Digital Accessibility in InfoSec Risk Assessment Questionnaire

SECURING ACCESSIBILITY
moregood solutions

1. Asset Identification

Digital Assets and Systems:

List all websites used by the organization.

List all software applications, both internal and external. List all databases that store sensitive information.

List all communication tools (e.g., email, video conferencing used by the organization.

Identify any systems that store, process, or transmit personal data.

2. Compliance Evaluation

Accessibility Compliance Checks:

Are the organization's websites compliant with WCAG 2.1 standards?

Are the organization's software applications compatible with screen readers and other assistive technologies?

Are all digital documents (e.g., PDFs, Word documents) accessible (e.g., tagged PDFs, alternative text for images)?

Are communication tools equipped with accessibility features (e.g., captioning, sign language interpretation)?

Is email formatted to be compatible with screen readers?

3. Risk Identification

Identified Risks:

What legal risks are associated with non-compliance with accessibility laws and regulations?

What potential damage to the organization's reputation could occur if accessibility issues are discovered by users or the public?

How might accessibility issues impact the usability and effectiveness of InfoSec systems for employees with disabilities?

What security risks might arise from inaccessible systems leading to insecure workarounds?

4. Risk Analysis

Likelihood and Impact Assessment:

Rate the likelihood of legal risks occurring (e.g., high, medium, low).

Rate the potential impact of legal risks (e.g., financial, legal consequences).

Rate the likelihood of reputation risks occurring.

Rate the potential impact of reputation risks (e.g., loss of trust, negative publicity).

Rate the likelihood of operational risks occurring.

Rate the potential impact of operational risks (e.g., reduced efficiency, increased errors).

Rate the likelihood of security risks occurring.

Rate the potential impact of security risks (e.g., potential security breaches).

5. Mitigation Strategies

Policies and Governance:

Does the organization have a comprehensive digital accessibility policy in place?

Are accessibility considerations integrated into InfoSec policies and procedures?

Training and Awareness:
Is there regular training for InfoSec staff on digital accessibility best practices?

Are there awareness programs for all employees on the importance of accessible InfoSec practices?

Technical Controls:
Are InfoSec systems designed and maintained to be accessible (e.g., user interfaces, authentication mechanisms)?

Are security controls accessible (e.g., multi-factor authentication methods accommodating various disabilities)?

Regular Audits and Testing:
Are regular accessibility audits conducted using automated tools and manual testing?

Is accessibility testing included in the InfoSec system development lifecycle (SDLC) and change management processes?

6. Review and Update Schedule

Periodic Reviews:
How often are digital accessibility compliance reviews conducted?

How often are the risk assessment and mitigation strategies updated?

7. Documentation and Reporting

Records of Findings and Actions:
Are all findings from the risk assessment documented?

Are implemented mitigation strategies and their effectiveness recorded?

Reporting Structure:
Are regular reports on accessibility compliance and improvements provided to senior management, the IT department, and the InfoSec team?

Are all accessibility compliance efforts and improvements documented?