DTE-I Governance Self-Assessment Checklist

Digital Trust Ethics - Islamic-Inspired Framework

Organizational Governance Maturity Assessment

Document Information

- Version: 1.0
- Date: August 2025
- Author & Owner: Abed Al Rahman Naboulsi, CISSP / DTE-I Framework Initiative
- Validity: 12 months from assessment date

Foreword by the Author

Dear Reader,

It is with immense dedication and foresight that I present this Digital Trust Ethics - Islamic-Inspired Framework (DTE-I) Governance Self-Assessment Checklist. As the author and architect behind the DTE-I Framework, my core objective is to bridge the critical gap between technological advancement and ethical governance in our rapidly evolving digital landscape, with a particular focus on Artificial Intelligence.

This checklist is not merely a theoretical exercise; it is a practical, actionable tool designed to empower organizations to objectively measure their maturity in integrating crucial ethical considerations into their cybersecurity and AI governance strategies. This is a foundational step in a broader series of tools aimed at fostering a more human-centric, trustworthy, and ethically sound digital future for all.

I encourage you to utilize this tool diligently, engaging multiple stakeholders within your organization to gain a comprehensive understanding of your current posture. Your commitment to this assessment is a vital contribution to building a global model that harmoniously balances innovation with humanity.

Sincerely,

Abed Al Rahman Naboulsi, CISSP

Founder & Author, DTE-I Framework

https://www.linkedin.com/in/abed-al-rahman-naboulsi/

ASSESSMENT INSTRUCTIONS

Rating Scale:

- **0 = Not Implemented:** No formal process or control exists
- **1 = Ad-hoc:** Informal practices exist but lack documentation or consistency
- **2 = Defined:** Formal processes documented and generally followed
- **3 = Optimized:** Mature processes with continuous improvement and measurement

Completion Guidelines:

1. Involve multiple stakeholders (IT, Legal, Risk, HR) for comprehensive assessment
2. Provide evidence or examples for ratings of 2 or 3
3. Use "N/A" only when the control is genuinely not applicable to your organization
4. Complete all sections for accurate maturity scoring

GOVERNANCE & ACCOUNTABILITY ASSESSMENT

1. Risk Ownership Structure

Assessment Item: Designated risk owners for cybersecurity and AI ethics risks

What this means: Clear assignment of cybersecurity and AI ethics risk ownership to specific individuals with appropriate authority, accountability, and resources to manage these risks effectively.

Evidence to look for:

- Named CISO or equivalent for cybersecurity risks
- Designated AI Ethics Officer or equivalent role
- Job descriptions including risk management responsibilities
- Clear escalation paths for risk-related decisions
- Regular risk owner meetings and reporting

Frameworks alignment: ISO 27001 (Leadership), NIST CSF 2.0 (Govern), EU AI Act (Governance)

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

2. Risk Appetite Documentation

Assessment Item: Documented risk appetite statement for digital trust and AI ethics

What this means: Formal, board-approved statements defining the organization's willingness to accept specific types and levels of digital and AI-related risks, including quantified thresholds where possible.

Evidence to look for:

- Written risk appetite statements approved by senior management
- Quantified risk tolerance levels (e.g., "Accept up to 5% bias variance in AI decisions")
- Regular review and update of risk appetite based on business changes
- Communication of risk appetite to relevant staff
- Decision-making alignment with stated risk appetite

Frameworks alignment: ISO 27001 (Risk Management), NIST CSF 2.0 (Govern-Risk Strategy), EU AI Act (Risk Management System)

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

3. Ethical Decision Documentation

Assessment Item: Ethical decision-making processes and their records are maintained

What this means: Systematic documentation of ethical decisions, especially when technical controls conflict or when AI systems impact individuals, including the rationale, alternatives considered, and approval process.

Evidence to look for:

- Decision log or register for ethical choices
- Documentation of trade-off decisions (e.g., privacy vs. security)
- Ethics committee or review board meeting minutes
- Stakeholder consultation records for significant decisions
- Post-decision review and learning processes

Frameworks alignment: NIST CSF 2.0 (Govern), EU AI Act (Quality Management), Ethics-by-Design principles

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

4. Training and Competency

Assessment Item: Regular training programs on cybersecurity and AI ethics for all relevant personnel

What this means: Structured, ongoing education ensuring staff understand both technical cybersecurity requirements and ethical implications of technology decisions, with competency verification and role-specific content.

Evidence to look for:

- Annual cybersecurity awareness training with completion tracking
- Role-specific AI ethics training for developers, data scientists, product managers
- Competency assessments and certification requirements
- Training content updates reflecting current threats and regulations
- Ethics scenario-based training and decision-making exercises

Frameworks alignment: ISO 27001 (Human Resources Security), NIST CSF 2.0 (Govern-Workforce), EU AI Act (Personnel Competency)

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

5. Organizational Structure Clarity

Assessment Item: Clearly defined RACI matrix for security and AI governance roles

What this means: Documented responsibility assignment matrix clearly defining who is Responsible, Accountable, Consulted, and Informed for cybersecurity and AI governance activities across the organization.

Evidence to look for:

- RACI matrix covering key cybersecurity processes (incident response, risk assessment, policy approval)
- RACI matrix for AI governance (model approval, bias testing, ethical review)
- Regular review and update of role assignments
- Clear escalation paths and decision rights

- Communication of roles to all relevant stakeholders

Frameworks alignment: ISO 27001 (Organization of Information Security), NIST CSF 2.0 (Govern-Roles), EU AI Act (Quality Management)

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

6. Regulatory Compliance Tracking

Assessment Item: Tracking of EU AI Act obligations for high-risk AI systems

What this means: Systematic identification, classification, and compliance monitoring for AI systems that fall under EU AI Act high-risk categories, with documented compliance measures and regular assessments.

Evidence to look for:

- Inventory of AI systems with risk classification
- Compliance gap analysis for high-risk systems
- Implementation plan for EU AI Act requirements
- Regular compliance status reporting
- Documentation of conformity assessment procedures

Frameworks alignment: EU AI Act (High-Risk AI Systems), ISO/IEC 23053 (AI Risk Management), NIST AI RMF

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

7. Conflict of Interest Management

Assessment Item: Regular review of potential conflicts of interest in AI development and deployment

What this means: Proactive identification and management of situations where personal, financial, or professional interests might compromise objective decision-making in AI development, deployment, or governance.

Evidence to look for:

- Conflict of interest disclosure processes for AI team members
- Regular review of vendor relationships and financial interests
- Ethical review of AI partnerships and data sharing agreements
- Clear policies on personal AI system usage and development
- Whistleblower or ethics reporting mechanisms

Frameworks alignment: Corporate governance standards, EU AI Act (Quality Management), Professional ethics codes

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

---

8. Executive Oversight and Reporting

Assessment Item: Board-level reporting on digital trust and AI ethics posture

What this means: Regular, structured reporting to board of directors or senior executive committee on the organization's cybersecurity and AI ethics performance, risks, and strategic decisions.

Evidence to look for:

- Regular board reports on cybersecurity and AI ethics (at least quarterly)
- KPI dashboards for digital trust metrics
- Executive briefings on emerging AI regulations and their impact
- Board involvement in major AI ethics decisions
- Documentation of board oversight activities and decisions

Frameworks alignment: ISO 27001 (Management Review), NIST CSF 2.0 (Govern-Strategy), Corporate governance principles

Rating: ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N/A

Comments/Evidence:

SCORING SUMMARY

Individual Scores:

1. Risk Ownership: ___/3
2. Risk Appetite: ___/3
3. Ethical Decisions: ___/3
4. Training Programs: ___/3
5. RACI Matrix: ___/3
6. Regulatory Tracking: ___/3
7. Conflict Management: ___/3
8. Executive Reporting: ___/3

Total Score: ___/24

Governance Maturity Percentage: ___% (Total ÷ 24 × 100)

Maturity Level:

- **0-25%:** Initial - Ad-hoc practices with significant gaps
- **26-50%:** Developing - Some formal processes but inconsistent implementation
- **51-75%:** Defined - Systematic approach with room for optimization
- **76-100%:** Optimized - Mature governance with continuous improvement

---

RECOMMENDED NEXT STEPS

Based on your assessment results:

For scores 0-25% (Initial):

1. Establish basic governance structure with named risk owners
2. Develop initial risk appetite statements
3. Implement basic training programs
4. Create simple decision documentation process

For scores 26-50% (Developing):

1. Formalize existing ad-hoc processes
2. Implement regular review and update cycles
3. Enhance training with role-specific content
4. Establish KPI measurement and reporting

For scores 51-75% (Defined):

1. Implement continuous improvement processes
2. Enhance automation and measurement capabilities
3. Expand stakeholder engagement and communication

4. Develop advanced analytics and predictive capabilities

For scores 76-100% (Optimized):

1. Share best practices with industry peers
2. Contribute to standards development
3. Explore emerging technologies and regulations
4. Mentor other organizations in their digital trust journey

Assessment Completed By:

Name: _____

Title: _____

Date: _____

Signature: _____

Quality Review:

Reviewer Name: _____

Title: _____

Date: _____

Signature: _____

DISCLAIMER: This assessment tool is provided for educational and self-evaluation purposes. It does not constitute legal advice or guarantee compliance with any specific regulations. Organizations should consult with qualified legal and technical professionals for compliance guidance specific to their jurisdiction and circumstances.