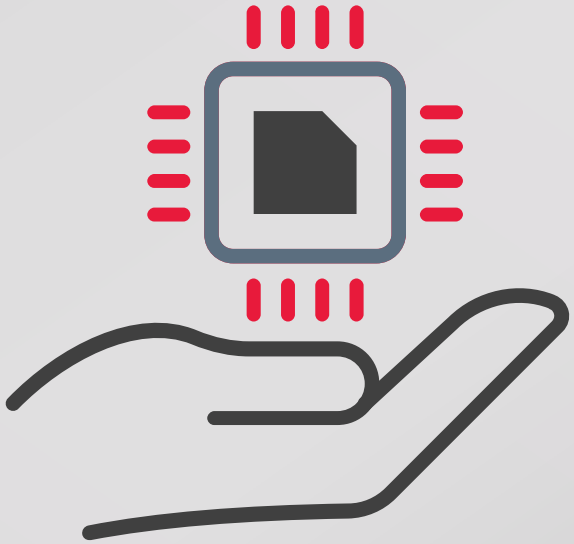
AI Governance and Compliance By Design



NOVEMBER 2024

Agenda

Security and Trust as a Feature

Role of the Board

Key AI Risks and Controls

Governance as a Culture

VARUN PRASAD
Third Party Attestation
Managing Director

415-490-3050
vprasad@bdo.com

About Me

- 15+ years of IT Audits, Risk Management and Compliance reviews
- Focused on tech, cloud security and privacy assessments
- SOC 2 and ISO audits for SaaS & PaaS companies
- Building Trust in AI
- Vice President of SF ISACA chapter & other ISACA WGs

ISACA Articles

- Cybersecurity Risk of AI-Based Applications Demystified – April 2024
- AI Algorithm Audits: Key Control Considerations – August 2024

Security vs. Compliance

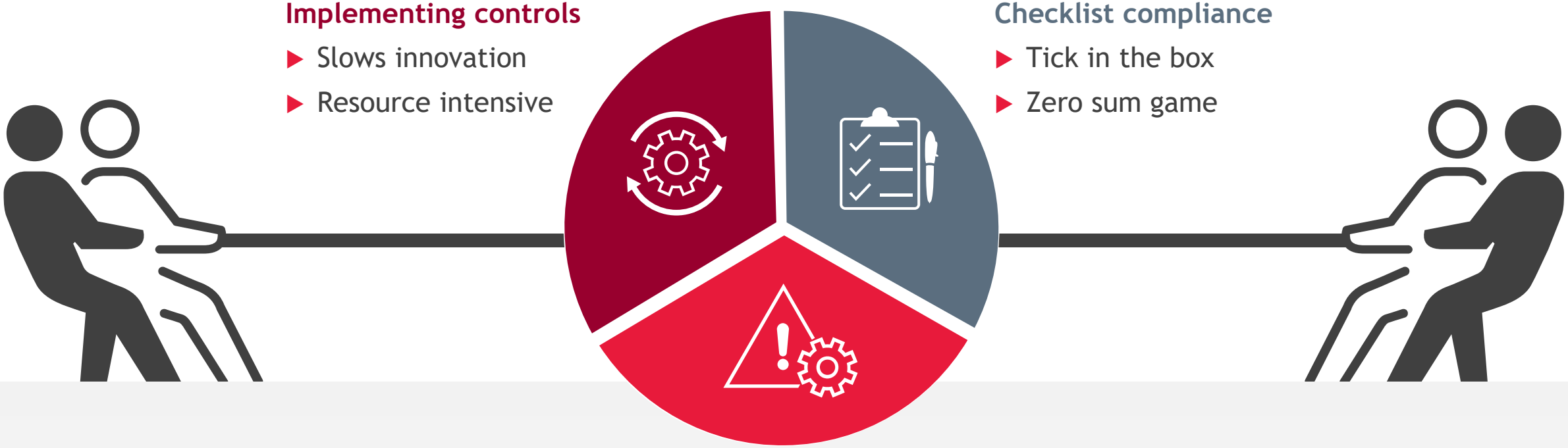
A VICIOUS CIRCLE

Implementing controls

- Slows innovation
- Resource intensive

Checklist compliance

- Tick in the box
- Zero sum game



Baking in controls

- Poor design
- Unauditable controls

Trust as a Feature

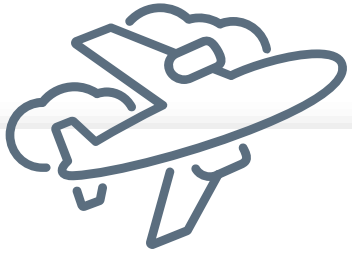
- Build compliance as a product feature
- Key differentiator in the GTM strategy
- Consumers prefer trust
- Positive compliance posture drives revenue
- Cross-functional organizational initiative
- Governance as a culture

Why should boards care?

AI Does Fail!

ZILLOW

- Zestimate algorithm failed
- ‘Zillow Offers’ shut down
- Zillow posted huge losses



AIR CANADA

- Chatbot provided incorrect info to customer
- Airline paid compensation and damages

TRIVAGO

- ACCC vs. Trivago
- Misled customers to book hotels with higher commission
- Paid ~$44M penalties

Wave of Regulations

EU AI Act

U.S. Presidential EO

Colorado AI Act

ISO 42001

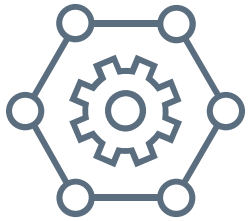
U.S. Federal Law
AI Accountability Act

Source: IAPP Research and Insights

Role of the Board

Define Boundaries

- Potential uses for AI
- Dos and don’ts
- Establish principles for AI



AI Risk Management

- Establish risk management framework.
- Approve risk tolerances
- Review methodology

Heightened Awareness

- Be informed about AI
- Review board composition
- Knowledge of regulatory landscape.

Provide Resources

- Develop AI governance function
- Review IT resource needs
- Specialized tooling

Monitor and Review

- Residual risks
- KPIs
- Compliance results

Key Risks and Controls For AI Systems

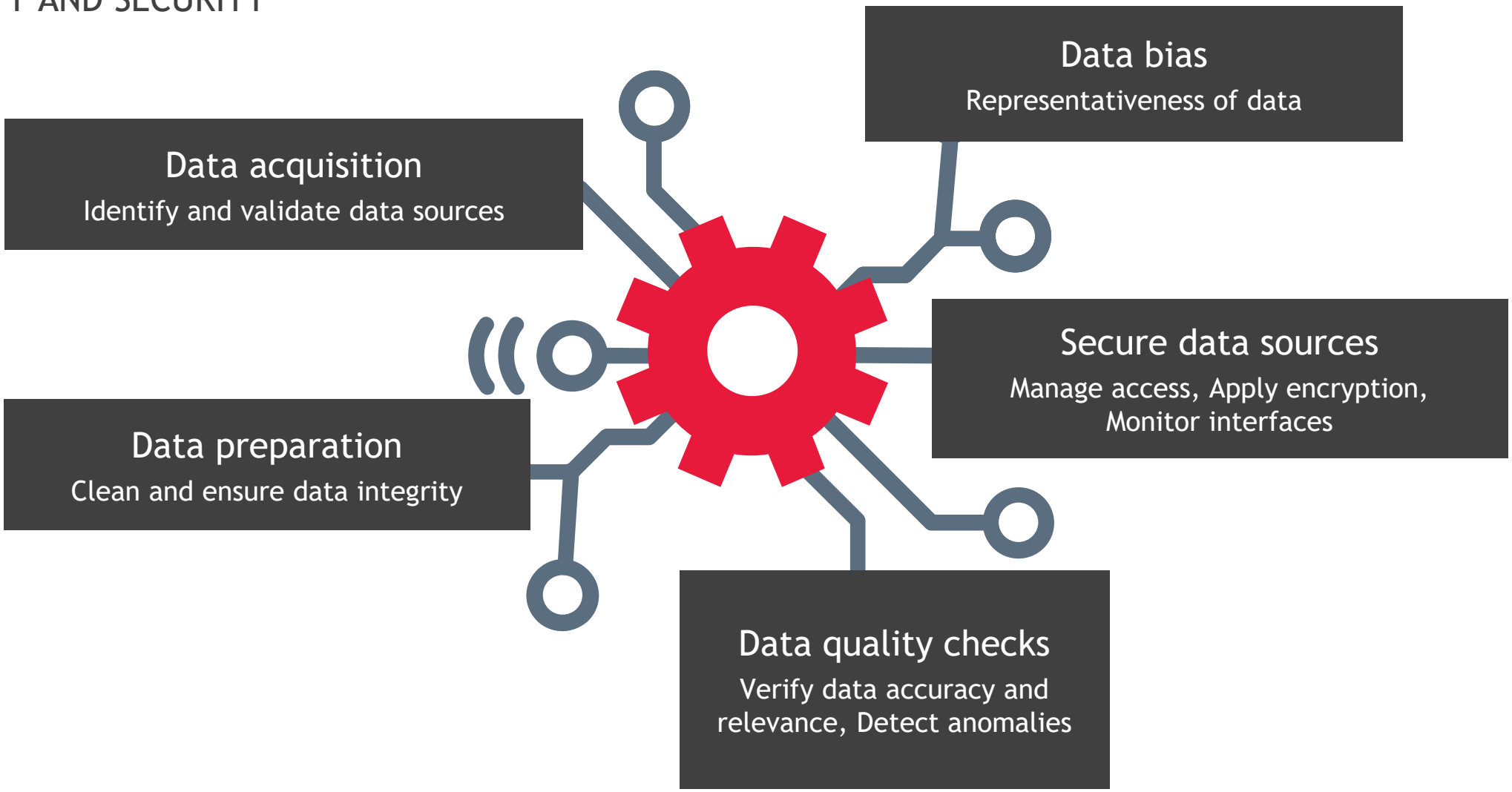

Responsible AI
AI Risk Management
Enhanced Policies
Model Development and Monitoring
Data Governance

Data Risks For AI Systems

DATA MANAGEMENT

Key Controls For Data Management

SAFETY AND SECURITY



Privacy-First Approach

Consent for specific use case

Data provenance/logging

Secure data processing
Use of PETs/Differential privacy

Data retention/deletion

Track and process opt-outs

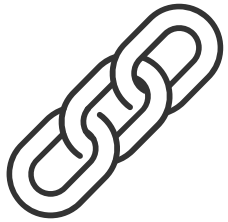
Model Development Lifecycle Process Risks

Incorrect Design

Insufficient Testing

Unauthorized Deployments

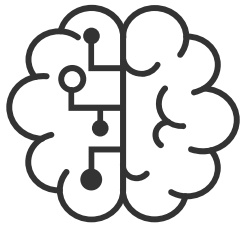
Application Security



ML Supply Chain

Model Development – Key Controls

DESIGN AND DEVELOP

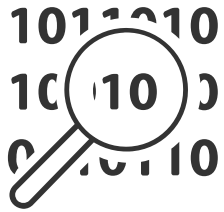


Robust Design

- Meet AI objectives
- Use ensemblies
- Watermarking
- Enable logging

Model Training

- Randomized data
- Regularization
- Retraining



Secure Coding

- Input validation
- Output handling
- API/Plugin security

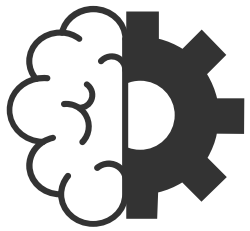
Supply Chain Security

- Scanning libraries
- SAST & DAST

Sandboxing

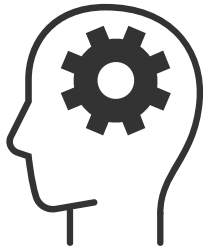
Model Verification and Validation Techniques

MODEL V&V



Model Accuracy and Robustness

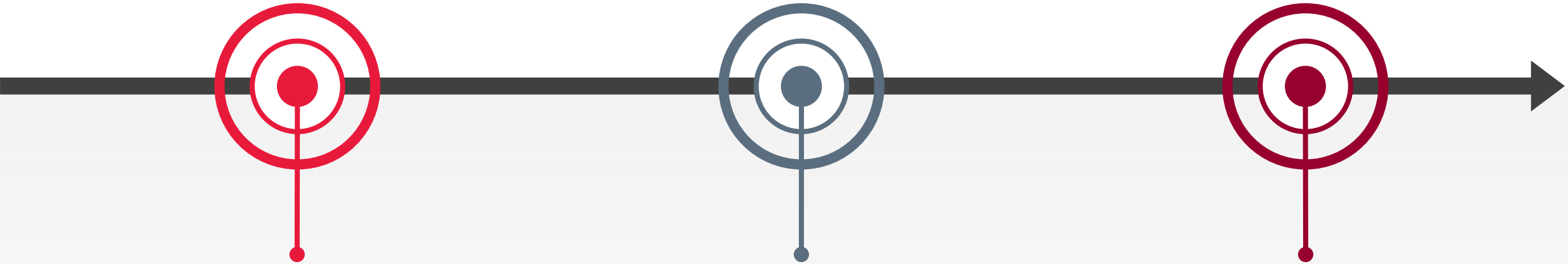
Adversarial Testing



Unfairness Testing

Red Teaming

Model Deployment Controls



Deployment Strategy

Identify and document deployment plan

(Canary, A/B, Static, Shadow)

Deployment requirements

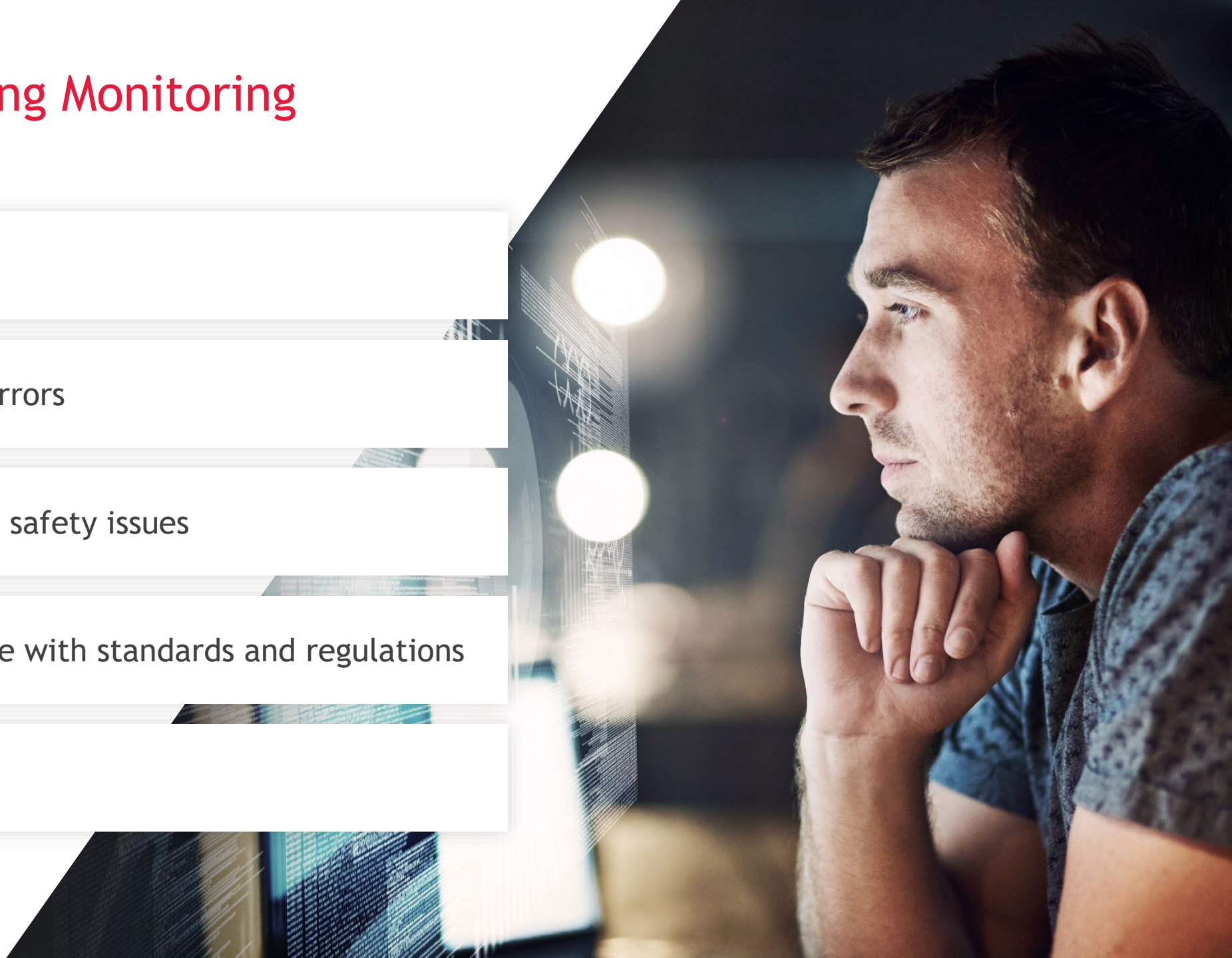
Define go/no-go conditions and checklist of testing results

Authorized approvals

Human oversight

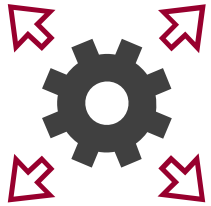
The Need For Strong Monitoring

- Track performance
- Identify potential errors
- Detect security and safety issues
- Maintain compliance with standards and regulations
- Avoid incidents

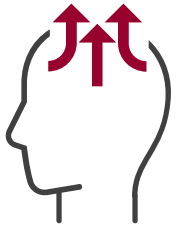


Model Deployment Pointers

Performance

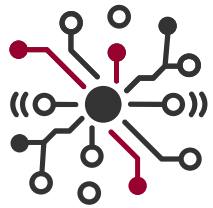


Drift



Bias

Explainability



Data

Security

Governance as a Culture

AI in the Board Agenda

CONTINUOUS OVERSIGHT

Metrics review

Effectiveness of controls

AI Use Cases

Applicable laws and regulations

Risk assessments update

Status of residual risks

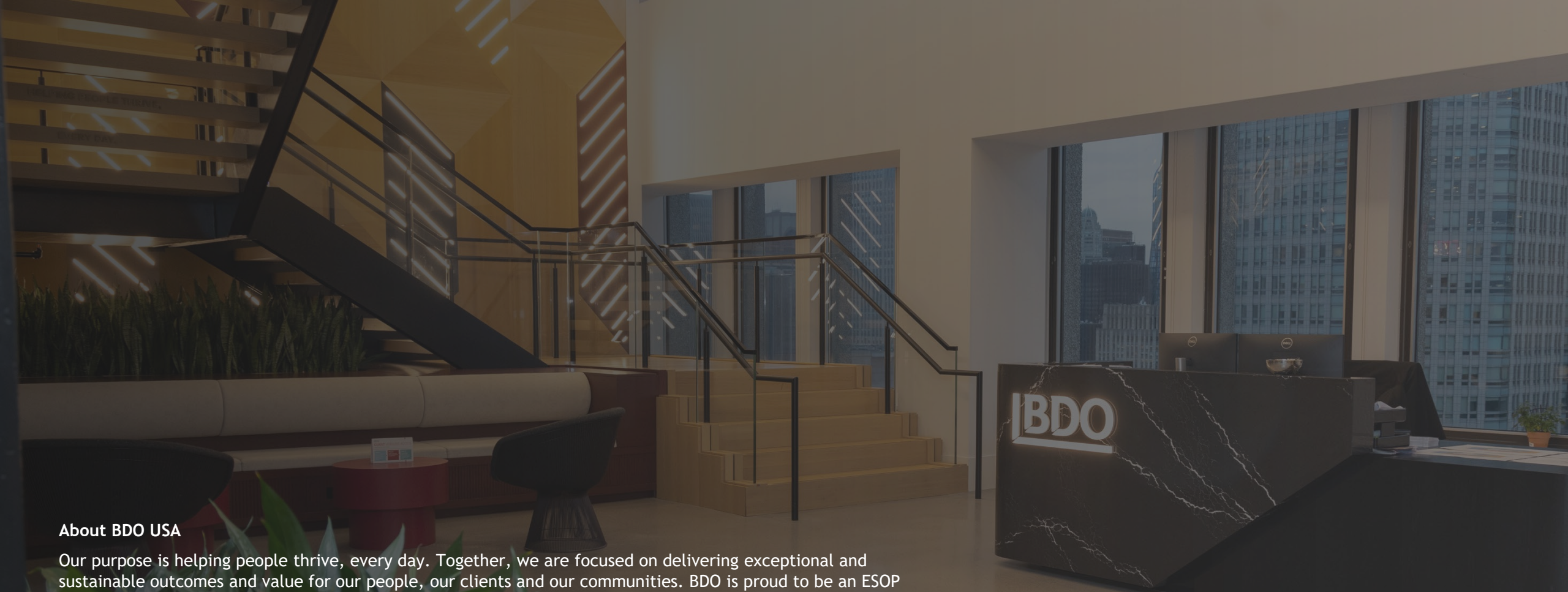
AI Governance Must-Haves

- [ ] Model inventory
- [ ] Comprehensive risk assessments
- [ ] Strong data governance processes
- [ ] Defined verification and validation steps
- [ ] Monitoring and detection

Thank you and Stay Connected!

VARUN PRASAD
Third Party Attestation
Managing Director

415-490-3050
vprasad@bdo.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.