CHECKLIST

# Deepfake defense: protecting your organization from emerging AI threats

Deepfakes are no longer a futuristic concern. They are here today, posing real risks to businesses, leaders, and employees. AI-generated audio, video and image manipulations can be used to spread misinformation, impersonate employees ranging from staff to executives, and commit fraud. Organizations must take proactive steps to safeguard their business, people, clients, systems, and reputations.

**This checklist highlights governance, technology, and training measures your team should consider putting in place to help defend against deepfake threats.**

## Governance

- [ ] **Develop an AI Policy**: Define acceptable uses of generative/agentic AI, aligning with ethical standards and regulations.
- [ ] **Create a Deepfake Response Plan**: Add deepfake scenarios to crisis communication and incident response playbooks.
- [ ] **Engage Legal Counsel**: Stay informed on evolving legislation and ensure compliance when handling biometric and likeness data.
- [ ] **Develop an Incident Response Plan:** Establish a comprehensive framework for managing and responding to AI and deepfake-related incidents, including clear roles, escalation paths, and communication protocols.

## Technology

- [ ] **Implement Detection Tools:** Integrate AI-powered detection platforms into your cybersecurity ecosystem.
- [ ] **Verify Critical Communications**: Require multi-factor authentication for sensitive transactions or public-facing statements.

## Training & Awareness

- [ ] **Train Executives**: Educate senior leaders on deepfake risks, tactics, and red flags.
- [ ] **Train Employees**: Incorporate deepfake awareness into annual security training, including detection and reporting procedures.
- [ ] **Run Simulations**: Conduct mock deepfake simulations to test organizational readiness.

KAUFMAN ROSSIN