BDO

SIFM 66 Years of Celebration

SECURING THE NEW OPERATING MODEL:

Cyber Risk Management for AI-Powered Automation & User Experiences

The new operating model depends on AI & automation – proliferating risks that threaten the gains.

Join us to explore which risks are materializing and which mitigation strategies are truly making a difference. We'll share real-world examples of what to embrace—and what to avoid—when securing your assets in AI-driven environments where outcomes are unpredictable and threats can have devastating consequences.

From the boardroom to the compliance office, we'll help you sharpen your focus and build confidence in your readiness for the future of operations—and beyond.

BDO DIGITAL

NextGen Automation for Insurance:

Securing the New Operating Model

SIFM 66 Years of Celebration

SEPTEMBER 8, 2025

Agenda for Today

1. Framing the Future-Proof AI/Automation Operating Model
2. Systemic Risks in Finance, Audit, and Operations
3. Thrive with Secure AI: ISO Personas
4. Real-World Patterns: What to Embrace vs. Avoid
5. Securing Customer-Facing AI Experiences
6. Board and Compliance Implications; CPE Learning Objectives
7. 30-60-90 Day Action Plan
8. Q&A

Learning Objectives

1

Recognize Emerging Cyber Risks in AI-Driven Insurance Operations

Understand how AI and automation are reshaping operational models in insurance—and the specific cyber threats that can compromise financial integrity, customer trust, and regulatory compliance.

2

Evaluate Risk Mitigation Strategies with Real-World Insurance Use Cases

Gain insight into which cyber risk controls are proving effective in AI-powered environments, using examples relevant to claims automation and customer engagement.

3

Strengthen Governance and Compliance for AI in Customer-Facing Workflows

Explore the implications of integrating advanced AI into policyholder interactions, and learn how to align cybersecurity practices with evolving regulatory expectations and board-level accountability.

With You Today

JIM BLACKWELL

Market Leader BDO Digital

jblackwell@bdo.com

DENNIS GLENDENNING

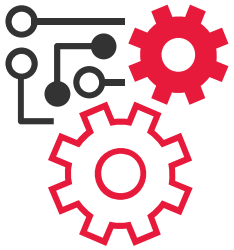
Security
Solutions Director

dglendenning@bdo.com

Why AI & Automation Are Redefining Insurance Finance

Internal audit moving to real-time risk detection & predictive analytics

Finance leadership shifting to forward-looking insights



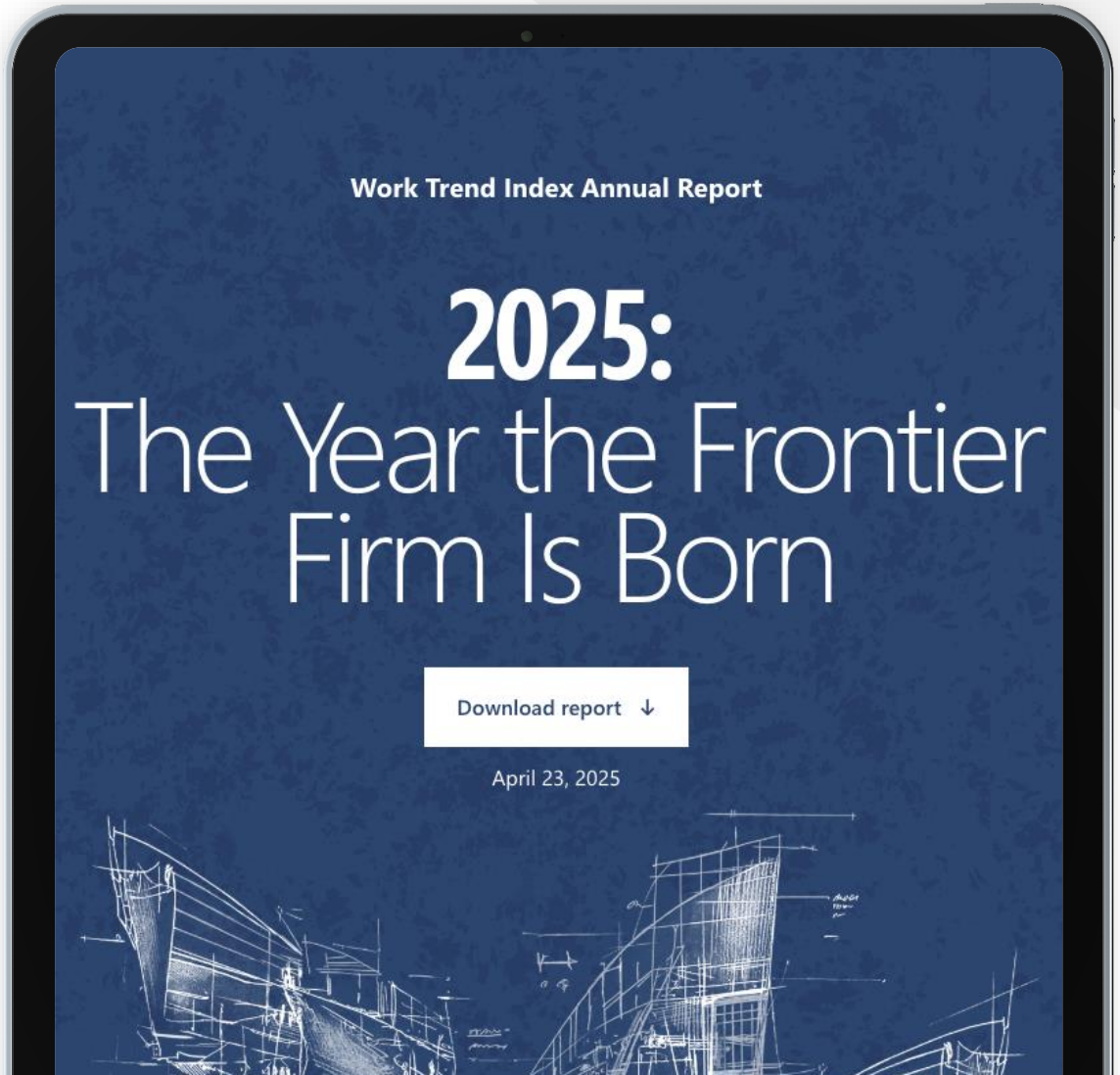
Boards prioritizing cybersecurity, data governance, and digital literacy

Operational resilience amid regulation, volatility, and talent shifts

“The Year the Frontier Firm Is Born”

MICROSOFT 2025 WORK TREND INDEX

- Reveals the emergence of “Frontier Firms” — organizations that successfully integrate AI agents into daily workflows.
- Based on a global study of **31,000 professionals** across **31 countries**
- Frontier Firms are outperforming peers: **71%** report thriving, compared to **37%** of other companies
- Highlights a **three-stage AI adoption journey**: from assistants → to digital colleagues → to AI-managed workflows
- Emphasizes the new role of “agentic” leaders who manage AI agents to drive results
- **82%** of business leaders say 2025 is a make-or-break year to adopt AI strategically
- Offers insights for companies looking to scale, stay agile, and redefine productivity in the AI era



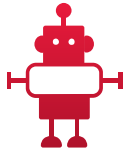
Source: [2025: The Year the Frontier Firm Is Born]

Strategic Imperatives and Organizational Shift

These reflect executive-level recognition that AI and agents are reshaping how businesses must operate.

82% of leaders say this is a pivotal year to rethink key aspects of strategy and operations

81% say they expect agents to be moderately or extensively integrated into their company's AI strategy in the next 12-18 months

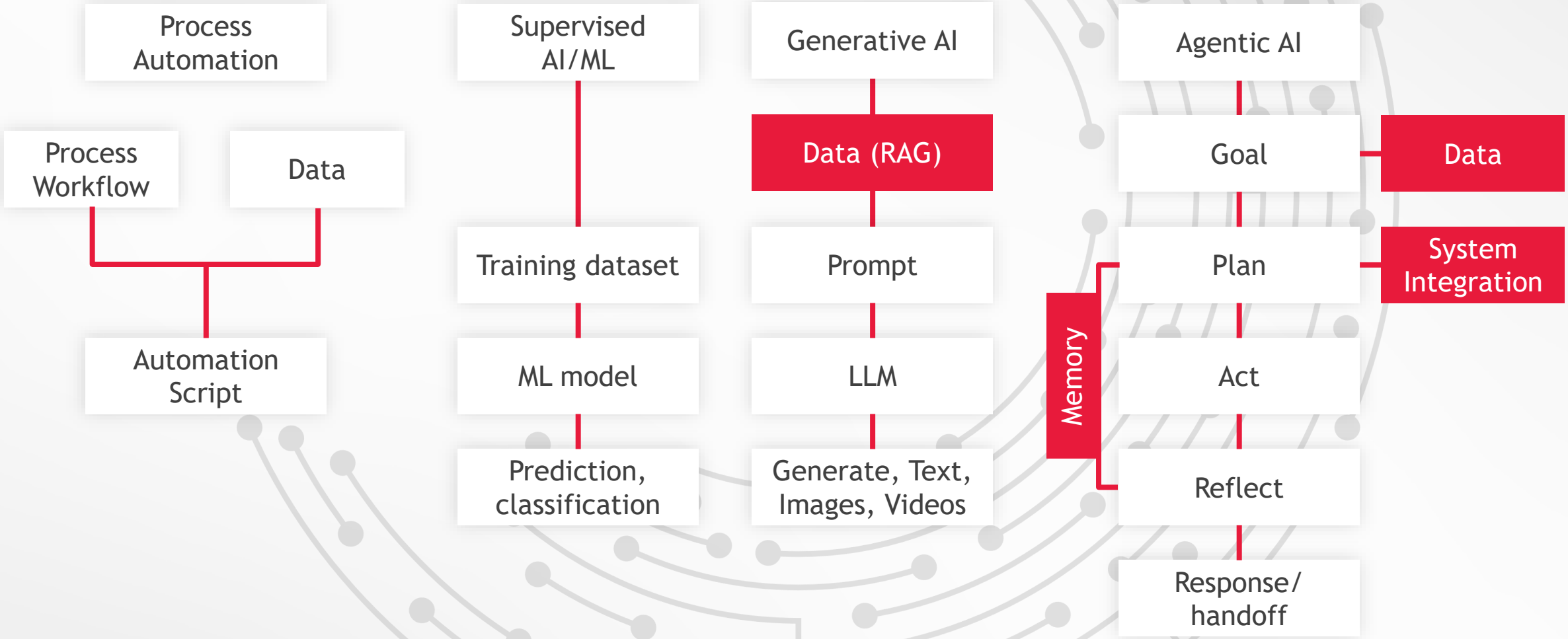


82% of leaders say they're confident they'll use digital labor to expand workforce capacity in the next 12-18 months

78% of leaders say their company is considering AI-focused roles

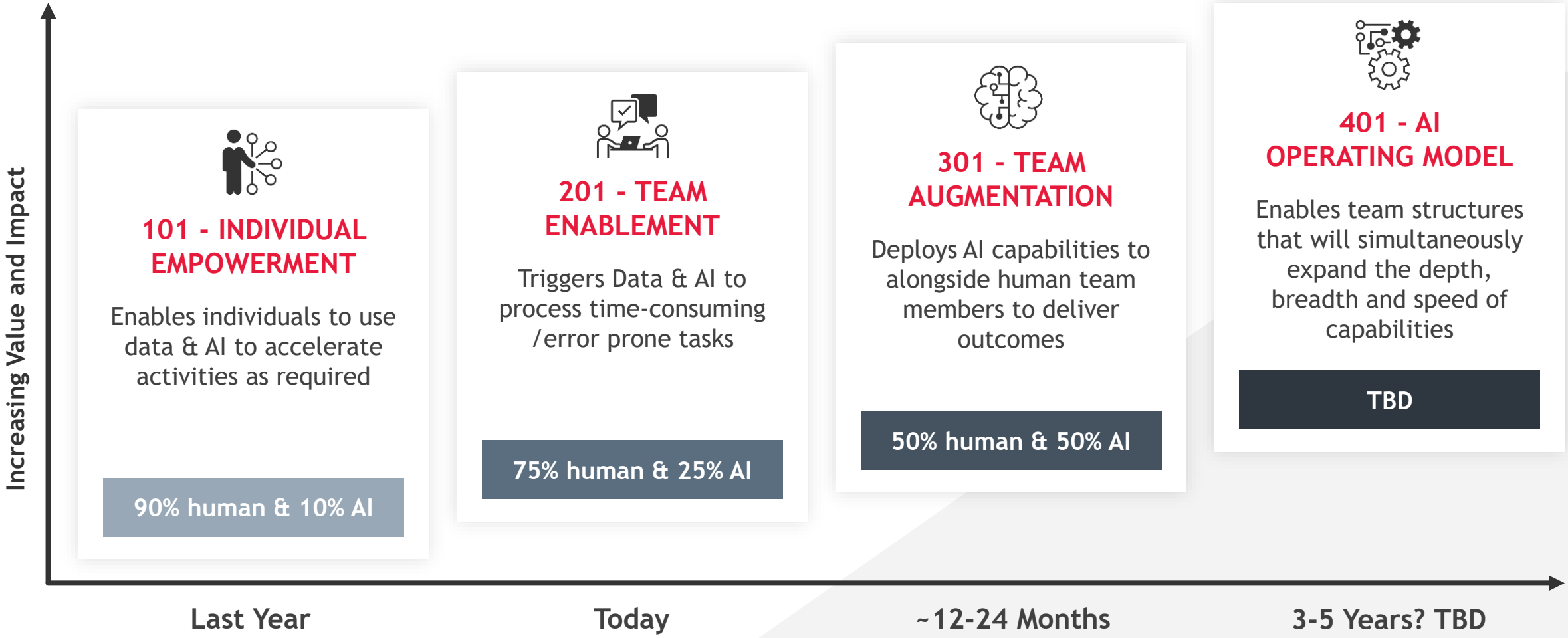
Source: 2025: The Year the Frontier Firm Is Born

Agentic AI Evolution



Evolving State of AI's Impact on Organizations

AI will undoubtedly change the division of work between humans and machines. Overtime, a greater portion of work will be completed by AI, requiring lesser and lesser, human intervention, freeing up capacity.



Framing the Future-Proof AI/Automation Operating Model

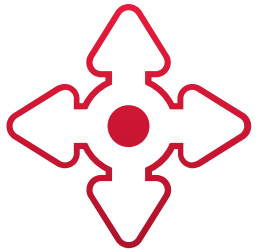
Insurance Finance at a Crossroads

Competitors are moving — delay means losing ground

The urgency is real.

82% 82% of insurance executives rank AI as a top strategic priority

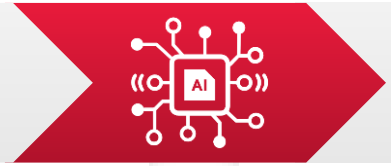
22% Yet only 22% have scaled beyond pilots



Source: Roots Automation, State of AI Adoption in Insurance 2025

From Back Office to Strategic Nerve Center

BEFORE
(today's reality)



AFTER
(with AI/automation)

- Finance teams spend weeks closing the books every month, manually reconciling spreadsheets
- Reports are mostly rear-view mirror — explaining what already happened
- Finance is often seen as a cost center — focused on controlling expenses

- The close is faster and more accurate — AI helps automate reconciliations and identify anomalies
- Finance can forecast and model ahead of time — predicting claims reserves, solvency risks, or capital needs before they become problems
- Finance shifts into a strategic role — providing insights that shape growth, pricing, and investment decisions

The Future-Proof Operating Model

Scalable — From pilots to enterprise-wide adoption

Secure — Governance, controls, explainability

Human + AI Partnership — People focus on insight, AI handles the grind

Massive Opportunities — If We Get the Risks Right

AI is redefining how insurance finance operates.

But with new power comes systemic risks:

- Financial,
- Trust, and
- Operations.

Systemic Risks in AI-Powered Audit, and Operations

Organizations Face Numerous Security Challenges When Adopting AI

FINANCE

Data security and privacy

80%+

of leaders cited leakage of sensitive data as their main concern

First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

TRUST

Shadow AI

78%

of AI users are bringing their own AI (BYOAI) to work

2024 Work Trend Index Annual Report, Microsoft and LinkedIn, May 2024, N=31,000.

OPERATIONS

New vulnerabilities and threats

77%

of orgs are somewhat concerned about indirect prompt injection attacks and 11% are extremely concerned

Gartner®, Gartner Peer Community Poll, If your org's using any virtual assistants with AI capabilities, are you concerned about indirect prompt injection attacks?

Non-compliance

55%

of leaders lack understanding of how AI is and will be regulated and are seeking guidance on how to adhere to these requirements

First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

Vulnerabilities to Manage in AI-Enabled Operations

FINANCE

1 Misaligned (Outcome Drift)

- Reserve/claims estimation drift; explainability gaps

2 Malware (Supply Chain & Model Exploitation)

- Prompt injection; tool exfiltration

TRUST

3 Misuse (Oversharing & Policy Violations)

- Sensitive data leakage; shadow agents

4 Malfeasance (Breach & Abuse)

- Agent abuse; credential attacks

OPERATIONS

5 Misconfiguration (Identity, Data, Apps)

- Over-permissive access; ungoverned connectors

6 Malfunction (Resilience & Reliability)

- Service outages; evaluation blind spots

Operations ⇔ Trust ⇔ Finance

Thrive with AI Responsibly, Safely & Confidently

Meet the AI Personas

3 Scenarios Defined in the ISO/IEC 42001 Standard for AI Management Systems

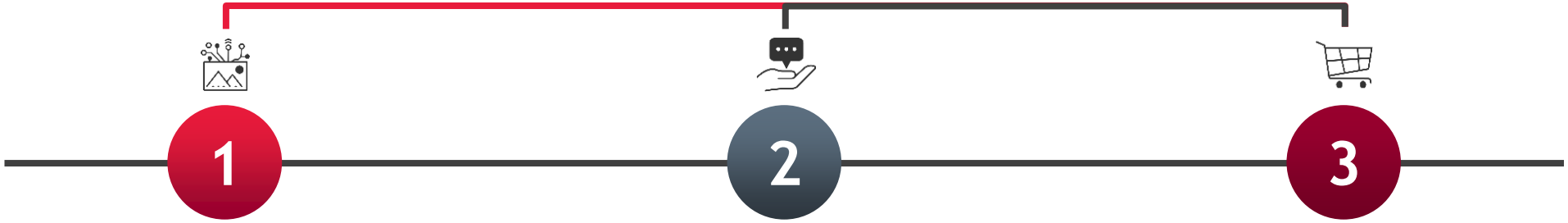
Some make AI, many deliver AI apps, and (soon) everyone consumes AI.

Producers creates & trains (or retrains) Generative AI models.

Providers operate an AI-enabled application. Providing AI presents an aggregated attack surface.

Consumers apply AI services at home, on their mobile device and at the workplace. Consumption of AI services has had record-setting adoption rates.

Examples



AI Producers:

- OpenAI (aka ChatGPT)
- Amazon - Olympus
- Google - DeepMind
- Anthropic

AI App Providers:

- Microsoft - Azure OpenAI
- AWS – Bedrock
- Google – Vertex, Gemini

Consumer AI Assistants:

- Copilot by Microsoft
- Q by Amazon
- Gemini by Google
- Claude AI by Anthropic

MEET THE AI PERSONAS

3 Scenarios Defined

Some make AI, many deliver AI apps, and (soon) everyone consumes AI.

AI Producers

Creates & trains (or retrains) Generative AI models

- OpenAI (aka ChatGPT)
- Amazon - Olympus
- Google - DeepMind
- Anthropic

AI App Providers

Operates AI-enabled applications that present an aggregate attack surface

- Microsoft - Azure OpenAI
- AWS – Bedrock
- Google – Vertex, Gemini

Consumer AI Assistants

Applies AI services at home, on their mobile device and at the workplace, Copilot by Microsoft

- Q by Amazon
- Gemini by Google
- Claude AI by Anthropic

Consumption has had record-setting adoption rates.

SOURCE: ISO/IEC 42001 Standard for AI Management Systems

Thriving with AI Across Personas

PRODUCER

Produce Trustworthy AI

- Transparent & explainable inference & outputs
- Verifiable controls for bias, fairness, and response drift
- Compliance with applicable regulations and standards

PROVIDER

Provide AI Safely

- Harden identity for humans, workloads, and agents
- Data protection to prevent oversharing
- Abuse prevention for prompts and responses
- Compliance audit trails

CONSUMER

Use AI Responsibly

- Usage policy, training, and monitoring
- DLP to prevent oversharing
- Audit & retention
- Human-in-the-loop workflows for decisions

Real-World Patterns

What To Embrace vs. Avoid

Top Security and Governance Concerns About Generative AI

Data oversharing and data leaks

80%

of leaders cited leakage of sensitive data as their main concern

First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

Identification of risky AI use

41%

of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement

Microsoft data security index 2024 report

AI governance and risk visibility

84%

Want to feel more confident about managing and discovering data input into AI apps and tools

Microsoft data security index 2024 report

What to Embrace

Grounded In Approved Data

- **Why it matters:** Ensures AI responses are accurate, relevant, and compliant by pulling from your organization's trusted data sources
- **Benefit:** Reduces hallucinations, improves confidence, and keeps outputs aligned with business policies

Human-in-the-Loop for High-Impact Finance & Claims Decisions

- **Why it matters:** Critical decisions require human oversight to maintain accountability and trust
- **Benefit:** Combines AI speed with human judgment for accuracy, compliance, and risk mitigation

Guardrails: Input/Output Filtering, Kill-Switches, Canary Prompts

- **Why it matters:** Protects against misuse, bias, and harmful outputs while ensuring ethical AI use
- **Benefit:** Builds trust and safety into every interaction, reducing operational and reputational risk

What to Avoid

Overshared Data or Legacy Permissions

- **Why it's risky:** Broad or outdated access controls can expose sensitive data and create compliance gaps
- **Impact:** Increases the risk of data leakage, regulatory violations, and reputational harm

Unvetted Agents with Access to Customer Data

- **Why it's risky:** External tools without proper vetting can introduce vulnerabilities and compromise customer trust
- **Impact:** Potential for data breaches, IP loss, and non-compliance with privacy regulations

Opaque Models Driving Financial Estimates

- **Why it's risky:** Black-box models can produce inaccurate or biased outputs without accountability
- **Impact:** Leads to flawed financial decisions, audit failures, and erosion of stakeholder confidence

Securing Customer-Facing AI Experiences

Securing Customer-Facing AI Experiences

Content safety & abuse prevention

- Rate limiting
- Session isolation

Disclose for transparent UX

- Provide dispute/appeal channel and human escalation

Continuous monitoring

- Include AI takedown/rollback playbooks

Lean into Recognized Frameworks

Audit-friendly framework:

- NIST AI Risk Management Framework
- Govern, Map, Measure, Manage

Trust-centric framework:

- Gartner MOST
- Model, Operations, Security, Trust

Trust-security standards:

- OWASP Top 10 for LLMs
- MITRE ATLAS for adversary behaviors

What's in your (governance) wallet?

Insurance Scenarios

FINANCE, AUDIT, CLAIMS

Close acceleration with AI-assisted reconciliations

- Establish & audit segregation of duties
- Review reasoning traces

Claims triage & fraud detection

- Bias testing
- Adverse action handling
- Drift alarms

Regulatory reporting aides

- Evidence capture
- Approval workflow
- Retention

Board & Compliance Implications

From the Boardroom to Compliance

Board-level AI risk **dashboards** & thresholds

Model risk **policy** aligned to OCC/SOX expectations

Independent testing, challenge, **audit** readiness

Measuring Readiness and Effectiveness

Coverage

- % AI use cases registered & reviewed
- % models with evaluation gates

Exposure

- # overshared containers remediated
- Privileged/agent identities reduced

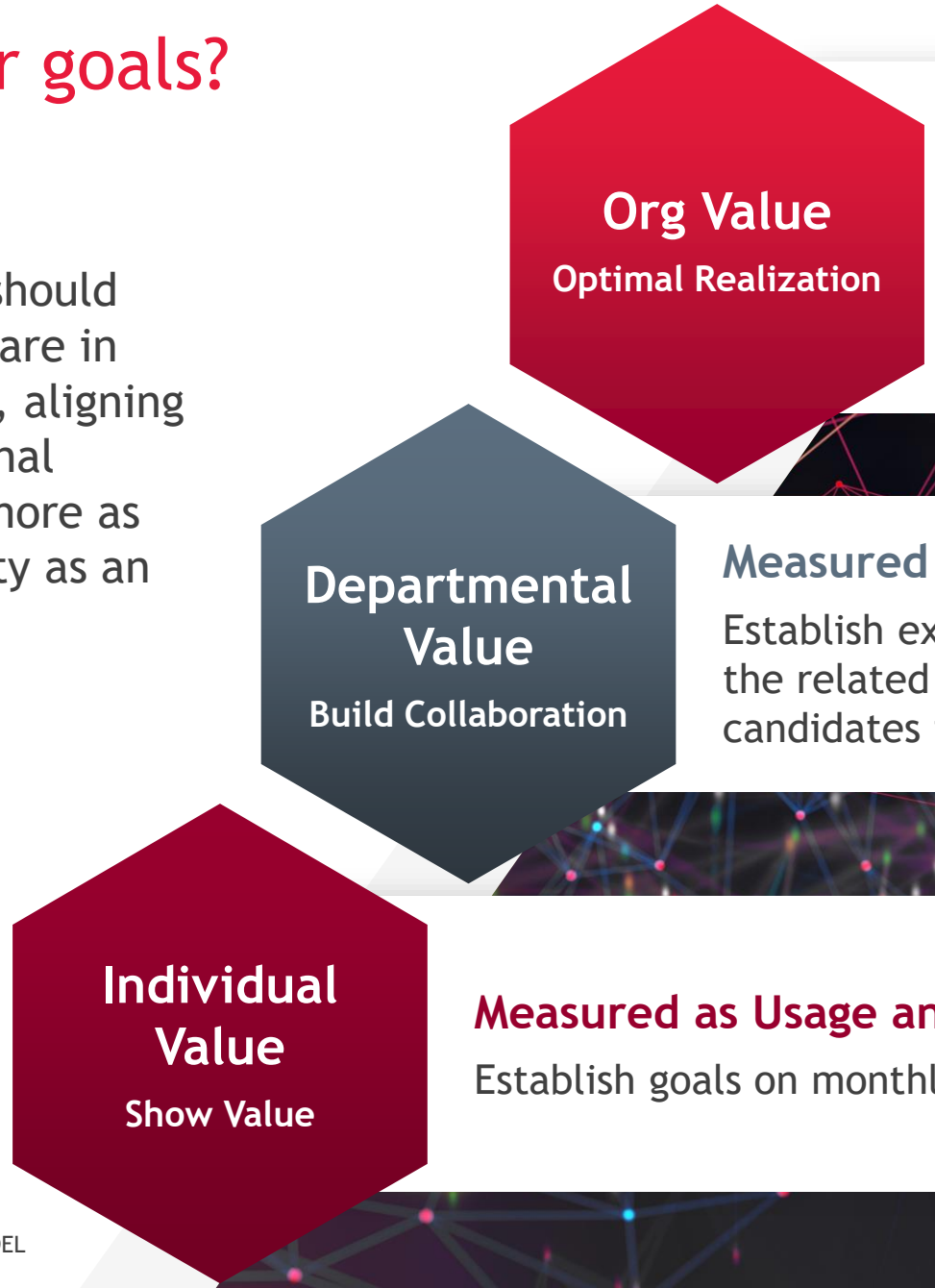
Resilience

- Mean time to detect/ respond to AI incidents
- Red-team findings closed

30-60-90 Day Action Plan

What are our goals?

Measuring success should align to where you are in your usage journey, aligning to your organizational metrics more and more as you grow in maturity as an AI organization.



Measured as Revenue Gains and Cost Reductions

Use your highest-level success metrics to measure success (e.g., supply chain costs, sales revenue, development costs, etc.)

Measured as KPIs

Establish expectations of use, and set goals on the related KPIs (e.g., leads pursued for Sales, candidates interviewed for HR, etc.)

Measured as Usage and Time Savings

Establish goals on monthly active usage (MAU)

Your 30-60-90 Day Plan

BY ISO PERSONA

DAYS 1-30 — Inventory and Stabilize

- **USE AI RESPONSIBLY**: publish policy & acceptable use; stand up usage logging
- **PROVIDE AI SAFELY**: identity hygiene; remediate oversharing
- **PRODUCE TRUSTWORTHY AI**: seed model/use-case registry

DAYS 31-60 — Govern and Protect

- **USE AI RESPONSIBLY**: training; escalation & exception process
- **PROVIDE AI SAFELY**: DLP/IRM baselines; incident playbooks
- **PRODUCE TRUSTWORTHY AI**: baseline evaluations; begin red teaming

DAYS 61-90 — Prove and Scale

- **USE AI RESPONSIBLY**: board reporting; KRIs
- **PROVIDE AI SAFELY**: pilot with guardrails; SIEM/XDR signals
- **PRODUCE TRUSTWORTHY AI**: evaluation SLOs; lessons learned

Resources

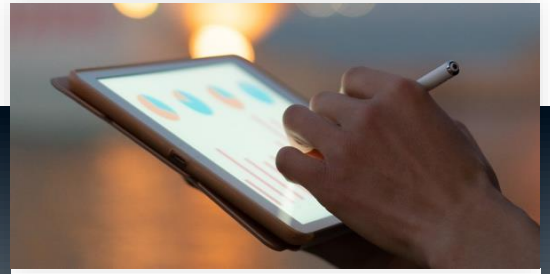
Resources

Get Started with

AI Cybersecurity

- NIST AI Risk Management Framework
- Microsoft shared responsibility models for AI services
- Gartner MOST
- OWASP Top 10 for LLMs

Unleashing the Power of AI with Microsoft Copilot



The Practical Guide to AI

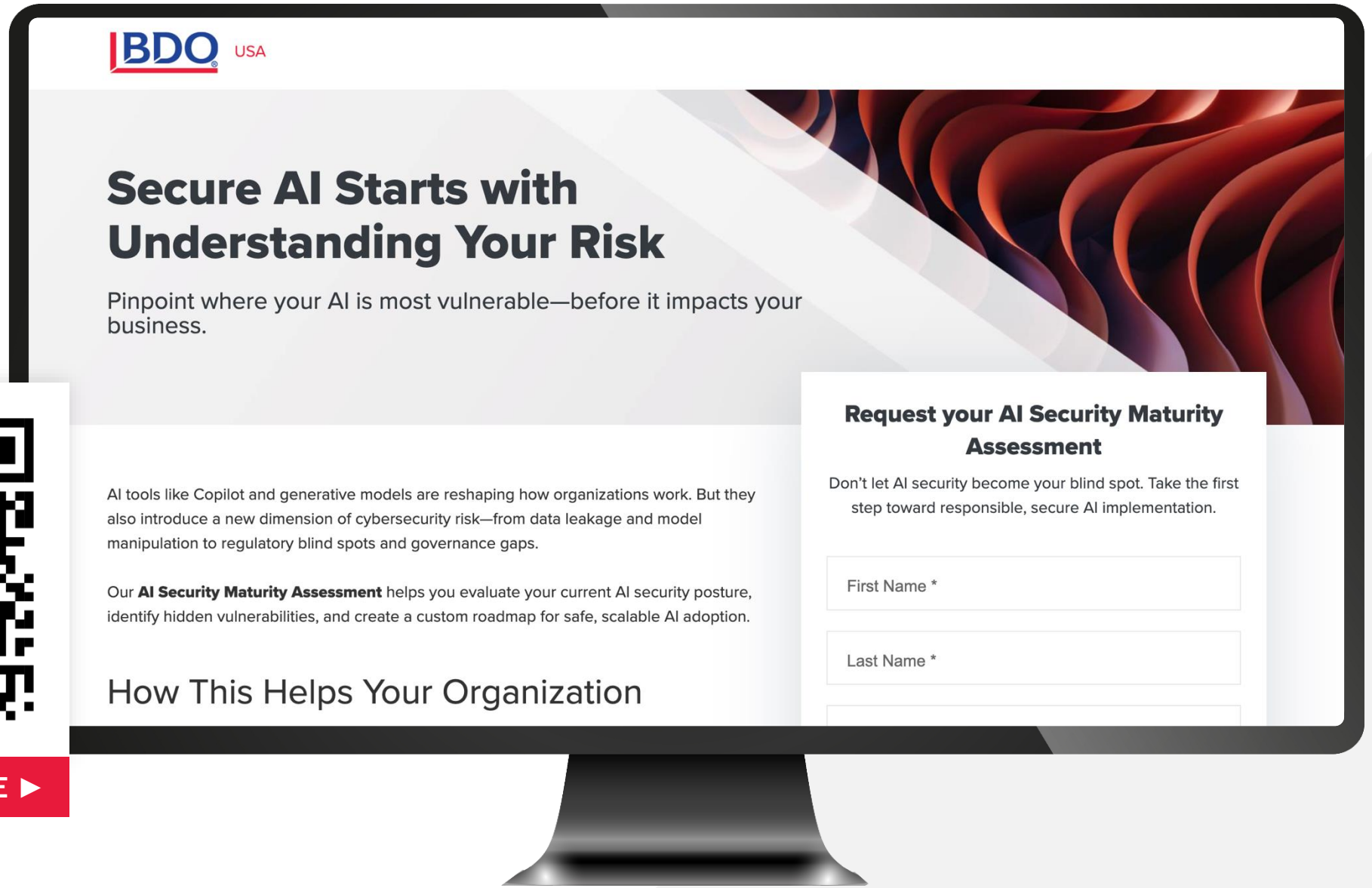
Copilot and Coffee Webseries

Data Security: A Key Component of Your Copilot Journey

Unlock Copilot with Purview Data Security and BDO

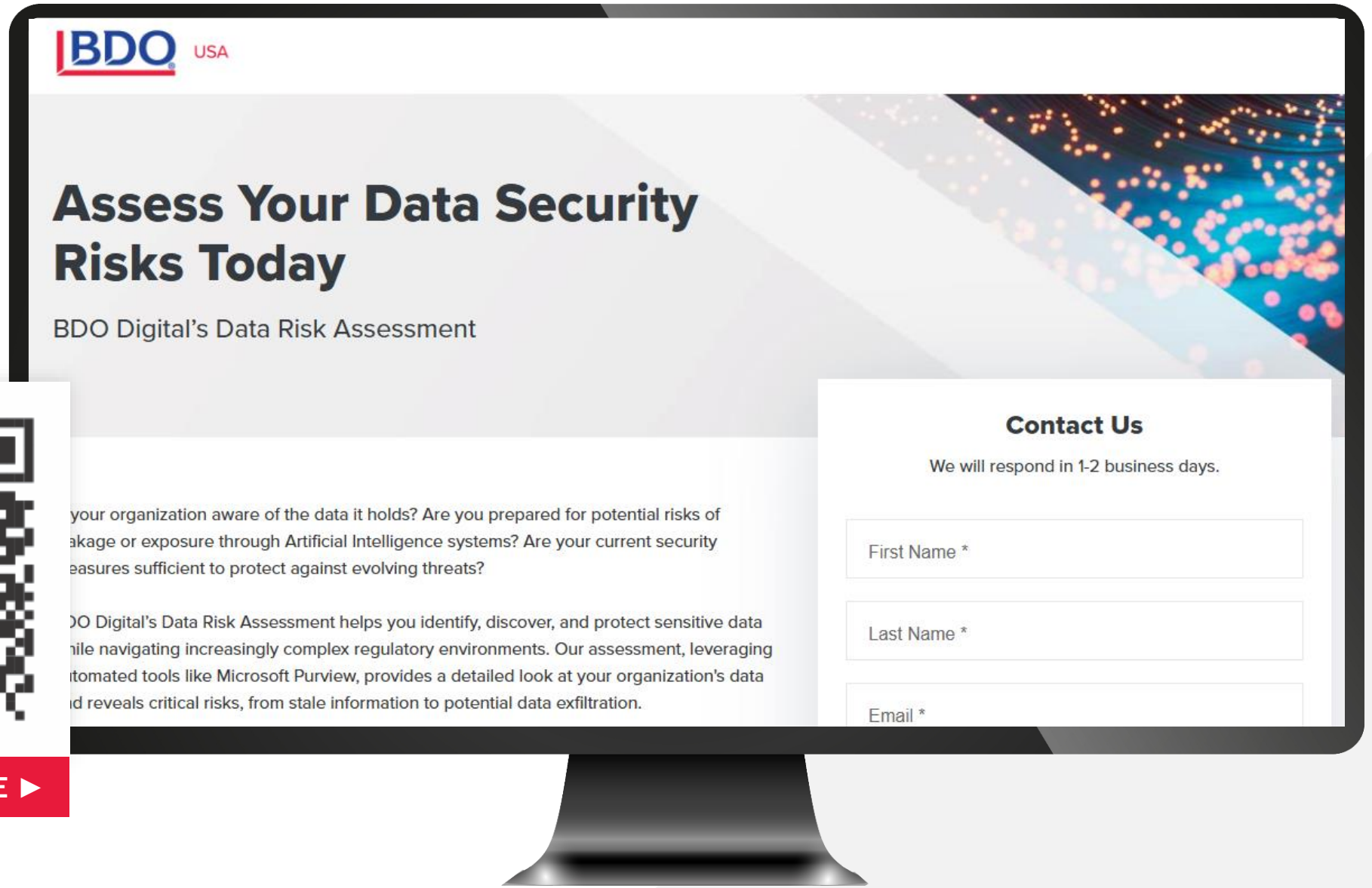
Digital Risk Management Toolkit

AI Security Assessment & Insights



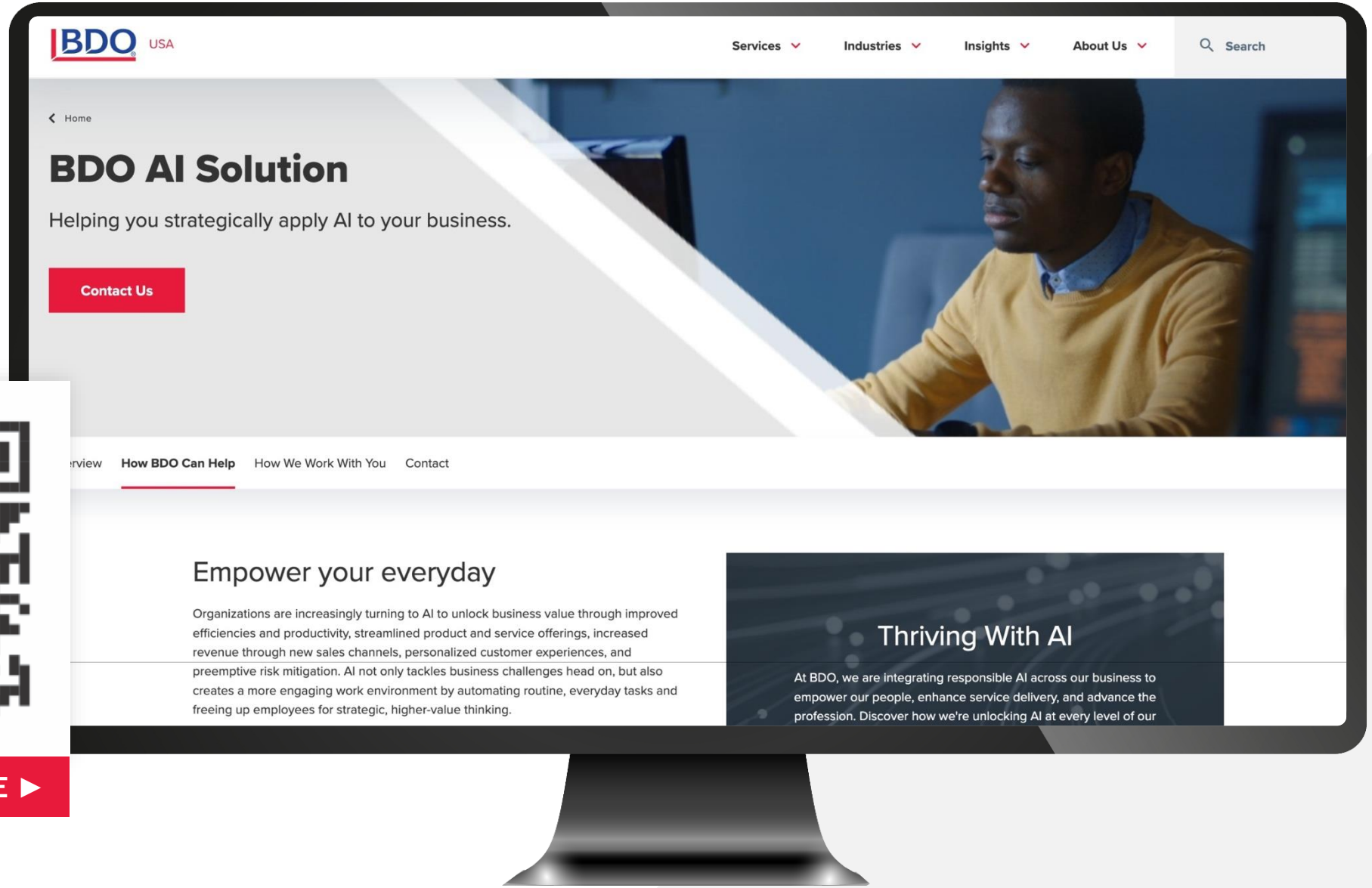
SCAN TO LEARN MORE ▶

AI Data Security QuickStart

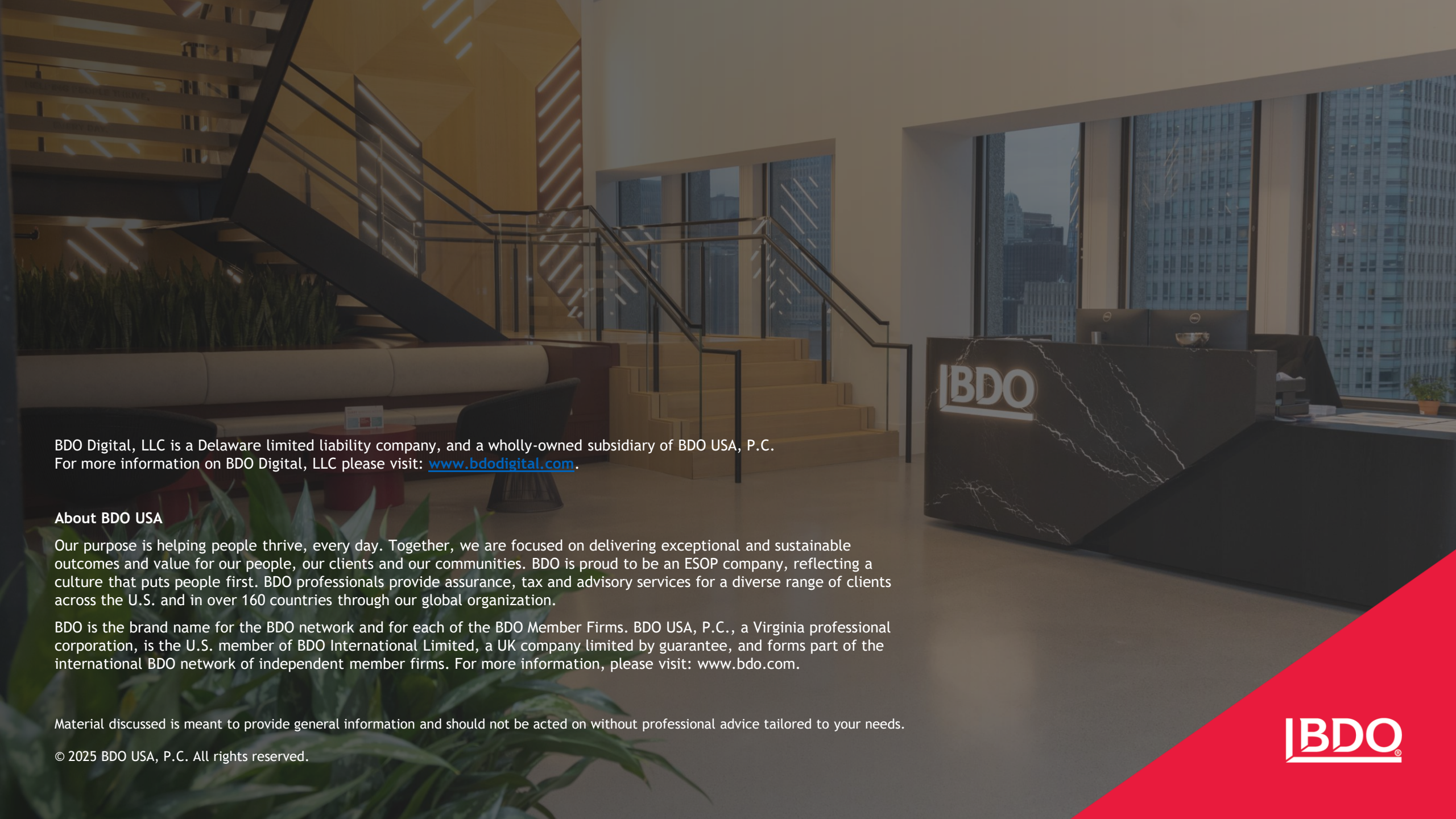


SCAN TO LEARN MORE ▶

Agentic Readiness



SCAN TO LEARN MORE ▶



BDO Digital, LLC is a Delaware limited liability company, and a wholly-owned subsidiary of BDO USA, P.C.
For more information on BDO Digital, LLC please visit: www.bdodigital.com.

About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.