Introduction 1.0

In recent years, digital technologies have increasingly contributed to economic growth and citizen empowerment. These technologies have become ubiquitous in everyday life and enable people to access various services from the comfort of their homes. Government has established web presence through multiple websites, web portals, web applications and mobile apps that offer information and services to the public. However, inconsistency in conventions, layout standards, navigation strategies and technologies adopted can reduce the effectiveness of websites/apps.

In this context, the National Informatics Centre (NIC) formulated the Guidelines for Indian Government Websites (GIGW) in the year 2009. GIGW aims to ensure quality and accessibility of government guidelines, by offering guidance on desirable practices covering the entire lifecycle of websites, web portals and web applications, right from conceptualisation and design to their development, maintenance and management. The Department of Administrative Reforms and Public Grievances made the same a part of the Central Secretariat Manual of Office Procedure.

The second version of GIGW (GIGW 2.0) was developed in 2019, taking into account feedback from and consultations with industry,

society and government organisations. GIGW 2.0 took note of the standards evolved by international bodies like the world-wide web consortium (W3C) and advancements in technology. It also included guidance on mobile apps.

This version is the third version of GIGW (GIGW 3.0). While the earlier versions were formulated in-house with external inputs, GIGW 3.0 has been formulated jointly with Standardisation Testing and Quality Certification (STQC) Directorate of the Ministry of Electronics and Information Technology and Indian Computer Emergency Response Team (CERT-In), so that the experience of conformity with GIGW gathered by the STQC Directorate auditors and the cybersecurity experience and knowledge of CERT-In also inform the GIGW. As in earlier versions, GIGW 3.0 too has also been formulated in association with industry and experts.

The key thrust of GIGW 3.0 is on offering specific guidance to government organisations on how to improve the user interface and user experience (UI and UX), by incorporating features such as intuitive page loading (using AI and analytics) based on user journey and user profile, using state-of-the-art content management system (CMS), user-centric information architecture (IA), centralised monitoring dashboard to identify and provide alerts on non-conformity and technical enablement of all content creators and publishers.

GIGW 3.0 also significantly enhances the guidance on the accessibility and usability of mobile apps, especially by offering specific guidance to government organisations on how to leverage public digital infrastructure devised for whole-of-government delivery of services, benefits and information. These cover aspects such as API level integration for use of integration with social media, India Portal, DigiLocker, Aadhaar-based identity, single sign-on, data sharing in open formats on the government's data platform, government's scheme discovery platform, government's citizen engagement platform MyGov, AI-based Indian language translation tools, seamless content/data access across web-based solutions of government organisations. GIGW 3.0 offers upgraded guidelines on accessibility of websites and apps, with a view to make access to cyberspace more inclusive. In view of incorporation of comprehensive guidance in this version on apps as well (in addition to websites), this version is titled "Guidelines for Indian Government Websites and Apps". However, since the acronym GIGW gained wide currency, the acronym has been retained, with the letter "W" being signifying "Websites and Apps".

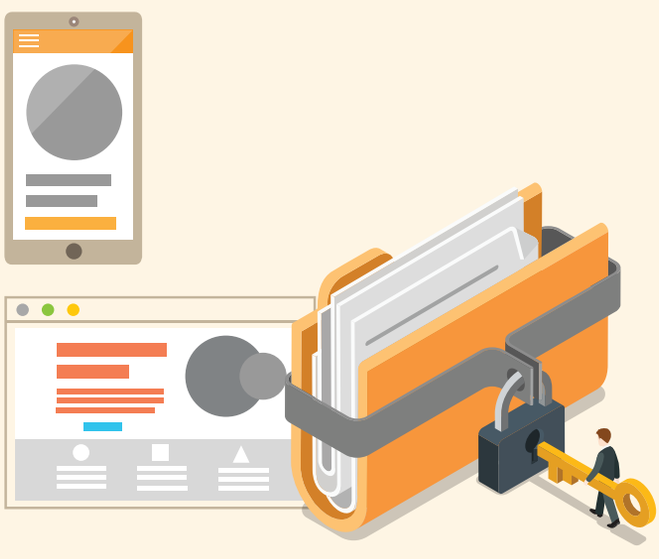
A chapter on cybersecurity, formulated by CERT-In, has also been incorporated so that GIGW can serve as a single point of reference on all the relevant aspects — quality, accessibility and security — relating to websites, web portals, web applications and mobile apps. Since cybersecurity requirements undergo continuous evolution in light of emerging threat scenarios, threat vectors and technologies, CERT-In continuously issues updated guidance and advisories to address the

same. Such guidance and advisories issued by CERT-In from time to time should be treated as updates to the guidance contained in the chapter on cybersecurity and any assessments or audit carried out with reference to GIGW 3.0 should also be cognizant of the same. Further, while government organisations may continue to establish conformity with GIGW 3.0 by obtaining Certified Quality Website (CQW) certification from the STQC Directorate, the certification of cybersecurity aspects by STQC may be done on the basis of the "safe to host" certificate issued by the cybersecurity auditors empanelled by CERT-In/STQC or the auditors of STQC or NIC.

To make the guidelines more readily usable, which entity/person has a role in implementing a particular guideline has been identified in every guideline. Thus, each guideline specifies whether the same is to be acted upon by the government organisation concerned or the developer or the evaluators.

The effectiveness of GIGW 3.0 in enhancing ease of living through various web-based initiatives of the government would depend on their effective implementation in letter and spirit by all government organisations and their implementation and evaluation partners. Government organisations are expected to carefully assess their existing websites, web portals, web applications and mobile apps against GIGW 3.0, identify areas requiring improvement, draw up time bound implementation plans to achieve conformity with GIGW 3.0 and obtain CQW certification from the STQC Directorate. Similarly, websites, web portals, web applications and mobile apps that are at the design or implementation stage may also be reviewed to ensure that their design, architecture, development and scope of audit conform to GIGW 3.0 and requisite approvals, resources etc. are tied up to ensure this.

While GIGW embodies general guidance for government websites, web portals, web applications and mobile apps, particular website/app use cases may require adoption of higher norms and specific technologies. Government organisations may keep this in mind while formulating their design, architecture and scope and may consult NIC in case they desire technical advice in the matter.



GIGW 3.0

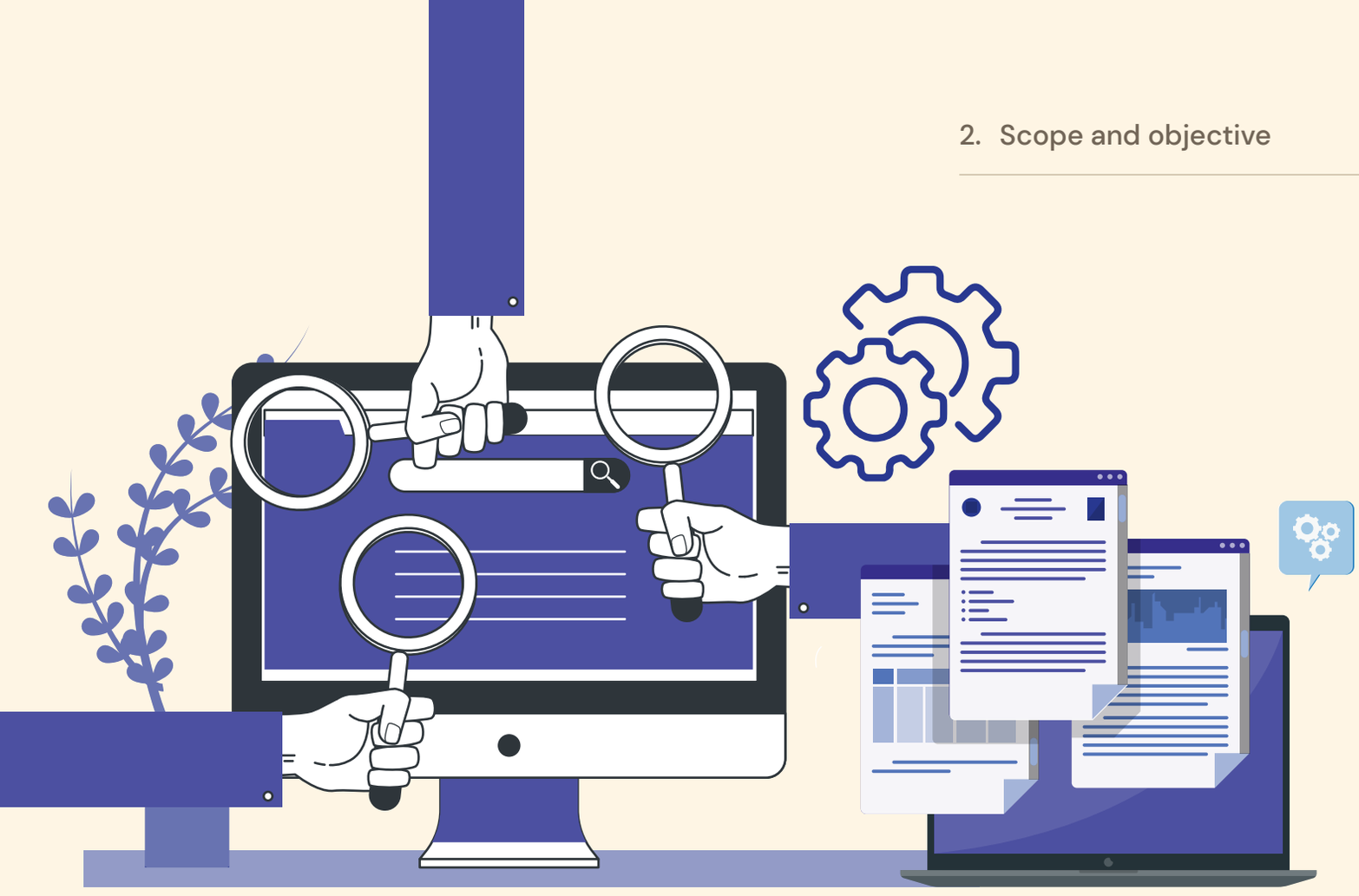
GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS

2. SCOPE AND OBJECTIVE

2 Scope and objective

2.1 Conformity to guidelines

2.2 How to use GIGW



Scope and objective 2.0

This document recommends policies and guidelines for Indian Government websites and Applications at any organisational level and belonging to both Central Government as well as State Governments (including district administrations and local governments) for making Indian government websites/apps user-centric, more user-friendly and secure. Conformity with these guidelines will ensure a high degree of consistency and uniformity in the content coverage, presentation security and accessibility and promote excellence in government solutions in the Indian web space.

These guidelines address common issues and practical challenges that government organisations face during development and management of their websites/apps. The guidelines aim to assist government organisations in ensuring that their websites/apps conform to a consistently high standard. This is expected to enhance the trust level of the citizens while accessing government information and availing of services online.

Conformity to guidelines 2.1

These guidelines have been framed with the objective to make the government websites/apps conform to the essential prerequisites of the UUU trilogy of usability, user-centricity and universal accessibility.

These guidelines are based on international standards, including ISO 23026, W3C's Web Content Accessibility Guidelines (WCAG 2.1) Rights of Persons with Disabilities Act, 2016, as well as the Information Technology Act, 2000. Further, the long-standing experience of the authors in the design, development and management of government websites/apps as well as their knowledge of the ground realities and challenges faced by government organisations in developing and managing their websites/apps, have helped significantly in drafting these guidelines.
These guidelines also form the basis for obtaining the Website Quality Certification from the STQC Directorate. Details of the certification scheme are available at https://www.stqc.gov.in/website-quality-certification-0.

These guidelines are being circulated amongst all Indian government organisations at all levels (Central, State and district/local). These should be followed and implemented on priority so that the overall aim of making all Indian government websites/apps citizen-focused and user-friendly may be realised.

How to use GIGW 3.0 2.2

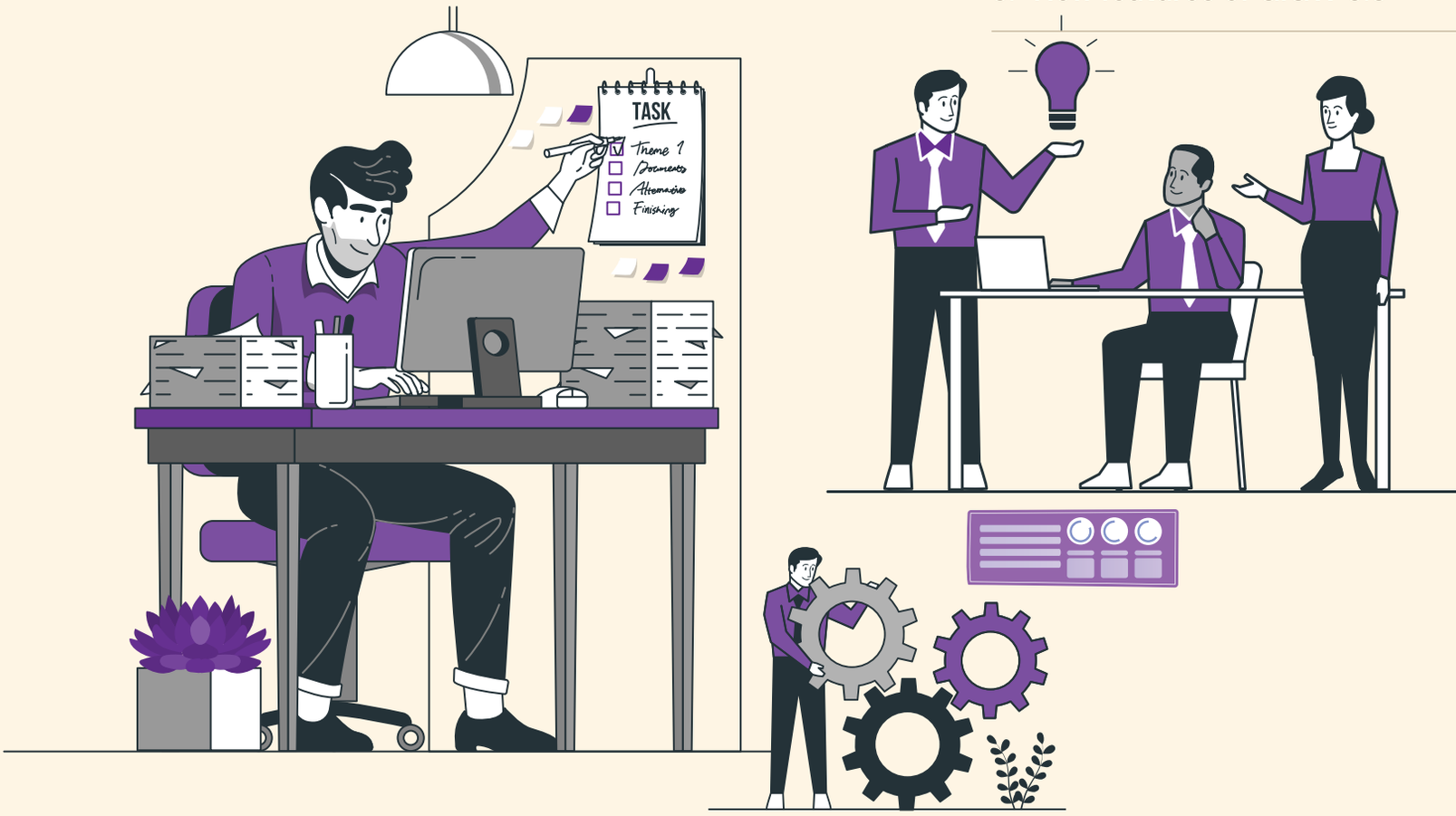
Government organisations are expected to read, understand and implement these guidelines on all of their web-based initiatives. In other words, all the websites/apps owned by government organisations must comply with these guidelines. It is recommended that browser-based intranet applications should also follow these guidelines. Depending upon their specific requirements, government organisations may draw up short-term and long-term timebound implementation plans for achieving conformity with these guidelines.

GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS

3. NEW FEATURES OF GIGW 3.0

3 New features of GIGW 3.0



The new version of the guidelines has several enhancements to make it more user centric, accessible, secure and at par with the global best practices and latest technological benchmarks. This version was reorganised to ease adoption and implementation and ensure wider conformity with GIGW. The following major enhancements have been included in the current version.

Structure 3.1

The new version of the guidelines is structured so as to reduce ambiguity and provide clarity on the roles and responsibilities of the implementers. The guidelines are structured under the following heads:

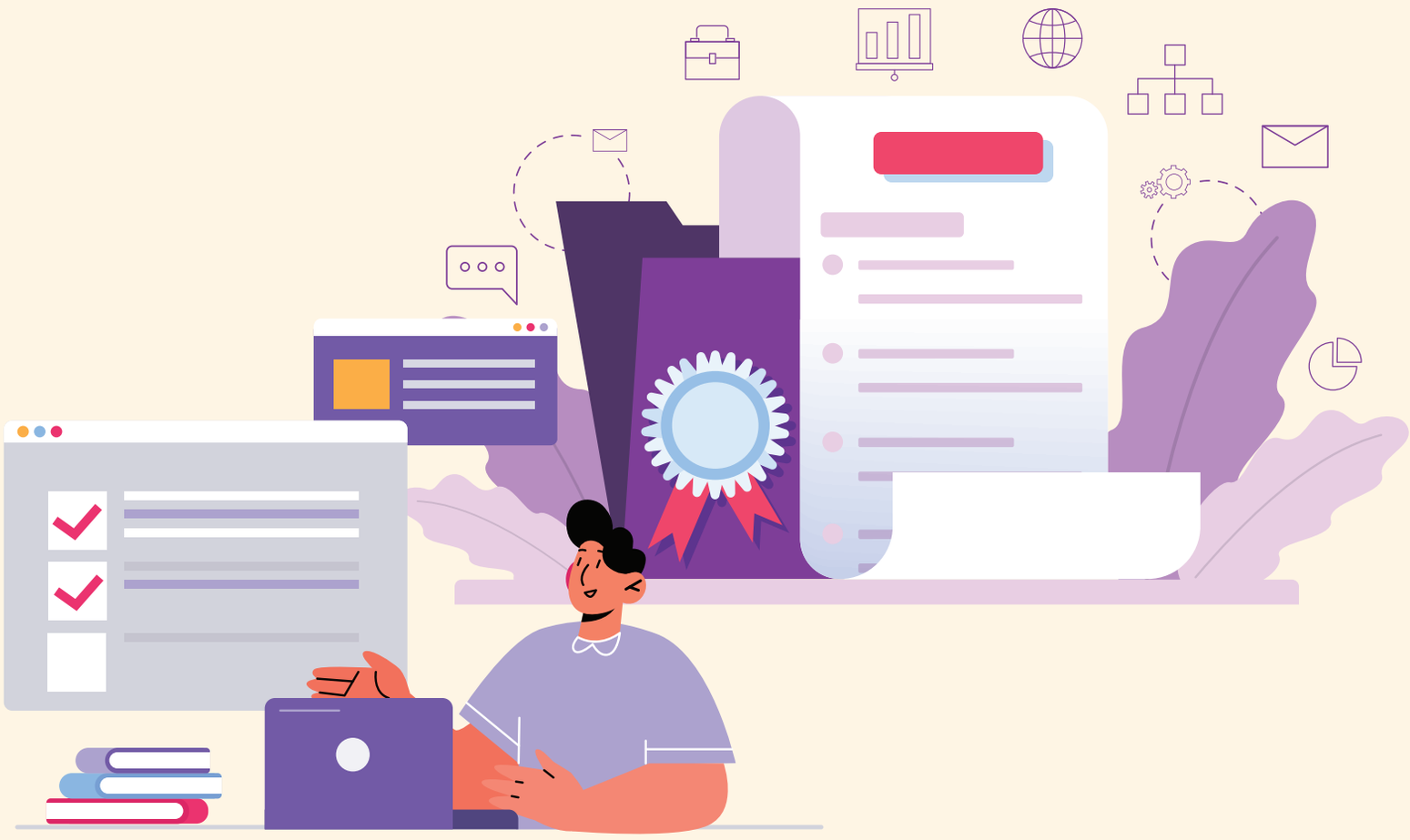
(a) **Statement:** Requirement or checkpoint to meet the particular guideline.

(b) **Benefits:** Positive outcomes achieved by following the requirements, such as improving user experience, accessibility, security and trust-building with citizens.

(c) **Government organisation action:** Actions pertaining to the owner government organisation. These will be undertaken by the respective WIM nominated by the organisation.

(d) **Developer action:** Specific tasks and actions a developer is responsible for in order to comply with the guidelines and ensure the website/app meets the desired standards of quality, usability and effectiveness.

(e) **Evaluator action:** Refers to testing of the website/app manually or with automated tools to verify conformity with this checkpoint.



Quality 3.2

The key thrust of GIGW 3.0 is on enhancing user interface and user experience (UI and UX) of websites/apps and the implementation of user-centric information architecture (IA) to ease the user journey and provide content as per the user profile. To ensure the quality of content throughout the lifecycle of the website, GIGW guides on the provisioning of a centralised monitoring dashboard to identify the issues and provide alerts on non-conformity. Content creators must also be supported with the right tools and technologies for accessible content creation.

GIGW 3.0 stresses on API level integration with platforms like India Portal, DigiLocker, Aadhaar-based identity, single sign-on, data and citizen engagement platforms, language translation tools to enable seamless content and data flow among the different web initiatives of government organisations. Social media integration also needs to be ensured.

Accessibility 3.3

Accessibility guidelines for web content have been formulated by W3C and are known as the web content accessibility guidelines (WCAG). GIGW 2.0 was compliant with version 2.0 of WCAG, however in the recent past WCAG has been upgraded to version 2.1 which inherits its requirement from WCAG 2.0 with additional guidelines to improve accessibility guidance for three major groups: users with cognitive or learning disabilities, users with low vision and users with disabilities on mobile devices.

GIGW 3.0 has been upgraded to include these additional requirements to ensure that websites/ apps can be used by the widest possible audience. The current version ensures conformity with Level AA of WCAG 2.1. In all 17 new success criteria have been added to the new version.

Cybersecurity 3.4

A chapter on cybersecurity, formulated by CERT-In, has also been incorporated which relates to websites, web portals, web applications and mobile apps. The chapter focuses on protecting web resources from unauthorised use, access, changes, destruction, or disruption. It also guides on the prevention of leakage of sensitive information like passwords, email addresses and credit card details, which cause both personal embarrassment and financial risks.

It deals with all aspects of security starting from design, coding and implementation to testing and deployment, which prevent malfunctioning, phishing, cyber-crimes or cyberattacks to avoid data loss of the organisations or users.

It is based on the best industry security practices and guidelines such as ISO 27001, the Application Security Verification Standard (ASVS) issued by Open Web Application Security Project (OWASP), OWASP Top 10 vulnerabilities and the Center for Internet Security (CIS) benchmarks as per the prevailing security policy.

This chapter must be read in conjunction with the guidance and advisories issued by CERT-In from time to time, which should be treated as updates to the guidance contained in the chapter.

Government organisations must continue to obtain a "safe to host" certificate issued by the cybersecurity auditors empanelled by CERT-In/STQC or the auditors of STQC or NIC.

Lifecycle management 3.5

The chapter on lifecycle management deals with the policies, processes and plans that the department has to put in place to guide the website management team in maintain the quality, accessibility security of the website throughout its lifecycle. It also stresses on the need for dedicated Web information Manager who is a senior official from the department to head the website management team.

Risk factors and their mitigations 3.6

Risk mitigation is one of the important criteria behind the formulation of any standard/ guideline. The new version of the guidelines outlines the risk factors associated with non-conformity with each section of these guidelines. They have also been mapped with each guideline and presented in the conformity matrix.

Therefore, while the description of each guideline informs the users about the benefits of conformance the conformity matrix will make the users aware of the risk involved in case, they fail to meet the guideline.