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 Metrics Framework

The following table illustrates how traditional security metrics can be enhanced with accessibility considerations to identify security vulnerabilities that standard approaches might miss:

Traditional Metrics	**Accessibility-Enhanced Metrics**	**Security Impact**
Policy Compliance Rate	Compliance Rate by Disability Status	Identifies controls creating disparities
Authentication Failures	Auth Failures by Assistive Technology	Reveals credential sharing vulnerabilities
Exception Requests	Exceptions by Accessibility Needs	Highlights controls needing remediation
Security Incident Rate	Incidents with Accessibility Factors	Quantifies impact of inaccessible controls
Help Desk Call Volume	Accessibility-Related Security Tickets	Exposes controls creating support burden
Mean Time to Detect	Detection Time Across User Groups	Identifies monitoring blind spots
Shadow IT Detection	Shadow Systems with Accessibility Causes	Reveals workarounds from inaccessible tools

These enhanced metrics don't just improve inclusion; they directly strengthen security by identifying vulnerabilities that traditional metrics systematically miss.

Security leaders implementing such metrics report that they provide visibility into vulnerabilities that traditional security measurements frequently miss, potentially reducing security incidents significantly by addressing gaps these metrics reveal.