture, resources, leadership, and workforce climate. However, the following are essential to an effective organizational communication strategy, especially one that involves a massive technology change. These principles build trust:

Transparency Ensures the entire workforce understands the why behind every decision that organization makes; they may not agree or fully support, but the key here is to provide information at the deepest level

Consistency No matter how great the communication medium, it will often not be received, read, or opened. Consistent messaging enforces the key facts about the adoption and builds a sense of trustworthiness about what is being said. Each message should be repeated across multiple and various channels (email, live sessions, meetings, etc.). Cascading messages would work well in this environment while ensuring consistency

Engagement No one wants to be talked to, especially in the midst of a major transition. A great deal of time should be dedicated to simply listening to understand needs, behaviors, issues, and shifts in culture or processes. If possible, capture the feedback in multiple ways (e.g. focus groups, surveys, townhalls)

Timely Communicating early reduces the spread of rumors. The absence of information leaves too much space for people to create their own stories. The organization should control the narrative by addressing concerns with a sense of urgency.

Empathy This leadership quality should not be overlooked when developing and executing the communication strategy for Zapier adoption. Empathetic leaders acknowledge concerns, address fears, and allow space for people to process their emotions. Empathy embedded in the communication strategy may look like slowing down implementation, taking the time for coaching, or listening to improvement ideas.

5.7 Cultural Readiness & Support

Pre-Implementation Cultural Assessment

Before rolling out Zapier and associated governance, it is imperative to assess organizational readiness. For example, an organization may have the right technical infrastructure, but may lack established and standardized workflows. Workforce assessments can be done via surveys (for the entire organization) and focus groups (for specific pockets and deep dives). The results provide insight into where there may be resistance, what to address during training and in the communication strategy, and how to design the governance policies and processes.

Sample questions include:

- How comfortable are you with AI and automation? (1-5 scale)
- Do you currently use automation in your work? If yes, describe.
- What concerns do you have about AI automation? (Open-ended)
- Do you feel your job is secure? (Yes/Somewhat/No)
- How much do you trust leadership to manage AI responsibly? (1-5 scale)
- What support would you need to adopt new automation tools? (Open-ended)
- "How should we govern automation to balance innovation and safety?"

Analyze results for:

- Overall readiness level (high/medium/low)
- Pockets of resistance (departments, roles, demographics)
- Key concerns to address in communication
- Training needs

5.8 Success Metrics & Continuous Improvement

Sample Governance Implementation Metrics

Track throughout 12-month rollout:

Metric Category	Specific Metrics	Target	Measurement
Adoption	% of eligible users trained	95%	LMS tracking
	# of governed automations created	200+ by Month 12	Zapier dashboard
	% of departments with active automations	80%	Department reports
Process Efficiency	Approval turnaround time	<48 hours (90% of requests)	Ticketing system
	% of automations approved vs. rejected	85% approved	Approval logs
	CoE meeting frequency needed	Bi-weekly by Month 12	Meeting calendar
Control Effectiveness	# of governance policy violations	<5% of automations	Audit results
	# of high-risk incidents	0 critical incidents	Incident reports
	% of high-risk Zaps with documented approval	100%	Compliance audit
User Experience	User satisfaction with governance process	75%+ satisfied	Quarterly survey

	Net Promoter Score for CoE support	50+	Post-interaction survey
	# of escalations due to frustration	<10 per quarter	CoE tracking
Cultural Adoption	Employee perception: "Governance enables me"	70% agree	Annual culture survey
	Employee trust in AI governance	75% trust	Annual survey
	Manager confidence supporting team	80% confident	Manager pulse survey
Business Impact	Time saved through automation	Measurable ROI	Productivity tracking
	Risk incidents prevented	Document near-misses	Incident reports

Section 6: Conclusion

This assessment identified 27 risks associated with Zapier's AI-powered automation platform and provided comprehensive mitigation strategies across technical, policy, process, and organizational controls. However, the most sophisticated governance frameworks remain theoretical until embedded into organizational culture, processes, and daily operations.

The implementation challenge is fundamentally an organizational development challenge, not merely a technical one. Zapier provides automation infrastructure and basic security features, but cannot provide what organizations need most: the governance culture, stakeholder alignment, change management expertise, and sustainable processes that transform policy documents into practice.

Organizations that outsource governance thinking to their automation vendor fundamentally misunderstand their regulatory, legal, and ethical obligations. Zapier can be held accountable for platform security and uptime, but organizations alone bear accountability for how they deploy AI tools and the outcomes those tools produce.

Organizations that successfully implement the governance framework outlined in this assessment will achieve:

- Risk Mitigation
- Operational Excellence

- Organizational Health
- Strategic Positioning

The most technically elegant governance framework will fail if it ignores the human dimension of AI adoption:

- Change Management
- Stakeholder Engagement
- Training Architecture
- Communication Strategy
- Cultural Considerations

Organizations that implement technical controls without addressing cultural readiness, employee fears, and change management fundamentals will encounter resistance, workarounds, shadow AI and IT, and ultimately governance failure.

6.1 The Path Forward

Successfully deploying the governance strategies outlined in this assessment requires expertise at the intersection of AI governance, organizational development, and change management. Bridging this implementation gap requires deliberate organizational investment.

The opportunity facing organizations is not whether to govern AI-powered automation, but how thoughtfully and proactively they choose to do so. The risks identified in this assessment are real and consequential, but they are also manageable when paired with deliberate organizational action.

6.2 Final Observations

Zapier is a powerful tool. It offers genuine efficiency gains, workflow optimization, and cognitive load reduction for knowledge workers. The platform's technical security is solid, privacy practices are transparent, and enterprise features provide necessary controls.

However, Zapier is not a governance solution. It is an automation platform that requires governance. Organizations that conflate the two expose themselves to the risks outlined in this assessment. Organizations that wait until regulatory enforcement, customer trust violations, or operational failures to occur make governance implementation far more expensive and painful.