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**.

Security-Accessibility Maturity Model

This proposed maturity model provides a framework for assessing your organisation's current state. Use this matrix to honestly assess your current state and prioritise improvements. Score your organisation across these five critical domains. If you're below Level 3 in any area, start planning remediation this quarter, not next year.

Key: ! = Vulnerable, * = Aware, + = Compliant, ++ = Inclusive,** = Leading

Authentication

How accessible are your authentication systems for users with different abilities?

Level	Status	Description
1: Vulnerable	!	Single authentication method with no alternatives
2: Aware	*	Some alternative methods but not equivalent security
3: Compliant	+	Multiple equivalent authentication options
4: Inclusive	++	Adaptive authentication tailored to individual needs
5: Leading	**	Security strengthened through cognitive diversity

Incident Response

Can all employees report security incidents regardless of disability?

Level	Status	Description
1: Vulnerable	!	Inaccessible reporting tools; no keyboard navigation
2: Aware	*	Basic keyboard support but complex workflows
3: Compliant	+	Accessible reporting through multiple channels
4: Inclusive	++	Inclusive design with user testing by disabled staff
5: Leading	**	Incident patterns identified through diverse perspectives

Security Monitoring

Are your security dashboards and alerts usable by all staff?

Level	Status	Description
1: Vulnerable	!	Dashboards rely on colour alone; no screen reader support
2: Aware	*	Some colour contrast improvements but core functions still inaccessible
3: Compliant	+	Core functions usable with assistive technology
4: Inclusive	++	Personalised interfaces supporting different cognitive styles
5: Leading	**	Enhanced threat detection through neurodivergent talent

Physical Security

Can everyone access secure areas independently?

Level	Status	Description
1: Vulnerable	!	Biometric-only access; no alternatives
2: Aware	*	Alternative paths exist but require assistance
3: Compliant	+	Independent access through multiple methods
4: Inclusive	++	Universally designed access seamlessly accommodating all users
5: Leading	**	Security innovation driven by inclusive design

Training & Awareness

Is your security training effective for all learning styles?

Level	Status	Description
1: Vulnerable	!	Visual-only training; no captions or alternatives
2: Aware	*	Multiple formats but not fully accessible
3: Compliant	+	Fully accessible content with alternatives
4: Inclusive	++	Security awareness designed for neurodivergent learning styles
5: Leading	**	Security culture strengthened through diverse representation

Shadow System Detection

How effectively do you identify unofficial security workarounds?

Level	Status	Description
1: Vulnerable	!	No formal detection methods: Shadow Systems discovered only after incidents
2: Aware	*	Basic technical scanning but limited insight into accessibility-driven workarounds
3: Compliant	+	Regular Shadow System audits including accessibility evaluation
4: Inclusive	++	Proactive detection through diverse user input and technical monitoring
5: Leading	**	Continuous Shadow System intelligence gathering integrated with risk management

Alternative Control Pathways

Do you provide accessible alternatives to standard security controls?

Level	Status	Description
1: Vulnerable	!	Single method for each security control with no alternatives
2: Aware	*	Limited alternatives for some controls, unofficial or inconsistent
3: Compliant	+	Formally supported alternatives for critical security functions
4: Inclusive	++	Multiple equivalent security pathways designed for diverse users
5: Leading	**	Universal design principles embedded in all security architecture