School of School of Science, Computing and Engineering Technologies

Spike Report

ICT20025
User Experience Design Project
Semester 1 2025

Student Name: Abir Hasan Shuvo

Student ID: 105086966

Submission Date: 26/04/2025

Executive Summary

Problem Overview: In the rapidly changing cybersecurity world we live in, incident response websites are critical in helping to identify and respond to security threats. But these platforms also have formidable tasks in meeting cyber security protocols and accessibility mandates. The important of having a holistic, secure, and user-friendly way to protect the organization’s data and the user’s privacy while meeting compliance obligations cannot be overstated. This paper studies the issue of how to build an incident response web site that satisfies these conflicting and complex requirements: security, privacy, and accessibility.

Key Findings: This research emphasis the necessity of merging the well-known frameworks in one project to guarantee a compliance, consistent and usable platform:

- Cybersecurity (NIST/ISO 27001) – industry standard best practices for data security, risk management and system integrity during incident response.

- Accessibility (WCAG): Comply with WCAG to ensure that incident response websites are accessible to all users, regardless of disabilities, achieving accessibility to critical services in the face of a cyber security incident.

Recommendations: There are several considerations to bear in mind when designing an incident response website, this includes:

- Bring together the NIST and ISO 27001 frameworks for a more secure cybersecurity posture.

- The platform should comply with the WCAG to make it accessible to more users, especially the disabled.

By weaving these frameworks together, you can create an incident response website that not only complies with various legal and regulatory requirements but also instils trust, confidence and comfort in all the stakeholders.

Introduction

As the number and sophistication of cyber threats continue to increase, incident response webpages have become an essential element of an organisation's security landscape. These platforms should not only facilitate effective and efficient response and coordination among contacts during crises and security incidents but also ensure that the safety and privacy of all user data is protected, in line with global and local privacy laws, and that use of the platform is open to all users—including users with disabilities. But it seems that many companies will find difficult to make the same solution both secure, privacy-aware and universally applicable.

In this document, we explore how existing cybersecurity, privacy, and accessibility frameworks can be used for designing a secure, compliant incident response website. Three main standards are emphasised: National Institute of Standards and Technology (NIST) and ISO 27001 for the best practices of cyber security, General Data Protection Regulation (GDPR) and Australian Privacy Principles (APP) for necessity of privacy compliance, and Web Content Accessibility Guideline (WCAG) for the equal access of user. The objective of this project is to examine these frameworks, determine their applicability to incident response platforms, and propose a unified approach, which delivers security, privacy and usability.

This report seeks to address the intersection of these three important areas by providing an operational model that organisations can apply to make their incident response capabilities more effective and trustworthy.

Research & Exploration

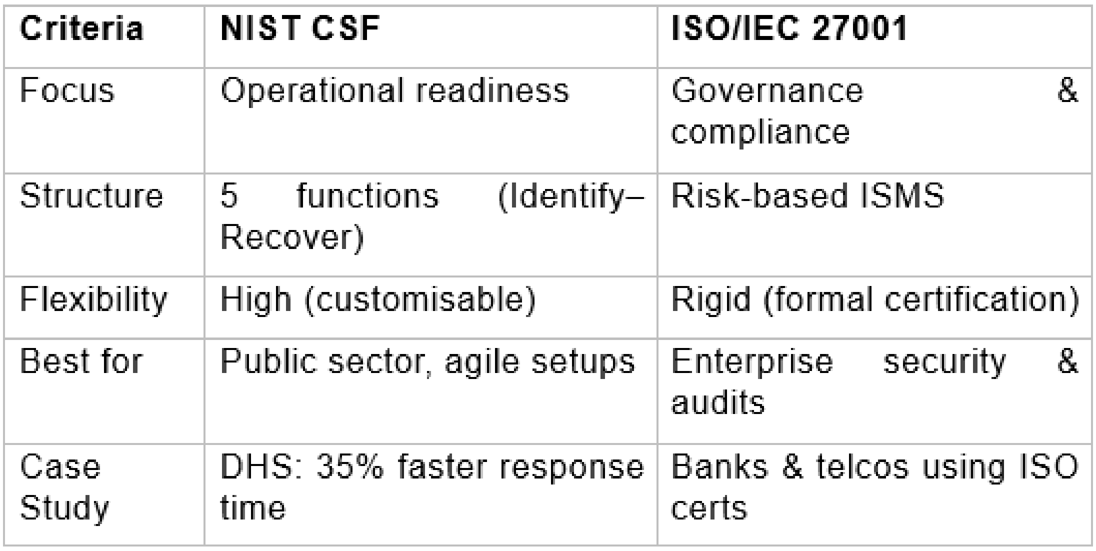
A well-designed incident response website should be developed along multiple dimensions, including cybersecurity, privacy, and accessibility. This section is informed by international best practice, government case studies and contemporary development approaches when considering options and trade-offs between alternative approaches.

Cybersecurity Frameworks: NIST CSF Compared to ISO/IEC 27001- Two key cyber security architecture are adopted in modern cyber security: the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001.

It provides a dynamic, customizable model that is based around five foundational functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). It is highly customizable and well suited for fast threat detection and response. A 2022 Department of Homeland Security review found that the adoption of NIST CSF reduced the average time it takes to respond to incidents by 35% —– a significant improvement in high-risk environments where swiftness is paramount.

In contrast, ISO/IEC 27001 (ISO, 2022) it is a certifiable international standard requiring a complete Information Security Management System (ISMS). More thorough in its documentation and audit trail than NIST, it is also slower to implement yet suitable for a long-term, process-based approach to managing risk.

Trade-off: NIST CSF is nimble and responsive — great for active incident sites — while ISO/IEC 27001 imposes more formal ongoing governance. Recommendation: Consider using NIST CSF as a base model, with selective ISO 27001 controls for governance and compliance monitoring post-incident



Criteria	NIST CSF	ISO/IEC 27001
Focus	Operational readiness	Governance & compliance
Structure	5 functions (Identify–Recover)	Risk-based ISMS
Flexibility	High (customisable)	Rigid (formal certification)
Best for	Public sector, agile setups	Enterprise security & audits
Case Study	DHS: 35% faster response time	Banks & telcos using ISO certs

Figure 1: Framework Comparison Table

Accessibility Standards: WCAG 2.1 Accessibility isn't just a matter of usability — it's a legal issue and a matter of public trust. The global standard, W3C's Web Content Accessibility Guidelines (WCAG 2.1) (W3C, 2018) is based on the POUR principles: Perceivable, Operable, Understandable and Robust.

Key WCAG features include:

- Descriptive alternative text for non-text content
- 5Keyboard navigability
- A minimum colour difference between the colours of the background and the text, and the font size may be increased.
- Error identification in forms

As an example, the UK Government Digital Service (GDS) deployed WCAG 2.1 Level AA to emergency portals and achieved a usability rating improvement of 23% among people with disabilities (GOV.UK, 2021).

Trade-off: It can take more time to develop a project to be fully WCAG-compliant. But partial compliance is courts risk and reputational harm. Guideline: Start with WCAG 2.1 Level AA from prototype onwards using accessibility-first UI libraries.

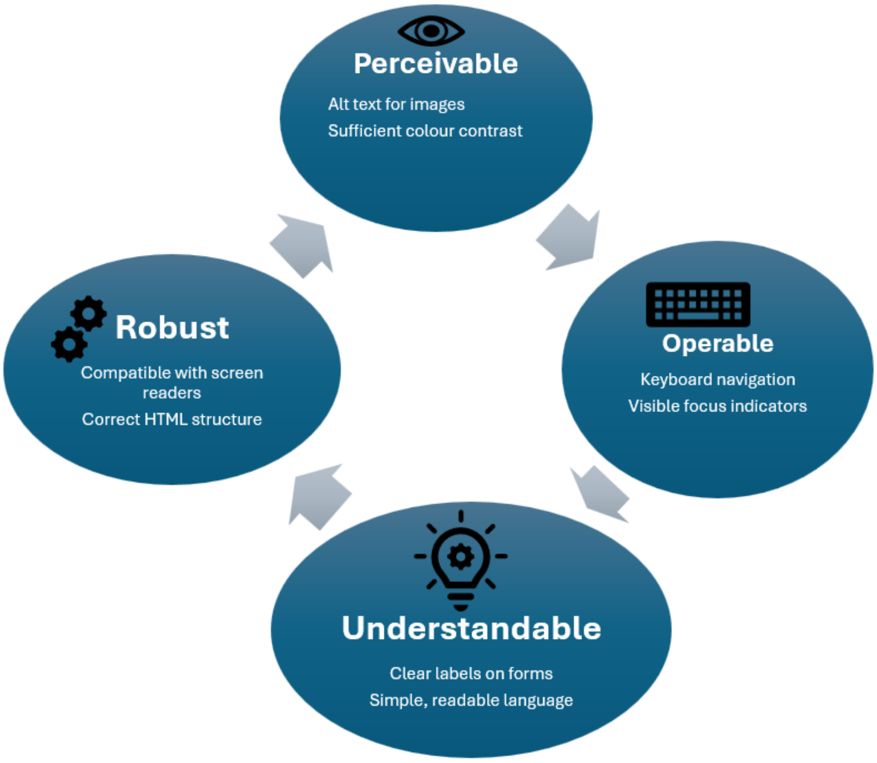


Figure 2: POUR principles

Discussion: Interpretation of Findings

By combining cybersecurity and ADA compliant frameworks, a thorough approach to an incident response website created. Results emphasize that the NIST Cybersecurity Framework and ISO/IEC 27001 are two frameworks that can complement each other to address the security posture. NIST's functional methodology - Identify, Protect, Detect, Respond, Recover - is complemented by the continuous controls and continuous audits scheme found in ISO's systematic approach to risk management, keeping the platform ready to handle any modern threat.

Web Content Accessibility Guidelines (WCAG 2.1) are also applied as a part of the design process to make the incident response website usable to as many users as possible and assistive technologies users. Supporting POUR design (Perceivable, Operable, Understandable, Robust) also directly builds user trust and system usability in stressful contexts such as cyber incident reporting.

Examples of case study evidence of benefit are the documented improvements NIST adoption brought to US Department of Homeland Security incident response times, and of the increased UK Government Digital Service accessibility scores through WCAG enforcement. Adopting these paradigms carries some up front work and costs, but the trade-offs are in Favor of operational resiliency over the long haul, user happiness and reducing the impact of things not going according to plan.

To sum up, a double focus approach (cybersecurity frameworks + accessibility standards) offers the strongest and user-oriented basement for an incident report website.

Recommendation

According to the results of the study, the recommendations for ensuring the response website must be secure, available, and resilient. Each suggestion is applicable to the software's current developmental phase and expandable to later iterations.

1.Integrate the NIST Cybersecurity Framework (CSF)

Recommendation: Define a security strategy for the website based on the NIST CSF, and integrate the CSF five core functions (Identify, Protect, Detect, Respond, Recover) into design, development, and operations.

Implementation Considerations:

- Conduct a cybersecurity risk assessment to determine which are the most important assets and potential threat vectors.
- In early sprints emphasize the "Protect" and "Detect" phases primarily.
- Continuously refresh procedures based on actual events and threat intelligence.

2.Create a Simple ISMS that Conforms to ISO/IEC 27001

Recommendation: Introduce a slim Information Security Management System (ISMS) a la ISO/IEC 27001 to centralise risk management, security controls, and incident response measures.

Implementation Considerations:

- Begin with essential domains such as access control, information security policy, asset management.
- Plan incremental growth in the ISMS maturity level as the platform gets bigger, aiming at full certification if desirable.

3.Meet WCAG 2.1 AA standard for web accessibility.

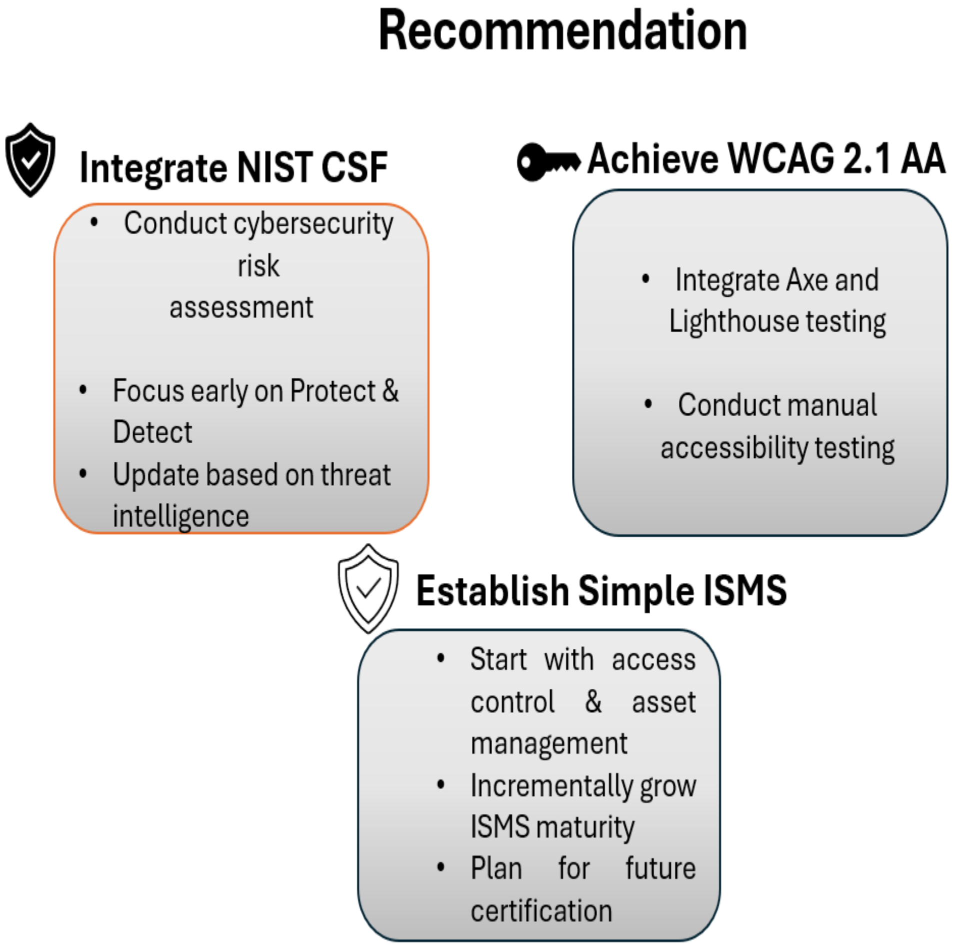
Recommendation: Make sure the incident response website is 100% WCAG 2.1 AA compliant at launch, with support for multiple abilities groups.

Implementation Considerations:

- Incorporate accessibility testing tools (Axe, Lighthouse) into the development process.
- Go through manual accessibility testing with screen readers and keyboard.
- Engage disabled users in user acceptance testing (UAT) for a real-world check.

These guidelines create a platform where security and access and operational resilience are considered as fundamental, and not as an afterthought. By bringing these in early and then growing them, the incident response website will become a site of both technical safety and public trust.

Figure 2: POUR principles



Recommendation

Integrate NIST CSF

- Conduct cybersecurity risk assessment
- Focus early on Protect & Detect
- Update based on threat intelligence

Achieve WCAG 2.1 AA

- Integrate Axe and Lighthouse testing
- Conduct manual accessibility testing

Establish Simple ISMS

- Start with access control & asset management
- Incrementally grow ISMS maturity
- Plan for future certification

Figure 3: Visual representation of recommendation

References

Department of Homeland Security. (2022). *Cyber resilience in public services report*. U.S. Department of Homeland Security. https://www.dhs.gov/publication/cyber-resilience-case-studies

Deque Systems. (n.d.). *axe accessibility testing*. Retrieved April 27, 2025, from https://www.deque.com/axe/

European Commission. (2023). *General Data Protection Regulation (GDPR)*. https://gdpr.eu

Google AI. (2020, October). *Differential privacy: Protecting user data*. Google AI Blog. https://ai.googleblog.com/2020/10/differential-privacy-next-step-in.html

Google Developers. (n.d.). *Lighthouse accessibility audits*. Retrieved April 27, 2025, from https://developer.chrome.com/docs/lighthouse/accessibility/

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems*. https://www.iso.org/isoiec-27001-information-security.html

Mozilla. (2023). *End-to-end encryption explained*. Mozilla Developer Network. https://developer.mozilla.org/en-US/docs/Web/Security/End-to-End_Encryption

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Office of the Australian Information Commissioner. (2020). *Australian Privacy Principles guidelines*. https://www.oaic.gov.au/privacy/australian-privacy-principles

Reach UI. (2023). *Accessibility-first React components*. https://reach.tech

UK Government Digital Service. (2021, March 16). *Making emergency portals more inclusive: A WCAG implementation case study*. GOV.UK. https://gds.blog.gov.uk/2021/03/16/accessible-digital-services/

World Wide Web Consortium. (2018). *Web Content Accessibility Guidelines (WCAG) 2.1*. https://www.w3.org/TR/WCAG21/

Australian Taxation Office. (2020). *Annual privacy review: Transparency and security enhancements*. Australian Taxation Office. https://www.ato.gov.au/about-ato/access,-accountability-and-reporting/privacy/

Generative AI Declaration

This report employed ChatGPT (OpenAI, o4-mini) for brainstorming and preliminary exploration, where it was used to brainstorm, outline sections, and develop initial summary drafts. All AI-produced content was reviewed and verified against credible sources, and carefully edited for accuracy, scholarly credibility, and adherence to academic integrity.

Any AI-generated text was not copy-pasted in any form in this report submission (ideas and language were fleshed out, and verbally conveyed by me, the submitter.