



Use of this framework

This document is part of the *Access Denied* collection by Jemma Davis. You are welcome to adapt or apply it for internal learning, accessibility planning, or research. If you intend to use it as part of paid consultancy, training, or commercial work, please request permission first at info@accessdeniedbook.co.

Shadow System Risk Assessment Framework

Use this assessment tool to identify, categorise and prioritise Shadow Systems in your environment. Complete each column to develop a clear remediation strategy for each identified Shadow System, focusing first on those with critical security impact.

Shadow System	Organisational Need	Security Impact	Accessibility Barrier	Remediation Priority	Remediation Approach
Shared authentication credentials	Access to secure systems for screen reader users	CRITICAL: Eliminates audit trails, enables unauthorised access	Authentication app not compatible with screen readers	URGENT (1-2 weeks)	<ol style="list-style-type: none">1. Implement keyboard-accessible authentication alternative.2. Reset all shared credentials.3. Audit access logs for unusual patterns
Personal cloud storage for document sharing	File sharing with external partners	HIGH: Uncontrolled sensitive data, potential regulatory violations	Official system not compatible with motor impairment adaptations	HIGH (2-4 weeks)	<ol style="list-style-type: none">1. Configure accessible official alternative.2. Implement secure migration path from

					<p>personal to corporate storage.</p> <p>3. Create data loss prevention monitoring for personal storage services</p>
Text-based notes with customer data (neurodivergent staff)	Reference during customer calls	HIGH: Sensitive data in unsecured locations, no retention control	Complex CRM creates cognitive overload for neurodivergent staff	HIGH (2-4 weeks)	<p>1. Create low-cognitive load interface.</p> <p>2. Implement secure note system with appropriate controls.</p> <p>3. Train on alternative navigation methods</p>
Physical security badge borrowing (trauma-informed)	Building access without triggering PTSD	CRITICAL: Unauthorised physical access, compromised audit trails	Biometric scanning triggers trauma responses	URGENT (1-2 weeks)	<p>1. Implement alternative access methods.</p> <p>2. Create trauma-informed security protocols.</p> <p>3. Train security personnel on appropriate accommodations</p>

Simplified password spreadsheets (dyscalculia)	Password management for staff with dyscalculia	CRITICAL: Plaintext credentials, unsecured storage	Password manager's numeric complexity overwhelms dyscalculia users	URGENT (1-2 weeks)	<ol style="list-style-type: none"> 1. Implement pattern-based authentication. 2. Create accessible password management tool. 3. Develop non-numeric security verification methods
--	--	--	--	--------------------	--