सत्यमेव जयते

GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS




GIGW
3.0

CONTENTS

01 Introduction 7

02 Scope and Objective 12

2.1 : Conformity to guidelines 13

2.2 : How to use GIGW 13

03 New features

3.1 : Structure 16

3.2 : Quality 17

3.3 : Accessibility 18

3.4 : Cybersecurity 19

3.5 : Lifecycle management 20

3.6 : Risk factors and their mitigation 21

04 Focus Areas

4.1 : Quality 24

4.2 : Accessibility 25

4.3 : Cybersecurity 27

4.4 : Lifecycle management 29

05 Guidelines

5.1 : Quality: Guidelines and attributes 32

5.2 : Accessibility: Guidelines and attributes 47

5.3 : Cybersecurity: Guidelines and attributes 80

5.4: Lifecycle management: Guidelines and attributes 92

Annexure I 99

Committee composition

Annexure II 100

Matrix for checking conformity

Annexure III 116

Important terms

Annexure IV 119

Role of Web Information Manager

GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS



1. INTRODUCTION



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".

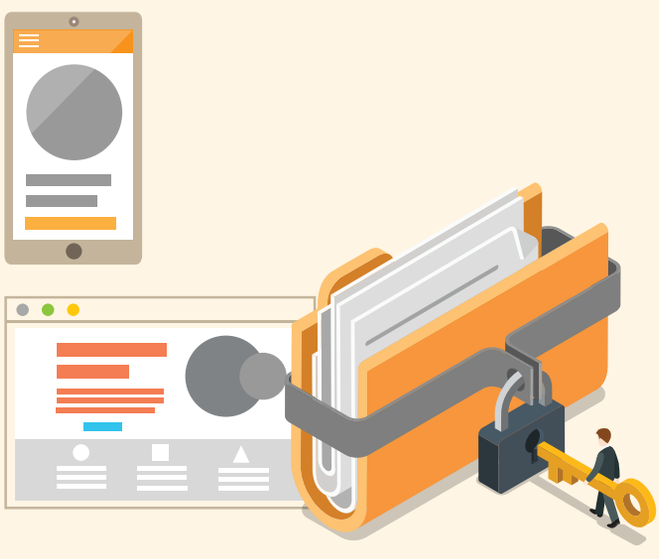
A chapter on cybersecurity, formulated by CERT-In, has also been incorporated so that GIGW can serve as a single point of reference on all the relevant aspects — quality, accessibility and security — relating to websites, web portals, web applications and mobile apps. Since cybersecurity requirements 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

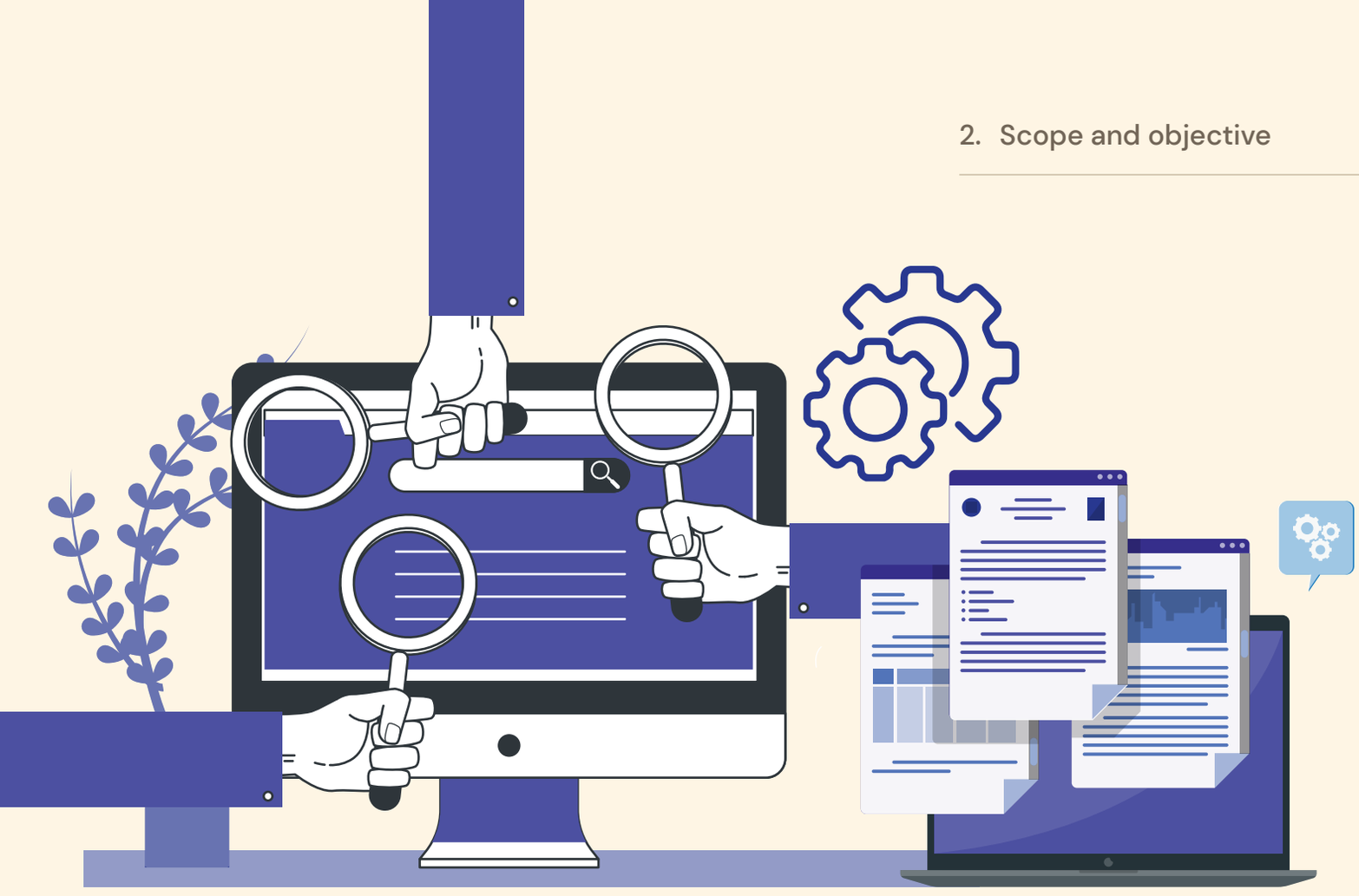
GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS

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.



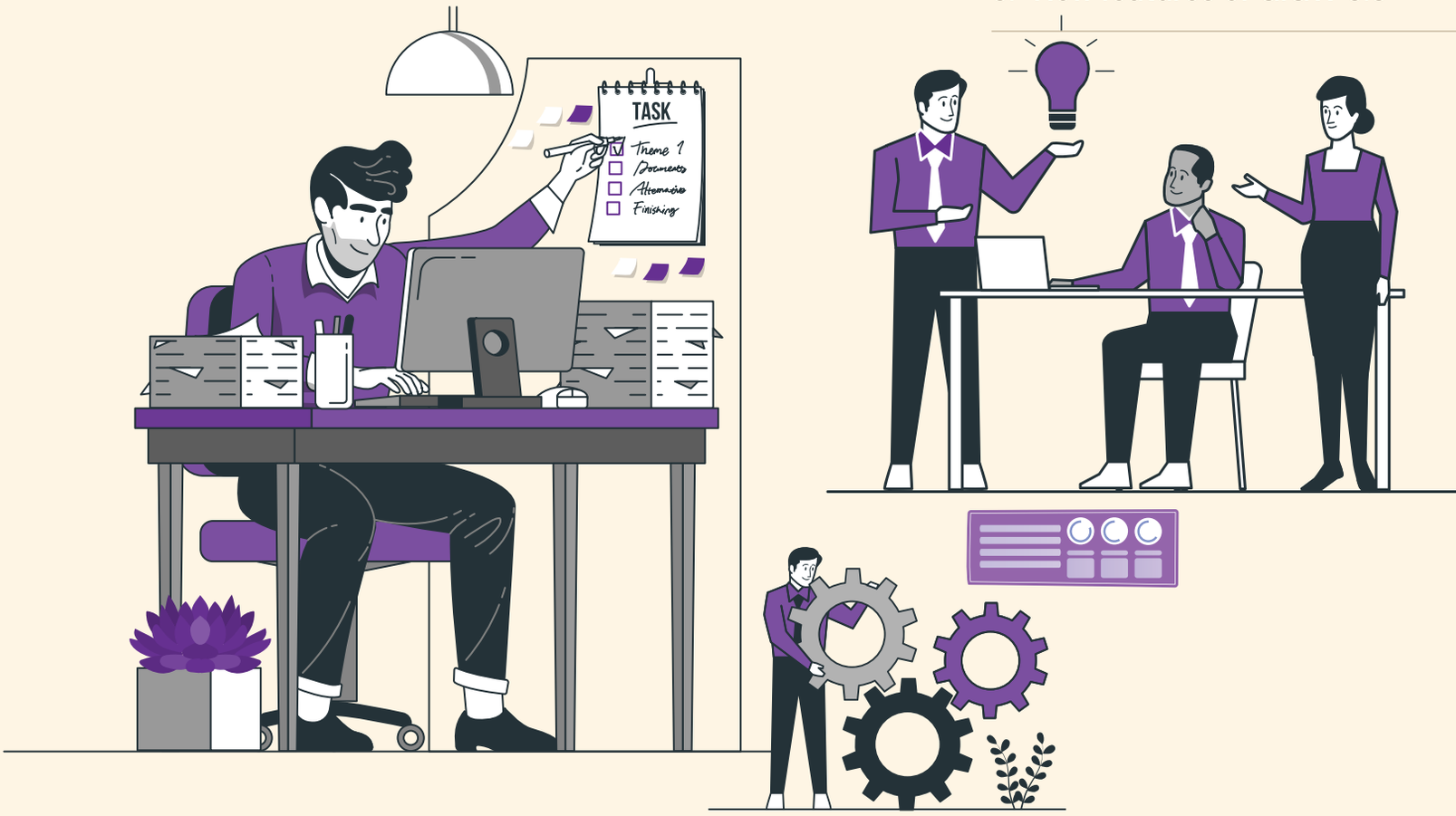
GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS

3. NEW FEATURES OF GIGW 3.0

3 New features of GIGW 3.0

3.1 Structure
3.2 Quality
3.3 Accessibility
3.4 Cybersecurity
3.5 Lifecycle management
3.6 Risk factors and their mitigation



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:

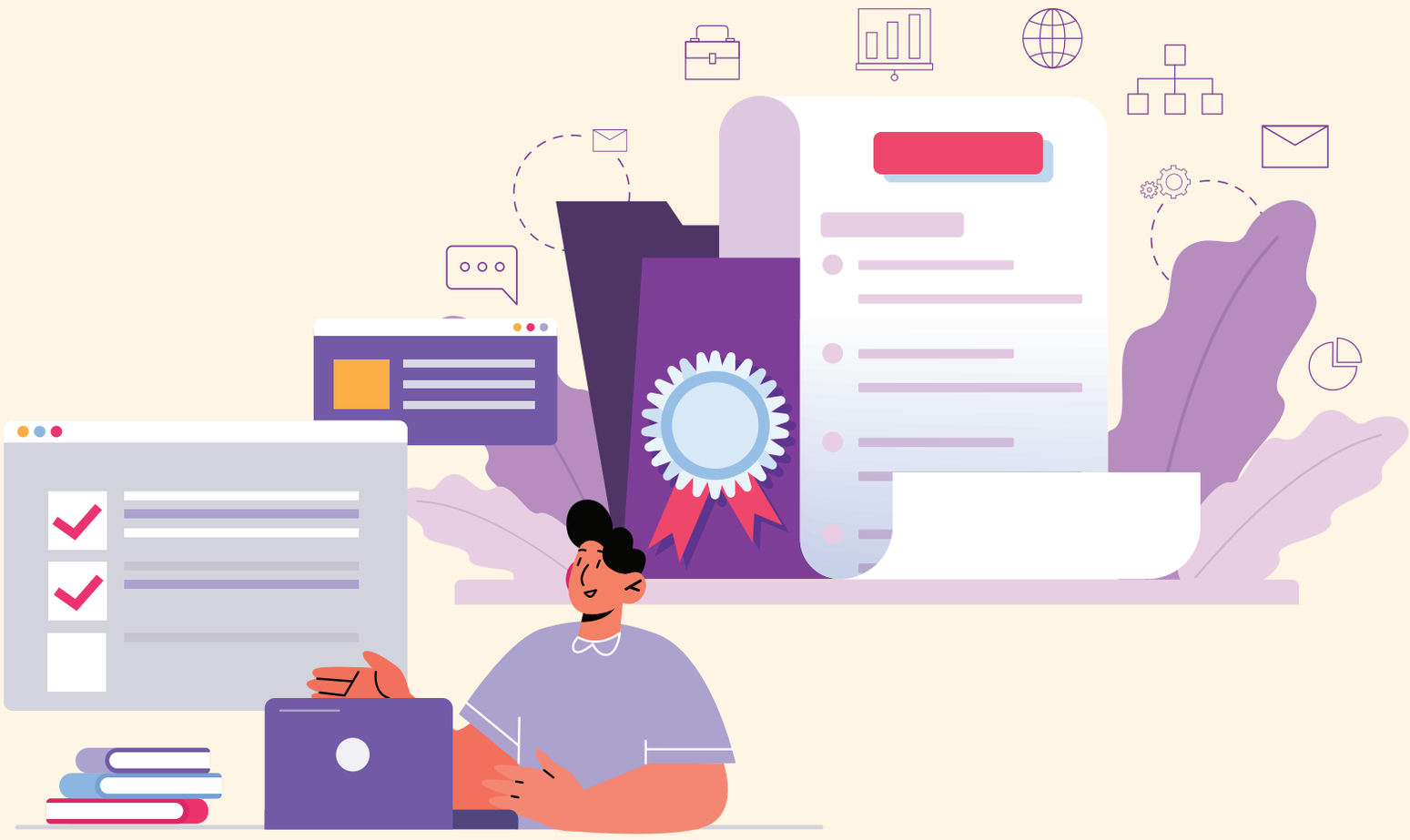
(a) **Statement:** Requirement or checkpoint to meet the particular guideline.

(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.

GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS



4. FOCUS AREAS

4 Focus areas

4.1 Quality
4.2 Accessibility
4.3 Cybersecurity
4.4 Lifecycle management



Quality 4.1

Quality criteria for websites/apps are essential to ensure a website/app is trustworthy, reliable and engaging for users. A website/app should be easy to use, accessible to all users, load quickly, have high-quality content, be secure, optimised for mobile devices and have a visually appealing design. Meeting these criteria can help ensure a website's success and make it stand out from the millions of websites/apps available on the internet. By prioritising these criteria, owners can create a high-quality website/app that provides value to its users.

Risks associated with non-conformity with quality guidelines: 4.1.1

Q1. Websites/apps can have inconsistent and outdated content on a website/app if the responsibility and ownership of the website/app is not assigned to a person or team.
Q2. People may not be able to get the information about the website/app.

Q3. Without correct copyright policy, any information on the website/app may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed without any consent.
Q4. The overall quality of a website's content can be degraded if the authenticity and relevance of the 'linked' information is not defined through hyperlinking policy.
Q5. Without terms and conditions on websites/apps it is difficult to uphold and maintain the trust imposed on them by the users to the sites, the government websites/apps should not out rightly 'disclaim' the content of another government website/app.
Q6. If Content is not selected keeping the audience in mind, people from diverse professional, educational and demographic backgrounds cannot easily comprehend the same.
Q7. People cannot get the right information from the website/app if Content is not up to date, incomplete, inconsistent or scattered.
Q8. Users cannot identify an authenticated government website.
Q9. Websites/apps with poor design methodology may not be accessible with slow internet connectivity.
Q10. Without feedback and help sections, users will not be able to participate in the improvement of website/app quality and the government organisation will not be able to get the information regarding problems faced by users.

Accessibility 4.2

Web accessibility means that people with disabilities can also perceive, understand, navigate and interact with the Web and that they can contribute to the Web. It encompasses all disabilities that affect access to the Web, including visual, auditory, physical, speech, cognitive and neurological disabilities. The website/app should be designed and developed in such a way that they are accessible by all people, whatever may be their hardware, software, language, culture, location, or physical or mental ability.



Legal provisions 4.2.1

The United Nations General Assembly adopted its Convention on the Rights of Persons with Disabilities on the 13th day of December 2006. India is a signatory to the Convention and has ratified the Convention on the 1st day of October 2007. To implement the Convention, India has enacted the Rights of Persons with Disabilities Act, 2016 on 27th December, 2016. With regard to ICT, one of the important provisions in the act is that all contents available in audio, print and electronic media must be in accessible format.

International Guidelines and Standards (WCAG) 4.2.2

W3C's Web Content Accessibility Guidelines (WCAG) covers a wide range of recommendations for making Web content accessible. Implementing these guidelines will make content accessible to persons with disabilities. Details are available at https://www.w3.org/TR/WCAG21/.
GIGW has been developed in accordance with level AA of WCAG 2.1 which are the latest guidelines on accessibility.

Risks associated with non-conformity with accessibility guidelines 4.2.3

A1. Visually impaired people cannot access the content.
A2. People with epileptic may get seizures if the website/app has content which blink very fast.
A3. Hearing/Auditory impaired people cannot access the content.
A4. People with cognitive Disability cannot access the time dependent function/content which does not have pause/extend/back/ forward options.
A5. People with Locomotor/Physical Disability cannot access the whole content present on the website.

A6. If the content is not robust enough to be interpreted reliably by a wide variety of user agents, including assistive technologies, the content becomes inaccessible to large audiences suffering from different impairments.
A7. People who do not understand English language cannot access website/app content and services.
A8. The government organisation concerned can face legal actions as per national and international laws if the content of the website/app is not accessible.
A9. Labels or instructions are not provided when content requires user input, which jeopardises the security or purpose of the content.

Cybersecurity 4.3

Cybersecurity is the activity of protecting websites/apps from unauthorised use, access, changes, destruction, or disruption. website/app security can be a complex (or even confusing) topic in an ever-evolving landscape. GIGW provides a clear framework for website/app owners seeking to mitigate risk and apply security principles to their web properties.
It is important to keep in mind that security is never a set-it-and-forge-it solution but is a continuous process that requires constant assessment to reduce the overall risk. Sometimes websites/apps become unavailable due to denial-of-service attacks or display modified information on their homepages. Millions of passwords, email addresses and credit card details have been leaked into the public domain exposing website/app users to both personal embarrassment and financial risks. The purpose of website/app security is to prevent such risks.
Website/app security requires vigilance in all aspects starting from requirements through design and implementation to testing and deployment. Organisations should implement appropriate security analysis, defences and countermeasures for protection of a website/app against malfunctioning, phishing, cyber-crimes, or cyberattacks to avoid data loss of the organisations or customers.



Risks associated with non-conformity with security guidelines 4.3.1

S1. Malicious users can deface the website.
S2. Any harmful actor may get access to confidential information.
S3. The availability of the website/app can be hampered.
S4. The malicious user may change/modify the content on the website.
S5. Security failures typically lead to unauthorised information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.
S6. A file upload flaw allows an attacker to retrieve the password database. Security of web applications determine the protection needs of data in transit and at rest. Attackers can steal such information for example, passwords, credit card numbers, health records, personal information and business secrets require extra protection, mainly if that data falls under privacy laws, Personal data protection bill etc.
S7. An attacker monitors network traffic (e.g., at an insecure wireless network), downgrades connections from HTTPS to HTTP, intercepts requests and steals the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data. Instead of the above they could alter all transported data, e.g., the recipient of a money transfer.
S8. Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.
S9. Attackers have to gain access to only a few accounts, or just one admin account to compromise the system. Depending on the domain of the application, this may allow money laundering, social security fraud and identity theft, or disclose legally protected highly sensitive information.
S10. Security flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks. The business impact depends on the protection needs of all affected applications and data.
S11. Attackers acting as users or administrators, or users using privileged functions, can create, access, update or delete every record.
S12. Security misconfiguration frequently gives attackers unauthorised access to some system data or functionality. Occasionally, such flaws result in a complete system compromise.

S13. The impact of XSS is moderate for reflected and DOM XSS and severe for stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.
S14. While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components.
S15. Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of a successful exploit to nearly 100%.

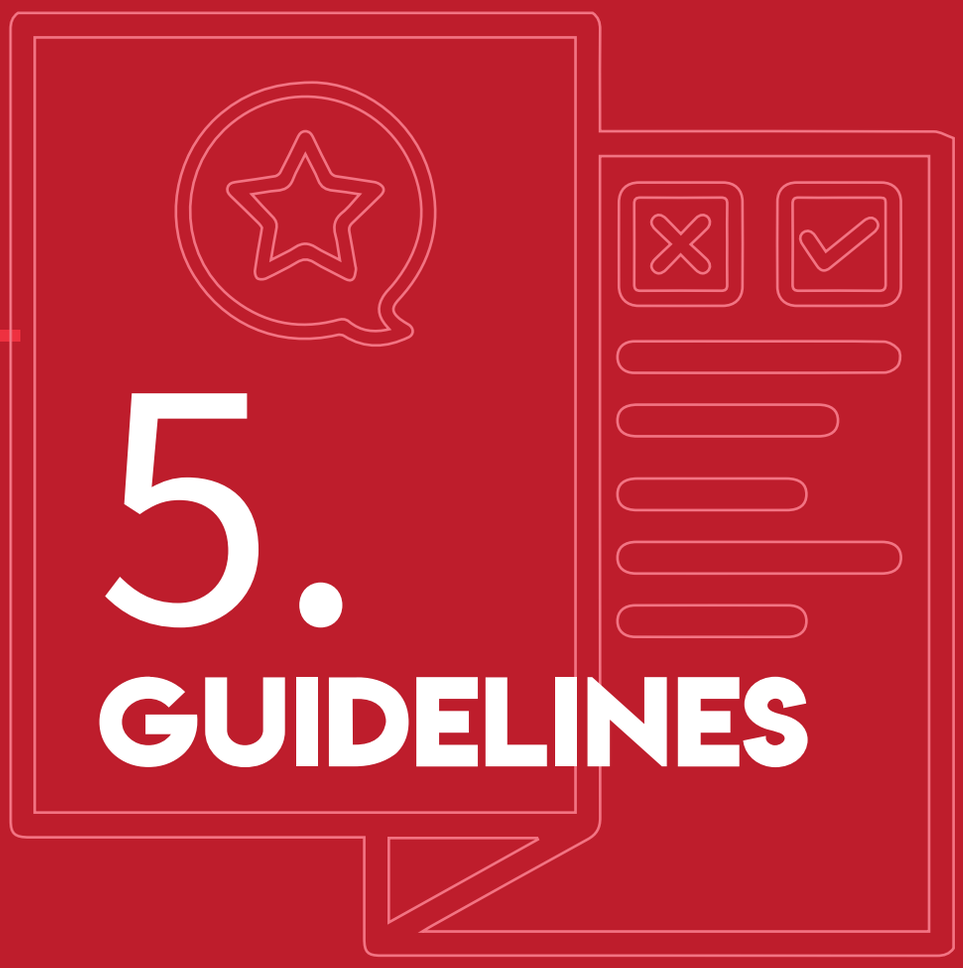
Lifecycle management 4.4

Maintaining a website/app is just as important as developing it because a website/app is a dynamic entity that requires regular updates and monitoring to remain relevant, functional and secure. Without proper maintenance, a website/app can become vulnerable to security breaches, performance issues and content that is outdated or irrelevant, which can negatively impact the user experience and drive away potential visitors. Regular maintenance can help prevent security breaches, ensure functionality, keep content up-to-date and optimise the website/app for search engines. Therefore, website/app life cycle management, including ongoing maintenance, is crucial for the success and longevity of a website.

After launching a website, ongoing maintenance is essential to keep the website/app up-to-date and functioning properly. This involves updating website/app content, monitoring performance, ensuring security, fixing bugs and errors and optimising the website/app for search engines. Establishing policies and procedures for website/app maintenance is important, including a change management process, backup and disaster recovery plans, security policies and a content management plan. Regularly monitoring the website's performance, user engagement and search engine optimization is crucial to ensure that the website/app is meeting its objectives and to identify areas for improvement.

The risks already identified under 'Quality' are also associated with the non-conformity of the Lifecycle Management guidelines.





5. GUIDELINES

5 Guidelines

5.1 Quality: Guidelines and attributes

5.2 Accessibility: Guidelines and attributes

5.3 Cybersecurity: Guidelines and attributes

5.4 Lifecycle management: Guidelines and attributes





Quality 5.1

Statement: Association to government is demonstrated by the use of emblem/logo in proper ratio and colour, prominently displayed on the homepage of the website or homescreen of the app. 5.1.1

Benefit: Reassures visitors that the government website/app is authentic and trustworthy. Moreover, the government organisation's brand identity is reinforced.

Government organisation action: Government organisations must select proper visual identity elements like emblems or logos to highlight government ownership of the website/app. The State emblem of India must be displayed on the homepages of the websites and homescreens of the apps of Central Government Ministries/Departments. State Governments should display their Emblems and public Sector organisations and autonomous bodies should display their official logo on the homepage of the website or homescreen of the app to reinforce their identity

Developer action: Visual Identity elements (logos and emblem) must prominently stand out on the page, in a proper ratio and colour. Developers must ensure that all logo images are accompanied by proper alternate text so that the screen reader users may be informed of the same. The usage of the State Emblem of India must comply with the provisions of the State Emblem of India (Prohibition of Improper Use) Act, 2005.

Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.

Statement: Ownership information is displayed on the homepage/homescreen and on all important entry pages/screens of the website/app and each subsequent page/ screen is a standalone entity in terms of ownership, navigation and context of content. 5.1.2

Benefit: Helps to build trust in the visitors and reinforces the government organisation's branding. Also, search engines use the ownership information to verify the legitimacy of the websites/apps and accord higher ranks in search results.
Government organisation action: Provide complete ownership information for publishing on the website
Developer action: Ensure display of ownership information, either in the header or footer, on the homepage/homescreen and all-important entry pages/screens of the website/app.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.

Statement: Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned. 5.1.3

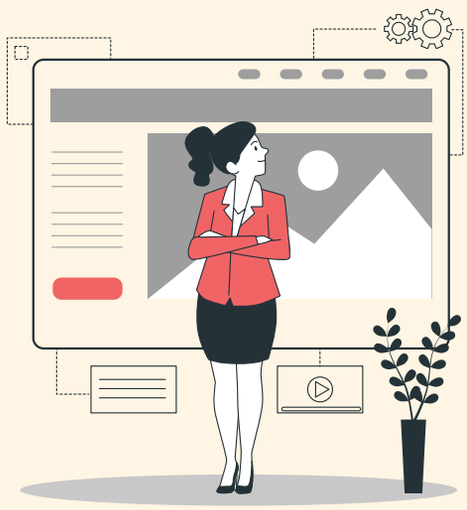
Benefit: Audiences can rely upon the credibility of authentic information being published by the government organisation. Additionally, giving the credit to the authoring organisation helps establish an environment of respect for intellectual property of other organisations and discourages plagiarism.
Government organisation action: If any published government document/report is being reproduced on the government organisation's website/app, whether as excerpts or in full, the organisation must cite the source of the same (complete title of the document/report, along with the name of the owner organisation and the year of publication).
Developer action: Ensure provision of appropriate data input fields in the CMS to input the source (owner organisation of each published document/report and the year of publication).
Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.

Statement: Due permissions have been obtained for publishing any content protected by copyright. 5.1.4

Benefit: Publishing copyrighted information after obtaining due permission protects the government organisation from legal issues, establishes an environment of respect for information copyrighted by others in addition to discouraging plagiarism.
Government organisation action: The government organisation must follow proper procedures to obtain the permission, prior to publishing any information that is copyrighted by any third party.
Developer action: None.
Evaluator action: The evaluator shall check the implementation of copyright policy in backend audit.

Statement: Homepage/homescreen of the website/app displays the last updated/ reviewed date. 5.1.5

Benefit: Providing information about the last updated/reviewed date helps visitors to build trust that the government organisation is providing updated information. Also, search engines accord a higher ranking to web sites that publish updated content, so they will automatically appear amongst the top-ranking sites on search results.
Government organisation action: Publish regular and updated content for publishing on the website/app and review the content of the website/app as per the content review policy.
Developer action: Ensure publishing, on the homepage/homescreen and every important entry page/screen, of the date on which the information was posted on the website/app, or the date on which the content was last reviewed and/or modified.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.





Statement: Complete information including title, size, format and usage instructions is provided for all downloadable material. 5.1.6

Benefit: Downloading material from the Internet can be an expensive and time-consuming exercise. Therefore, government websites/apps must prov ide Information that will help visitors determine whether they want to access downloadable material. Providing all required information about downloadable material helps improve clarity & accessibility, especially for those using assistive technologies.

Government organisation action: Provide all necessary content details to the content team. The total size of the file should be kept to a minimum to ensure acceptable download times for all users, especially those that do not have high-speed, reliable Internet connections. Prior to making downloadable material available for visitors, government organisations should check for viruses and malware.

Developer action: Ensure that there is a mechanism in the CMS to input the following information about the downloadable material:

(a) Self-explanatory title of the document/file;

(b) Download and use instructions (install, open, view); and

(c) File format and file size.

Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.

Statement: In respect of each circular, notification, document, form, scheme, service and recruitment notice, the following should be clearly listed on the website/app: 5.1.7

(a) Complete title;

(b) Language (if other than English);

(c) Purpose/procedure to apply (as applicable); and

(d) Validity (where applicable).

Benefit: Details such as the correct title, language, validity, purpose, procedures would lead to an accurate search output for information on that scheme/service/recruitment notice etc and it would be easy for the users to locate & use these documents, schemes, services etc.

Government organisation action: The attributes as specified in the guideline must be provided with each Circular, Notification, Document, Form, Scheme, Service and Recruitment notice
Developer action: Ensure provision of all fields necessary for publishing of all information about documents, schemes, services, along with the necessary archival procedures to archive the information once the validity expires.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.

Statement: All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are removed from the website/app and/or placed into the archives as per the archival policy 5.1.8

Benefit: Outdated and irrelevant content must not be served to the visitors and there should be a proper archival section to access the outdated content.
Government organisation action: The government organisation must ensure that the expiry date is provided for all time sensitive content
Developer action: Ensure that the mechanism is in place to automatically remove the content after the expiry date or move it to the archives as per the approved Archival Policy.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.



Statement: All information about the government organisation which is useful to users is present in the 'About us' section and a mechanism is in place to keep the information up to date. 5.1.9

Benefit: Helps the visitor access all information about the government organisation, useful for the citizen.
Government organisation action: The government organisation must prepare the content describing itself for the About us section.
Developer action: Ensure the website/app has an About us page.
Evaluator action: The evaluator shall manually test the website/app for verifying the content as required by this checkpoint is present on the website. The evaluator shall verify the conformity to the mechanism required in the checkpoint through backend audit.

Statement: Website/app has a 'Contact us' page providing complete contact details of important functionaries in the government organisation and this is linked from the homepage/ homescreen and all relevant places on the website/app. 5.1.10

Benefit: Enables users to contact any government organisation or entity to ask questions, get information, seek clarifications and resolve problems.
Government organisation action: Provide complete contact information on the Contact us or Who's who sections or on the Directory page, including the telephone numbers/fax numbers, postal address and email addresses, along with the timings, if any, earmarked for personal/public dealing.
Developer action: Ensure that the CMS has the provision to publish the contact details of citizen-facing functionaries in the government organisation.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity with this.



Statement: Feedback is collected through online forms and a mechanism is in place to ensure timely response to feedback/queries received through the website. 5.1.11

Benefit: Helps the visitors to express their ideas, satisfaction levels, suggestions etc. that can be valuable inputs for enhancement of future versions of the website. Additionally, government organisations can learn meaningful insights about the usage pattern of the website, which can further help to focus on near and far term enhancements.
Government organisation action: Ensure feedback received is processed on a regular basis.
Developer action: Ensure providing the mechanism to collect structured feedback from visitors using Forms. Also, ensure responding to the feedback explaining how it will be processed.
Evaluator action: The evaluator shall manually test the website/app for verifying that the feedbacks are collected through online forms at the website. The evaluator shall verify the conformity to the mechanism required in the checkpoint through backend audit.

Statement: Website/app provides a prominent link to the 'National Portal' from the homepage and webpages belonging to the 'National Portal' load in the new browser window. 5.1.12

Benefit: india.gov.in, the National Portal of India (NPI) is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders. Linking to the NPI will help visitors find information or services they could not find easily on a government organisation website.
Government organisation action: The government organisation website/app must provide a prominent link to the National Portal from the homepage and other important pages of citizen's interest.
Developer action: Ensure that the government website/app provides a prominent link to the National Portal from the homepage and other important pages of citizen's interest. Also, the hyperlinked pages belonging to the National Portal must load into a newly opened browser window of visitors.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity to this checkpoint.

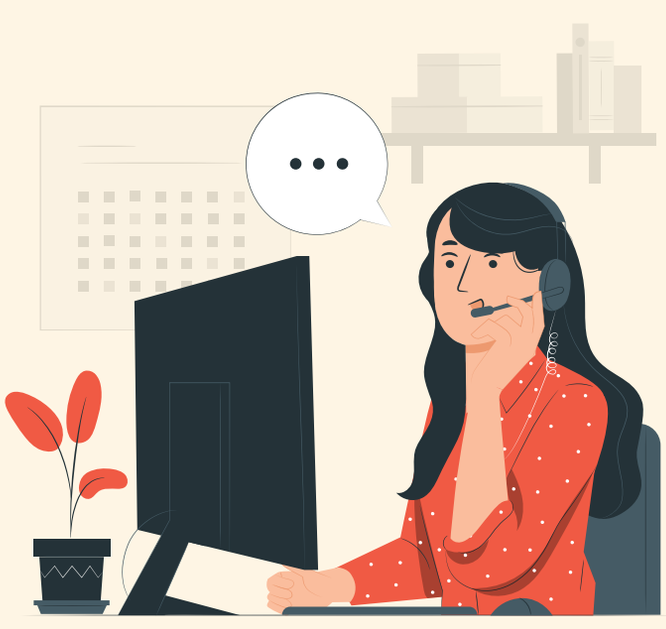
Statement: The website has been tested on multiple browsers. Hindi/Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout). 5.1.13

Benefit: Visitors can easily read content and interact with the website in their native language, thus improving the website's accessibility and reach.
Government organisation action: Government organisations must ensure the accuracy of the translated content.
Developer action: Ensure use of Unicode characters when using Hindi/Regional language fonts & also, testing of the website on multiple browsers and versions of browsers, operating systems, connection speeds and screen resolutions to ensure access by all and no loss of layout.
Evaluator action: The evaluator shall manually test the website on different browsers for verifying conformity to this checkpoint.

Statement: The website/app has a readily available Help section linked from all pages of the website. 5.1.14

Benefit: Allows a pleasant experience while browsing the website.
Government organisation action: None
Developer action: Must include Help content which allows for an easy and convenient navigation for the visitor to the website/app (e.g., online help, how to open files of certain formats, how to access audio/video on the portal, kinds of plug-ins required etc.). Further, the content which clarifies the purpose of the website/app as well as its policies for the visitors should also be included in this category. Help should be linked from all pages of the website/app and should be displayed in a consistent location across the website.
Evaluator action: The evaluator shall manually test the website/app for verifying conformity to this checkpoint.





Statement: Website uses Cascading Style Sheets (CSS) to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes. 5.1.15

Benefit: For the visitors, a consistent look and feel of the website's User Interface (UI)and its availability on all devices and screen sizes is important. For the government organisation and developers, CSS offers ease of making global changes to the layout and design in one place instead of having to do so on individual pages. Different presentations of the content (for example a large text alternative for visually impaired users) can be achieved using different style sheets. The document code is also reduced in size and complexity since it does not need to contain any presentational markup.

Government organisation action: None.

Developer action: Use CSS for controlling content layout and presentation, in addition to offering a responsive interface for visitors. Also, ensure testing on different devices.

Evaluator action: The evaluator shall test the website by using browser extension/ tool for verifying conformity to this checkpoint.

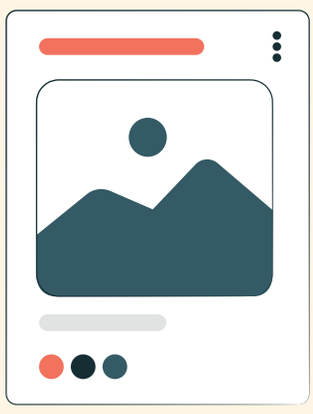


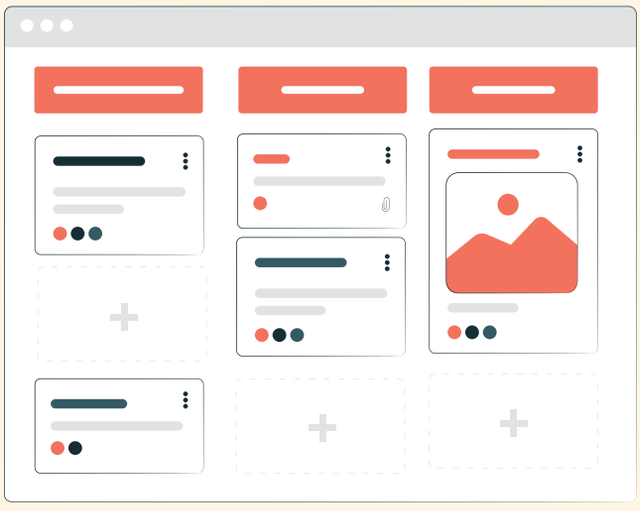
Statement: Website is readable even when style sheets are switched off or not loaded. 5.1.16

Benefit: Helps provide readable content not only for visually challenged users who may be using screen readers, but also in some instances where the style sheets may not load swiftly or load at all due to reasons such as slow connections, technical errors, or due to use of some incompatible mobile devices.
Government organisation action: None.
Developer action: Ensure testing on different devices to ensure the website remains easily readable even on turning off style sheets.
Evaluator action: The evaluator shall test the website by using browser extension/ tool for verifying conformity to this checkpoint.

Statement: Proper page title and language attribute along with metadata for page like keywords and description are appropriately included. 5.1.17

Benefit: Once details such as government organisation name, services offered, schemes, location, help ensure enhanced accessibility, especially for those with screen readers who rely on things such as page titles, structured page headings and lists. Additionally, search engines rank such sites higher in search results.
Government organisation action: The government organisation must provide the relevant metadata for each page.
Developer action: Must ensure mentioning all necessary metadata in the <head> portion of the html page from where it is read by search engines.
Evaluator action: The evaluator shall test the website by using browser extension tools for verifying conformity to this checkpoint.





Statement: Minimum content as prescribed in the guidelines is present on the homepage/homescreen and all subsequent pages/screens. 5.1.18

Benefit: The homepage/homescreen being the primary entry page to the entire content of the website/app should allow visitors to get access to the most important content elements from the homepage/homescreen itself. Often, visitors may use a search engine for finding some information and, therefore, directly reach a subsequent page/screen of the website/app instead of the homepage/homescreen, therefore, it helps to have some minimum content on each page/screen of website/app, e.g., self-explanatory title, link to homepage/homescreen, ownership, link to Contact us etc.

Government organisation action: The government organisation must ensure the availability of:

Minimum content on the homepage/homescreen of a website/app

(a) Government organisation name (alternatively, the name of the project, service etc. as applicable);
(b) State emblem of India/Logo (as applicable);
(c) About the government organisation (including its main activities and functions);
(d) Link to all the major modules/sections of the site;
(e) Link to all the citizen services offered by the government organisation;
(f) Link to the 'Contact us' page of the website/app;
(g) Link to the "Feedback" page;
(h) Link to national portal;
(i) Search/Site Map; and
(j) Terms and conditions of use.

Minimum Content on subsequent pages/screens of a website/app

(a) Self-explanatory title of the page/screen;
(b) Link to the homepage/homescreen;
(c) Link to the parent section/top module of the individual page/screen;
(d) Ownership (name of the government organisation owning the website/app); and
(e) Link to the "Contact us" page.

Developer action: Ensure providing the minimum content as prescribed by the GIGW guidelines referred on the homepage/homescreen as well as the subsequent pages/screens.

Evaluator action: The evaluator shall manually test it for verifying conformity to this checkpoint.

Statement: Data tables have been provided with necessary tags/markup 5.1.19

Benefit: Proper use of markup in tables helps with accessibility, ensuring assistive technology users can easily navigate and comprehend the tabular content.
Government organisation action: None.
Developer action: Avoid use of tables for page layout. Proper tags and markup must be provided to identify row and column headers and associate data cells and header cells.
Evaluator action: The evaluator shall test the website by using browser extension/ tool for verifying conformity to this checkpoint.

Statement: Content of the web page prints correctly on an A4 size paper 5.1.20

Benefit: Offers enhanced accessibility to visitors who may prefer the print format.
Government organisation action: None.
Developer action: Ensure testing with font properties such that the text must print correctly on an A4 size paper.
Evaluator action: The evaluator shall manually test the website for verifying conformity to this checkpoint.

Statement: Website is in the nic.in or gov.in domain. Educational Institutions and Research and Academic Institutions, which are eligible for registration under 'gov.in' may use 'edu.in', 'res.in' or 'ac.in' domains 5.1.21

Benefit: The URL or the Web Address of any Government website is a strong indicator of its authenticity and status as being official. Use of gov.in or nic.in domain inspires trust in the visitor that the website being visited is authentic.
Government organisation action: The government organisations must obtain 'gov.in' or 'nic.in' domain exclusively allotted and restricted to government websites. The domain name conventions, as specified in the '.IN Registration' policy, should be followed while registering a 'gov.in' Domain Name. For detailed information and step-by-step procedure on how to register a gov.in Domain visit http://registry.gov.in.

Developer action: None.

Evaluator action: The evaluator shall manually test the website for verifying conformity to this checkpoint.

Statement: API integration with key government platforms (India Portal, DigiLocker, Aadhaar, Single-Sign-On, MyGov, Data Platform, MyScheme) and similar websites of the government organisation must be enabled for seamless exchange of Information and data. 5.1.22

Benefit: Integration with other websites and platforms provides the following benefits to the government organisation:

(a) Data/Information is consistent as it is being pushed from a single source to all the interfaces;

(b) It can be managed and maintained easily and is well synchronised across all the interfaces;

(c) Avoids duplication of effort content creation; and

(d) Ensures standardisation and security, e.g., use of DigiLocker, Aadhaar authentication or single sign-on ensures that any technical, functional or security enhancements are pushed to all the websites/apps in real time.

Citizens benefit by having a single identity which can be used across multiple websites/apps and a single repository of documents. They do not have to comprehend the same information and data from multiple sources.

Government organisation action: The government organisation must identify the websites and platforms with which the integration needs to be established as per their requirement so that no duplication efforts are being made. They must provide required APIs and Web Services to the developer/entity to enable integration.

Developer action: Developers must ensure that the integration is done as per the best practices pertaining to security and technology.

Evaluator action: The evaluator shall manually test the website for verifying conformity to this checkpoint.



Statement: The government organisation must ensure a consistent user experience and visual identities across all its websites/apps. 5.1.23

Benefit: Maintaining consistency enhances the ease of use for the visitors. If the visitors have browsed one website/app then the learning curve of using the other websites/apps of the government organisation is greatly reduced and visitors can interact and find information easily and quickly. Maintaining a consistent visual identity reinforces the authenticity and enhances the trust level of the visitors.

Government organisation action: The government organisations must ensure a consistent information architecture, navigation scheme, terminology and visual branding (logos, etc.) across the web initiatives of all organisations under them.

Developer action: Developers must create templates with common Information Architecture (IA), configurable components and neat user interface, which can be implemented on different websites/apps to achieve consistency.

Evaluator action: The evaluator shall manually test the website for verifying conformity to this checkpoint.

Statement: Websites/apps must provide integration with popular social media. 5.1.24

Benefits: Users and the government organisation are increasingly using social media to quickly connect, share information and even provide services. Social media platforms also provide an easy means of two-way communication between the user and government organisation. Younger generation also finds it easy to connect through social media on smart devices rather than the web interface.

Government organisation action: The government organisations must identify the information/content that needs to be pushed to the social media platforms directly from the websites/apps. The content must also be written in a way that is suitable for social media.

Developer action: Developer must ensure a two-way integration by providing a mechanism to push content from the website/app to the social media platform and also integrate the social media content into the website/app.

Evaluator action: The evaluator shall manually test the website for verifying conformity to this checkpoint.

Statement: The language is free from spelling and grammatical errors. 5.1.25

Benefit: The language used in a government website/app is very important for ensuring effective communication with the target audiences. When website/app visitors get clear and error free content, it raises the trust level of the citizens towards the government organisation.

Government organisation action: Check the content manually or with automated spelling and grammar tools before publishing.

Developer action: Ensure provision of a CMS that enables publishing of error free content both with respect to grammar and spellings.

Evaluator action: The evaluator shall test the website/app by using a tool for verifying conformity to this checkpoint. The evaluator shall check in the backend audit for implementation of the mechanism by verifying documented records.







Accessibility 5.2

The Success criteria under this section have been adopted from W3C Web content accessibility guidelines (https://www.w3.org/TR/WCAG21/). Developers are advised to refer to the W3C website for the complete description and techniques to meet the success criteria.

Statement: All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below: 5.2.1

(a) Controls, Input: If non-text content is a control or accepts user input, then it has a name that describes its purpose (Refer to Success Criterion 4.1.2 for additional requirements for controls and content that accepts user input);

(b) Time-Based Media: If non-text content is time-based media, then text alternatives at least provide descriptive identification of the non-text content (Refer to Guideline 1.2 for additional requirements for media);

(d) Sensory: If non-text content is primarily intended to create a specific sensory experience, then text alternatives at least provide descriptive identification of the non-text content;

(e) CAPTCHA: If the purpose of non-text content is to confirm that content is being accessed by a person rather than a computer, then text alternatives that identify and describe the purpose of the non-text content are provided and alternative forms of CAPTCHA using output modes for different types of sensory perception are provided to accommodate different disabilities; and

(f) Decoration, Formatting, Invisible: If non-text content is pure decoration, is used only for visual formatting, or is not presented to users, then it is implemented in a way that it can be ignored by assistive technology.

Benefit: Conformity makes information conveyed by non-text content accessible through the use of a text alternative. For example, a person who cannot see a picture can have the text alternative read aloud using synthesised speech. A person who cannot hear an audio file can have the text alternative displayed so that he or she can read it.

Government organisation action: A meaningful explanatory text equivalent must be specified for images and other non-text content. The description should summarise the content or purpose of the image. For example, to use the description 'Picture' to explain a graphic does not serve any purpose.

Developer action: For images text equivalent can be provided by using the ALT attribute. The ALT text for an image is displayed before the image is fully downloaded. It is the main source of image information for users of text-only browsers, users of browsers with graphics turned off and users who are sight impaired. The following situations are exceptions:

(a) If the non-text content is a control or accepts input e.g., a submit button then it must have a name describing the purpose of the control;

(b) If the non-text content is time-based media (audio/video) then the text equivalent provides a descriptive identification of the same;

(c) If non-text content is a test or exercise that would be invalid if presented in text, then text alternatives at least provide descriptive identification of the non-text content;

(d) If non-text content is primarily intended to create a specific sensory experience, then text alternatives at least provide descriptive identification of the non-text content;

(e) CAPTCHA: If the purpose of non-text content is to confirm that content is being accessed by a person rather than a computer, then text alternatives that identify and describe the purpose of the non-text content are provided and alternative forms of CAPTCHA using output modes for different types of sensory perception are provided to accommodate different disabilities; and

(f) If non-text content is pure decoration, is used only for visual formatting, or is not

presented to users, then it is implemented in a way that it can be ignored by assistive technology (by using blank alt attribute).

Reference: WCAG 2.1 - 1.1.1

Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/ accessibility plug-in/web accessibility tool to check the conformity of this checkpoint.

Statement: For pre-recorded audio-only and pre-recorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labelled as such: 5.2.2

(a) Pre-recorded Audio-only: An alternative for time-based media is provided that presents equivalent information for pre-recorded audio-only content; and

(b) Pre-recorded Video-only: Either an alternative for time-based media or an audio track is provided that presents equivalent information for pre-recorded video-only content.

Benefit: The intent of this Success Criterion is to make information conveyed by pre-recorded audio-only and pre-recorded video-only content available to all users. Alternatives for time-based media that are text based make information accessible because text can be rendered through any sensory modality (for example, visual, auditory or tactile) to match the needs of the user.

Government organisation action: Create the alternate for time-based media, i.e, transcript in case audio only and transcript or audio track in case of video only content. Captions are not needed when the synchronised media is, itself, an alternate presentation of information that is also presented via text on the Web page

Developer action: Make provision to provide alternatives for time-based media.

Reference: WCAG 2.1 - 1.2.1

Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.





Statement: Captions are provided for all pre-recorded audio content in synchronised media, except when the media is a media alternative for text and is clearly labelled as such 5.2.3

Benefit: This enables people who are deaf or hard of hearing to watch synchronised media presentations.
Government organisation action: The government organisations must create captions to provide the part of the content available via the audio track. Captions not only include dialogue but identify who is speaking and include non-speech information conveyed through sound, including meaningful sound effects.
Developer action: Ensure that the captions are available with audio content.
Reference: WCAG 2.1 - 1.2.2
Evaluator action: The evaluator will test the it manually to check the conformity of this checkpoint.

Statement: An alternative for time-based media or audio description of the pre-recorded video content is provided for synchronised media, except when the media is a media alternative for text and is clearly labelled as such. 5.2.4

Benefit: provides people who are blind or visually impaired access to the visual information in a synchronised media presentation
Government organisation action: The government organisations must provide audio description of the video content. The audio description augments the audio portion of the presentation with the information needed when the video portion is not available. Alternatively, all of the information in the synchronised media (both visual and auditory) may be provided in text form. If all of the information in the video track is already provided in the audio track, no audio description is necessary.
Developer action: Developer must provide provision for publishing the alternative for time-based media or audio description of the pre-recorded video content
Reference: WCAG 2.1 - 1.2.3
Evaluator action: The evaluator will test the it manually to check the conformity of this checkpoint.

Statement: Captions are provided for all live audio content in synchronised media. 5.2.5

Benefits: Enables people who are deaf or hard of hearing to watch real-time presentations.
Government organisation action: The government organisation must provide captions for live audio content.
Developer action: Provide provision to publish captions
Reference: WCAG 2.1 - 1.2.4
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Audio description is provided for all pre-recorded video content in synchronised media. 5.2.6

Benefits: Provides people who are blind or visually impaired access to the visual information in a synchronised media presentation. During existing pauses in dialogue, audio description provides information about actions, characters, scene changes and on-screen text that are important and are not described or spoken in the main soundtrack.
Government organisation action: Provide Audio description of pre-recorded video content
Developer action: Provide provision to publish audio description
Reference: WCAG 2.1 - 1.2.5
Evaluator action: The evaluator will test it manually a check the conformity of this checkpoint.

Statement: Information, structure and relationships conveyed through presentation can be programmatically determined or are available in text. 5.2.7

Benefits: Sighted users perceive structure and relationships through various visual cues present on a page (page headings are in a larger and bold font; list items are preceded by a bullet; form fields may be positioned as groups that share text labels; a different background colour may be used to indicate related items and so on). However, visually challenged users cannot take advantage of these cues. It must be ensured that these information and relationships are preserved even when the presentation format changes. (For example, when the content is read by a screen reader or CSS is turned off or replaced).

Government organisation action: None.
Developer action: Developers must ensure that information and relationships that are implied by visual or auditory formatting are preserved when the presentation format changes. For example, when the content is read by a screen reader or when a user style sheet is substituted for the style sheet provided by the author. For example, a form contains several required fields. The labels for the required fields are displayed in red. In addition, at the end of each label is an asterisk character (*). The instructions for completing the form indicate that "all required fields are displayed in red and marked with an asterisk *", followed by an example.
Reference: WCAG 2.1 - 1.3.1
Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.

Statement: When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined. 5.2.8

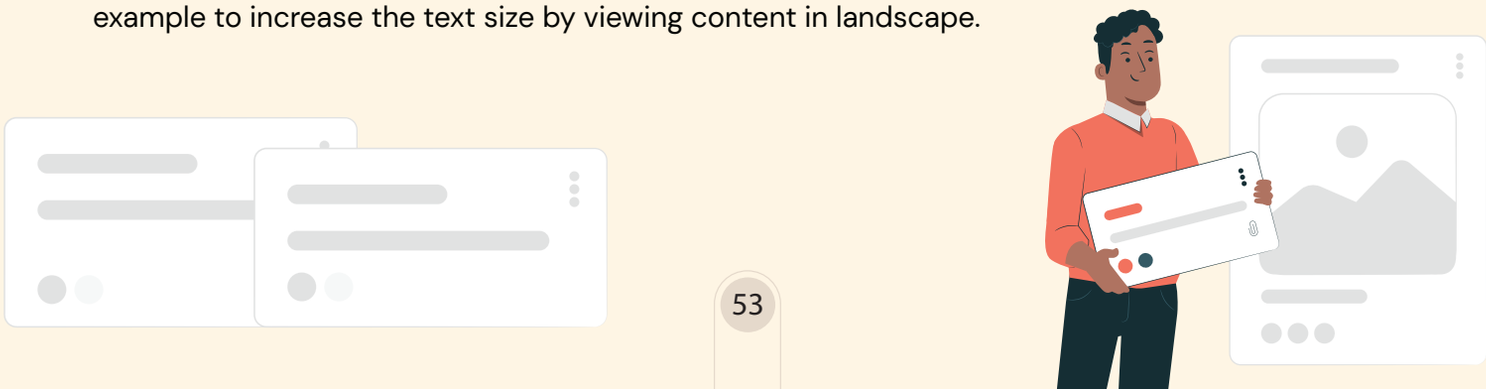
Benefits: This helps people who rely on assistive technologies like screen readers because the meaning evident in the sequencing of the information in the visual presentation will be the same when the content is presented in spoken form. This also preserves the meaning of the page when the CSS is turned off or not supported.
Government organisation action: None.
Developer action: Provide a meaningful reading sequence.
Note: Developers must keep in mind that a sequence is meaningful if change of order shall impact its meaning. Two independent content items like two separate articles in a page may be placed in any sequence without affecting the meaning. Similarly, the navigation block and the content area may be placed in any sequence without affecting their meaning. HTML text is always a meaningful sequence. Tables and ordered lists are meaningful sequences, but unordered lists are not. It must be clear that providing a particular linear order is only required where it affects meaning There may be more than one order that is "correct" and only one correct order needs to be provided.
Reference: WCAG 2.1 - 1.3.2
Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.

Statement: Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, colour, size, visual location, orientation, or sound. 5.2.9

Benefit: Many users including the visually challenged cannot perceive shape, size or use information about location or orientation. For such users the content that relies on knowledge of the shape or position of objects becomes inaccessible (for example, “round button” or “button to the right”).
Government organisation action: None.
Developer action: Provide additional information in content that relies solely on sensory characteristics of components such as shape, size, visual location, orientation, or sound. This can be done by providing textual identification of items that otherwise rely only on sensory information to be understood; for example, a round button is provided on a form to submit the form and move onto the next step. The button is labelled with the text "go." The instructions state, "to submit the form press the round button labelled go". This includes both shape and textual information to locate the button.
Reference: WCAG 2.1 - 1.3.3
Evaluator action: The evaluator will test it manually and by using the assistive technology to check the conformity of this checkpoint.

Statement: Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential. 5.2.10

Benefit: This Success Criterion requires content to display in the orientation preferred by the user and not restrict the orientation. This improves accessibility for users who rely on a specific orientation and promotes flexibility in technology design.
Users with dexterity impairments, who have a mounted device will be able to use the content in their fixed orientation.
Users with low vision will be able to view content in the orientation that works best for them, for example to increase the text size by viewing content in landscape.



Government organisation action: None.
Developer action: Developers must ensure that content displays in the orientation (portrait or landscape) preferred by the user. Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential. Examples of situations where a specific display orientation is essential could be a:
(a) Banking app that requires the device to be in landscape mode to capture an image of a check easily and accurately for deposit; and
(b) Piano app that requires the device to be in landscape mode to allow room for enough of the piano keys to be functionally usable. Since a piano app is emulating a physical piano keyboard that needs to retain relative physical characteristics between keys, either too few keys would be available, or the keys would be much too narrow.
Reference: WCAG 2.1 -1.3.4
Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.

Statement: The purpose of each input field collecting information about the user can be programmatically determined when: 5.2.11

(a) The input field serves a purpose identified in the Input Purposes for User Interface Components section; and
(b The content is implemented using technologies with support for identifying the expected meaning for form input data.

Benefit: People with language and memory related disabilities or disabilities that affects executive function and decision-making benefit from the browser auto-filling personal information (such as name or address). People with learning disability can employ assistive technology which adds icons to input fields to communicate the purpose of the fields visually and people with motor impairments also benefit from reducing the need for manual input when filling out forms.
Government organisation action: None
Developer action: Developers must ensure that the purpose of a form input collecting information about the user can be programmatically determined, so that user agents can extract and present this purpose to users using different modalities. Developers can use autofill attribute to programmatically link a pre-defined and published taxonomic term to the input, so that the inputs can also be machine-interpreted.

Reference: WCAG 2.1-1.3.5

Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.

Statement: Colour is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. 5.2.12

Benefit: Conformity to this guidelines benefits user who have difficulty perceiving colour e.g. People with partial sight or older users who do not see colour well. If a page has information that is conveyed by colour differences like: “required fields are red”, “error is shown in red” and “January sales are in red, July are in blue” then these users may not be able to access such information.

Government organisation action: None.

Developer action: Developers must ensure that when colour differences are used to convey information, such as required form fields, the information conveyed by the colour differences are also conveyed explicitly in text. Developers must provide a redundant visual cue for users who may not be able to discern a difference in text colour e.g., formatting for links on a page includes presenting them both in a different colour than the other text on the page underlining them to make the links identifiable even without colour vision.

Reference: WCAG 2.1 - 1.4.1

Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.



Statement: If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level. 5.2.13

Benefits: The ability for individuals who use screen reading software to turn off background sound provides numerous benefits. It ensures that the screen reader's speech output can be heard clearly without interference from other audio, which is especially important for those who are hard of hearing or have hearing impairments. Additionally, it benefits individuals who struggle to focus on visual content when audio is playing. This simple feature allows for a more accessible and inclusive experience for all users.
Government organisation action: None.
Developer action: Ensure that the sound that plays automatically when a page load stops within 3 seconds or provide a control at the beginning of the page to turn the sound off
Reference: WCAG 2.1 - 1.4.2
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: 5.2.14

(a) Large Text: (18 pt. or 14 pt. bold) Large-scale text and images of large-scale text have a contrast ratio of at least 3:1;
(b) Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement; and
(c) Logotypes: Text that is part of a logo or brand name has no contrast requirement.

Benefits: The contrast ratios are that they improve the readability and accessibility of text for a wider range of users, including those with visual impairments or colour deficiencies. By providing a minimum luminance contrast ratio between text and its background, text is more visible and legible, which can improve user experience and overall inclusivity.
Government organisation action: None.
Developer action: Developers must Ensure that a contrast ratio of at least 4.5:1 exists between text (and images of text) and background behind the text. It must be checked by the use of contrast

checking tools. Alternatively, they can provide a control with a sufficient contrast ratio that allows users to switch to a presentation that uses sufficient contrast

Reference: WCAG 2.1 - 1.4.3

Evaluator action: The evaluator will test it to see whether 'high contrast mode' is available and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool to check the conformity of this checkpoint.

Statement: Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality. 5.2.15

Benefits: It helps people with mild visual disabilities by allowing them to scale visually rendered text and text-based controls on a web page, without requiring the use of assistive technology. It ensures that the author creates web content that does not prevent user agents from scaling content effectively. By supporting text scaling, people with low vision can increase the size of text to a readable level, improving their ability to access and read web content.

Government organisation action: None.

Developer action: Developer must create Web content that does not prevent the user agent (e.g., browser) from scaling the content effectively. Ensuring that text containers resize when the text resizes and using measurements that are relative to other measurements in the content. Alternatively, developers may provide controls on the Web page that allow users to incrementally change the size of all text on the page up to 200 percent.

Reference: WCAG 2.1 - 1.4.4

Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/accessibility plug-in/web accessibility tool to check the conformity of this checkpoint.

Statement: If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text except for the following: 5.2.16

(a) Customizable: The image of text can be visually customised to the user's requirements;

(b) Essential: A particular presentation of text is essential to the information being conveyed;

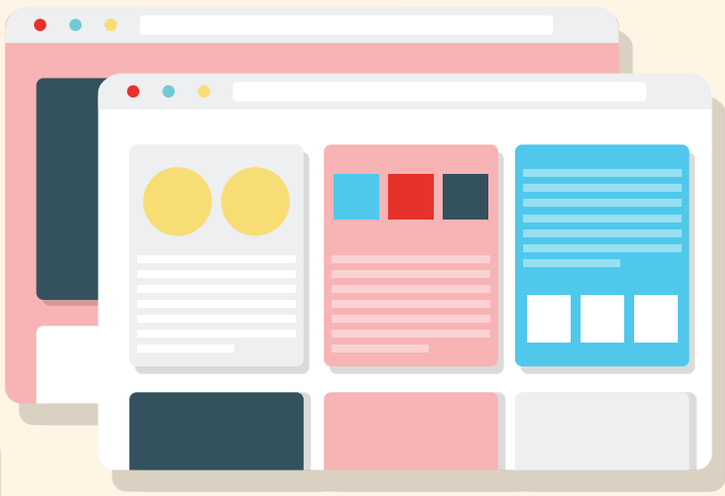
(c) Use of images for representing text should be limited.

Benefit: Though images add life to a website, they also increase downloading time. Images should only be used when it adds value to the content. Images should not be used to present text as those using text-only browsers shall not be able to access the information thus rendering the website inaccessible to many. Therefore, text must be used to convey information rather than images of text except for the cases given above. The use of text, rather than images of text, should be considered for page headings and website navigation items.
Government organisation action: Perform OCR on a scanned PDF document to capture actual text
Developer action: CSS properties like font-family, text-align, font-size etc. can be used to style text and avoid the need for text in images.
Reference: WCAG 2 1 - 1.4.5
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Content can be presented without loss of information or functionality and without requiring scrolling in two dimensions for: 5.2.17

(a) Vertical scrolling content at a width equivalent to 320 CSS pixels;
(b) Horizontal scrolling content at a height equivalent to 256 CSS pixels; and
(c) Except for parts of the content which require a two-dimensional layout for usage or meaning.

Benefits: Benefits especially to those with small screens such as mobile devices or limited screen resolutions. It ensures that content is presented in a way that is easily accessible without the need for excessive scrolling or complex navigation.
Government organisation action: None.
Developer action: Use responsive web design approach by using CSS media queries, grid or flexbox to present content without introducing a horizontal scroll bar at a width equivalent to 320 CSS pixels, or a vertical scroll bar at a height equivalent to 256 CSS pixels for text intended to scroll horizontally.
Reference: WCAG 2.1-1.4.10
Evaluator action: The evaluator will test it manually and by using the web accessibility tool to check the conformity of this checkpoint.



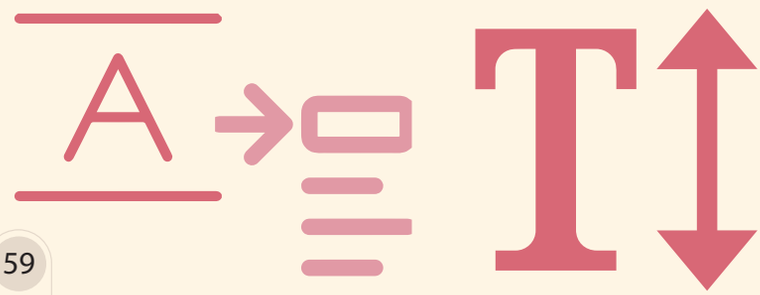
Statement: The visual presentation of the following has a contrast ratio of at least 3:1 against adjacent colour(s): 5.2.18

(a) User Interface Components: Visual information required to identify user interface components and states, except for inactive components or where the appearance of the component is determined by the user agent and not modified by the author;
(b) Graphical Objects: Parts of graphics required to understand the content, except when a particular presentation of graphics is essential to the information being conveyed.

Benefits: This benefits people with low vision or other visual impairments who may have difficulty perceiving low contrast controls and graphics and helps them better understand the content or functionality of the webpage without the need for contrast-enhancing assistive technology.
Government organisation action: None.
Developer action: Providing a control with a sufficient contrast ratio that allows users to switch to a presentation that uses sufficient contrast
Reference: WCAG 2.1- 1.4.11
Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool to check the conformity of this checkpoint.

Statement: In content implemented using markup languages that support the following text style properties, no loss of content or functionality occurs by setting all of the following and by changing no other style property: 5.2.19

(a) Line height (line spacing) to at least 1.5 times the font size;
(b) Spacing following paragraphs to at least 2 times the font size;
(c) Letter spacing (tracking) to at least 0.12 times the font size;
(d) Word spacing to at least 0.16 times the font size; and
(e) Exception: Human languages and scripts that do not make use of one or more of these text style properties in written text can conform using only the properties that exist for that combination of language and script.



Benefits: People with visual and cognitive disabilities can adjust text spacing to improve their reading experience without losing any content or functionality. By setting a minimum baseline for text styling adaptability, users can increase the spacing between lines, words, letters and paragraphs to effectively read text and other style preferences can be set. This can benefit people with low vision, dyslexia and cognitive disabilities who may require increased space between text to read or discern sections and call out boxes. Overall, this aims to improve accessibility and usability for a wider range of users.
Government organisation action: None.
Developer action: Ensure that content has the ability to be set to the above metrics without loss of content or functionality in case the user prefers to override the spacing provided by the developer
Reference: WCAG 2.1- 1.4.12
Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.

Statement: Where receiving and then removing pointer hover or keyboard focus triggers additional content to become visible and then hidden, the following are true: 5.2.20

(a) Dismissible: A mechanism is available to dismiss the additional content without moving pointer hover or keyboard focus unless the additional content communicates an input error or does not obscure or replace other content;
(b) Hover-able: If pointer hover can trigger the additional content, then the pointer can be moved over the additional content without the additional content disappearing; and
(c) Persistent: The additional content remains visible until the hover or focus trigger is removed, the user dismisses it, or its information is no longer valid.

Benefits: This benefits users with low vision, cognitive disabilities, low pointer accuracy and those who use magnification or larger mouse cursors by providing a way to view content without reducing their desired magnification or increasing the risk of triggering additional content accidentally.
Government organisation action: None.
Developer action: Ensure that content has the ability to be set to the above metrics without loss of content or functionality in case the user prefers to override the spacing provided by the developer

Reference: WCAG 2.1-1.4.13

Evaluator action: The evaluator will test it manually and by using the accessibility extension to browser/accessibility plug-in/web accessibility tool/assistive technology to check the conformity of this checkpoint.

Statement: All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints. 5.2.21

Benefits: By ensuring that content is operable through a keyboard or keyboard interface, this Success Criterion benefits people who are blind, people with low vision and individuals with hand tremors or other conditions that make using a mouse difficult. It also enables the use of operating system keyboard accessibility features, such as modifier key locking, which can further improve the accessibility of the content.

Government organisation action: None.

Developer action: Developers must Identify all functionality on the content and check that all functionalities can be accessed using only the keyboard or keyboard interface. It is important to consider functions performed using both the mouse and the keyboard together. Examples of functionality include the use of physical controls such as links, menus, buttons, checkboxes, radio buttons and form fields as well as the use of features like drag and drop, selecting text, resizing regions or bringing up context menus. This does not necessarily mean that each of the individual controls can be used from the keyboard as long as there are multiple methods to perform the same function available on the page. Developers must consider how users will discover any keyboard equivalents which are available in such a case.

Reference: WCAG 2.1 - 2.1.1

Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.



Statement: If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away. 5.2.22

Benefits: Whenever a web page is rendered using plug-ins or embedded applications, it is possible that functionality of the Web page restricts the keyboard focus to a subsection of the content, unless the user knows how to leave that state and "un-trap" the focus. This situation may affect navigation for people who rely on a keyboard or keyboard interface to use the Web, including visually challenged and people with physical disabilities.
Government organisation action: None.
Developer action: Developers must ensure that if focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface and, if it is not possible the user is advised of the method for moving focus away
Reference: WCAG 2.1 - 2.1.2
Evaluator action: The evaluator will test it manually and by using assistive technology to check the conformity of this checkpoint.

Statement: If a keyboard shortcut is implemented in content using only letter (including upper- and lower-case letters), punctuation, number, or symbol characters, then at least one of the following is true: 5.2.23

(a) Turn off: A mechanism is available to turn the shortcut off;
(b) Remap: A mechanism is available to remap the shortcut to include one or more non-printable keyboard keys (e.g., Ctrl, Alt); and
(c) Active only on focus: The keyboard shortcut for a user interface component is only active when that component has focus.

Benefits: Benefits speech users who can avoid firing batches of single-key shortcuts at once and make full use of programs that offer single-key shortcuts to keyboard users. It also benefits keyboard-only users who have dexterity challenges an d may accidentally hit keys, as they can turn off or modify problematic single character shortcuts.
Government organisation action: None.
Developer action: In case a developer has provided shortcuts in their applications to allow for faster user interaction which involve only character keys (letters, numbers, punctuation or symbol characters) without modifiers provision must be given to allow users to turn off or reconfigure shortcuts that are made up of only character keys. If the keyboard shortcut is only active when a particular user interface component has focus, then override mechanism is not required.
Reference: WCAG 2.1 – 2.1.4
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: For each time limit that is set by the content, at least one of the following is true: 5.2.24

(a) Turn off: The user is allowed to turn off the time limit before encountering it; or
(b) Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or
(c) Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the spacebar") and the user is allowed to extend the time limit at least ten times; or
(d) Real-time Exception: The time limit is a required part of a real-time event (for example, an auction) and no alternative to the time limit is possible; or
(e) Essential Exception: The time limit is essential and extending it would invalidate the activity; or
(f) 20 Hour Exception: The time limit is longer than 20 hours.

Benefits: In situations where web functions are time-dependent, (for example, filling out an online form) it will be difficult for people with disabilities such as blindness, low vision, dexterity impairments and cognitive limitations to perform the required functions before a time limit occurs. This may render the service inaccessible to them. For individuals who are deaf and communicate in sign language, having control over time limits is important when using a sign-language interpreter. Providing additional time to pause content can be helpful for those with reading and cognitive disabilities to better comprehend information.

Government organisation action: None.
Developer action: Developers must ensure that people with disabilities such as blindness, low vision, dexterity impairments and cognitive limitations are given adequate time to perform the functions that are time dependent whenever possible. The user must be allowed to turn off the time limit, adjust the default setting before encountering it or is warned before time expires and given the option to extend the time limit with a simple action (for example, "press the spacebar").
Reference: WCAG 2.1 - 2.2.1
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: For moving, blinking, scrolling, or auto-updating information, all of the following are true: 5.2.25

(a) Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and
(b) Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential.

Benefits: Avoiding content that flashes can prevent triggering seizures in people with photosensitive epilepsy.
Government organisation action: None.
Developer action: Allow the content to be paused and restarted from where it was paused or Use script to scroll content and provide a mechanism to pauseit or Create content that blinks for less than 5 seconds
Reference: WCAG 2.1 - 2.2.2
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.



Statement: Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds. 5.2.26

Benefits: Certain special effects such as blinking, or flashing have been reported to cause epileptic seizures. It is also seen that people are more sensitive to red flashing than other colours. Web pages must not contain anything that flashes more than three times in any one second period. It must also be checked that the Light/Dark status at the end of the 1- second period is the same as at the start
Government organisation action: None.
Developer action: Ensure that no component of the content flashes more than three times in any 1-second period or keep the flashing area small enough reference
Reference: WCAG 2.1 - 2.3.1
Evaluator action: The evaluator will test it manually and by using web accessibility tool to check the conformity of this checkpoint.

Statement: A mechanism is available to bypass blocks of content that are repeated on multiple Web pages. 5.2.27

Benefits: Web pages and applications often have content that is repeated on other pages or screens (for example navigation links, heading graphics, banner frames etc). A sighted user can ignore the repeated material by focusing on the main content area, but it is not possible for a person using a screen reader as the content is read sequentially.
Government organisation action: None.
Developer action: Developers must provide a mechanism to bypass blocks of content that are repeated on multiple Web pages. This may be done by:
(a) providing a link at the top of each page that goes directly to the main content area.
(b) providing a link at the beginning of the content block to go to the end of the block
(c) providing links at the top of each page that go to each area of content.
(d) Controls and programmatic focus can also be used to bypass blocks of content.
Reference: WCAG 2.1 - 2.4.1
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Web pages/app screens have titles that describe topic or purpose. 5.2.28

Benefit: This facilitates an easy and unambiguous identification of the webpage & also helps in a more relevant and visible presence in the search engine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.
Government organisation action: The government organisation must ensure that title is complete with the topic of the page. For the top-level page i.e., homepage/homescreen the name of the country must be included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Ministry of Health & Family Welfare, Government of India. Alternatively, in case of a State 'Department of Health, Government of Karnataka, India' Government Department, it should state 'Department of Health, Government of Karnataka, India'.
Developer action: there are scenarios when the Web page has a title, but the title does not identify the contents or purpose of the Web page. This may be caused because—
(a) Authoring tool default page titles, such as: "Enter the title of the HTML document here," "Untitled document" or "No title";
(b) Empty text in title;
(c) Filler or placeholder text; and
(d) A website generated using templates includes the same title for each page.
The developer should ensure that the above does not affect the page title.
Reference: WCAG 2.1 - 2.4.2
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability. 5.2.29

Benefits: When users navigate sequentially through content, they should encounter information in an order that is consistent with the meaning of the content and can be operated from the keyboard. Hence if a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components must receive focus in an order that preserves meaning and operability.

Government organisation action: Ensure correct reading order in PDF documents by structuring the document correctly in the authoring tool used to create the document before conversion to tagged PDF. Pages with complex layouts with graphics, tables, footnotes, sidebars, form fields and other elements may not convert to tagged PDF in the correct reading order. These inconsistencies must then be corrected with repair tools such as Acrobat.
Developer action: Ensure that interactive elements on a webpage receive focus in an order that follows sequences and relationships in the content. When designing the content, the interactive elements such as links and form controls must be placed in the content so that the default tab order follows the sequences and relationships in the content. Correct tab and reading order must also be ensured in PDF documents by using a tool for authoring PDF.
Reference: WCAG 2.1 - 2.4.3
Evaluator action: The evaluator will test it manually and by using the assistive technology to check the conformity of this checkpoint.

Statement: The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the of the link would be ambiguous to users in general. 5.2.30

Benefit: This helps users understand the purpose of each link so they can decide whether they want to follow the link. Assistive technology has the ability to provide users with a list of links that are on the Web page. Link text that is as meaningful as possible will aid users who want to choose from this list of links. Meaningful link text also helps those who wish to tab from link to link. Meaningful links help users choose which links to follow without requiring complicated strategies to understand the page.
Government organisation action: None.
Developer action: Developer must ensure that the text of, or associated with, the link describes the purpose of the link. In cases where the link takes one to a document or a web application, the name of the document or web application would be sufficient to describe the purpose of the link however it is not mandatory to use the name of the document or web application; other things may also describe the purpose of the link.
Reference: WCAG 2.1 - 2.4.4
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: More than one way is available to locate a web page within a set of web pages except where the web page is the result of, or a step in, a process. 5.2.31

Benefits: Providing multiple navigation options can help people find information faster, particularly those with visual or cognitive impairments. For instance, a person with a visual impairment may prefer using a search feature instead of scrolling through a large navigation bar with a screen reader. Similarly, a person with cognitive limitations may find a site map or table of contents more useful than a hierarchical navigation scheme.

Government organisation action: None.

Developer action: Developers must include either a "Search" box or a link to a "Search" page from every page of the website. The search box or link must be titled "Search", as it is a standard term understood by web surfers worldwide. As per internationally accepted Usability principles, search boxes are most effective when placed in the same position on all pages (usually within the upper third part of the webpage). Additionally, a sitemap or a link to all the pages of the website from the homepage/homescreen or a table of contents must be provided

Reference: WCAG 2.1 - 2.4.5

Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Headings and labels describe topic or purpose. 5.2.32

Benefit: It is imperative that the information and services on the website/app are well organised and categorised into relevant modules/sections and sub-sections so that any information can be located conveniently and is not buried deep inside Webpages. These sections or categories may be identified with headings or labels. Headings and Labels wherever used must correctly describe the topic or purpose of content.

Government organisation action: None.

Developer action: Developers must specify headings using HTML heading tags (H1 to H6) with proper hierarchy. When headings are clear and descriptive, users can find the information they seek more easily and they can understand the relationships between different parts of the content more easily. Developers must also provide descriptive labels to help users identify specific components within the content. Labels and headings do not need to be lengthy. A single word may suffice if it provides an appropriate cue to finding and navigating content.

Reference: WCAG 2.1 - 2.4.6

Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible. 5.2.33

Benefit: This helps the user know which element among the multiple elements present in the page has focus. For e.g., in case of a button a visual change in the button (e.g., colour, size) can indicate that the focus is on the button.
Government organisation action: None.
Developer action: When standard controls are used the users are informed of the focus location in a standard, predictable way. Visual appearance may also be enhanced via style sheets to provide visual feedback when an interactive element has focus or when a user hovers over it using a pointing device.
Reference: WCAG 2.1 - 2.4.7
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: All functionality that uses multipoint or path-based gestures for operation can be operated with a single pointer without a path-based gesture, unless a multipoint or path-based gesture is essential. 5.2.34

Benefit: This is particularly beneficial for those with cognitive or learning disabilities who may not understand custom gesture interactions. The benefits of providing alternative means for operating touchscreen or mouse-based content, particularly for users who may have physical, cognitive, or learning disabilities that these users can still effectively interact with the content. This can help to ensure that digital experiences are more inclusive and accessible for all users.
Government organisation action: None.
Developer action: Developer must provide controls to achieve the same result as path based or multipoint gestures
Reference: WCAG 2.1-2.5.1
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.



Statement: For functionality that can be operated using a single pointer, at least one of the following is true: 5.2.35

(a) No Down-Event: The down-event of the pointer is not used to execute any part of the function;
(b) Abort or Undo: Completion of the function is on the up-event and a mechanism is available to abort the function before completion or to undo the function after completion;
(c) Up Reversal: The up-event reverses any outcome of the preceding down-event;
(d) Essential: Completing the function on the down-event is essential.

Benefits: This will help users to prevent accidental or erroneous pointer input by allowing them to cancel pointer operations. The preferred method for cancellation is the up-event, which occurs when a touchscreen or mouse pointer is released. This will benefit all users by reducing the chance of accidental activation and ensuring a means of undoing or aborting an action is available.
Government organisation action: None.
Developer action: Incorporate pointer cancellation by making activation occur on the up-event. This can be done by using the default behaviour of controls and not override that behaviour with an explicit down-event trigger. The up-event is the default behaviour for almost all controls and any programming or markup language. Also, for drag and drop events it must be ensured that users who use a path-based drag-and-drop action to move an item from the initial location to a drop target can abort the action after picking up the target. This can be done either by releasing the item outside a drop area, or by moving the item back to its original position in a separate action that undoes the first action e.g., a website shows a file directory. Files can be picked up and moved over a trash can icon. When the picked-up file is released outside this target, it reverts to the old position.
Reference: WCAG 2.1- 2.5.2
Evaluator action: The evaluator will test the website manually to check the conformity of this checkpoint.



Statement: For user interface components with labels that include text or images of text, the name contains the text that is presented visually. 5.2.36

Benefits: This will allow users with disabilities to interact with the components using speech recognition or text-to-speech technologies more easily and with greater predictability. It is important to determine which text on the screen should be considered a label for any given control and to bias towards treating only the adjacent text as a label. The benefits of implementing this Success Criterion include more efficient navigation for speech-input users and a better experience for text-to-speech users.
Government organisation action: None.
Developer action: Ensure that the words and characters in the visible label of a control match or are contained within the programmatic name, also known as the Accessible Name.
Reference: WCAG 2.1- 2.5.3
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Functionality that can be operated by device motion or user motion can also be operated by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: 5.2.37

(a) Supported Interface: The motion is used to operate functionality through an accessibility supported interface;
(b) Essential: The motion is essential for the function and doing so would invalidate the activity;
(c) Functionality that can be operated by device motion or user motion must also be operable by user interface components and responding to the motion can be disabled to prevent accidental a ctuation, except when:
(i) Supported Interface: The motion is used to operate functionality through an accessibility supported interface;
(ii) Essential: The motion is essential for the function and doing so would invalidate the activity.



Benefits: This will help users with disabilities who may not be able to use device sensors or perform certain movements, as well as users who are unable to move their devices. By providing alternative methods of operating all functionality, this success criterion ensures that everyone can access and use web content.
Government organisation action: None.
Developer action: In Devices that have sensors that can act as inputs, (such as accelerometer and gyroscope sensors on a phone or tablet device) and allow the user to control something by simply changing the orientation or moving the device in particular ways the functionality offered through motion must also be available by another mechanism. The user must also have the ability to turn off motion actuation to prevent accidental triggering of functions due to tremors or other motor impairments.
Reference: WCAG 2.1- 2.5.4
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: The default human language of each Web page can be programmatically determined. 5.2.38

Benefits: This ensures that users with disabilities, who rely on assistive technologies to access the content, can understand it better. It benefits people who have difficulty reading written material or recognizing characters and alphabets, those with certain cognitive or learning disabilities who use text-to-speech software and those who rely on captions for synchronised media.
Government organisation action: None.
Developer action: Default language of the page must be indicated programmatically by the use of the lang attribute. In PDF document default language can be set using the Lang entry in the document catalogue. Specifying the default language in the HTTP header in relevant situations can be considered.
Reference: WCAG 2.1 - 3.1.1
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.



Statement: The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language and words or phrases that have become part of the vernacular of the immediately surrounding text. 5.2.39

Benefits: This will help people who have difficulty reading, recognizing characters and alphabets, decoding words and understanding phrases, as well as people with certain cognitive, language and learning disabilities who use text-to-speech software.
Government organisation action: None.
Developer action: If there are any changes in the default language of the document, either in the document's text or any text equivalents (e.g., captions), they also be clearly identified using the lang attribute. The language for a passage or phrase can be specified with the Lang entry in PDF documents.
Reference: WCAG 2.1 - 3.1.2
Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/ Accessibility plug-in/Web Accessibility tool/ Assistive Technology to check the conformity of this checkpoint.

Statement: When any user interface component receives focus, it does not initiate a change of context. 5.2.40

Benefits: This aims to prevent unexpected context changes that can be especially problematic for people with visual disabilities, cognitive limitations and motor impairments. By ensuring that focus changes are predictable and consistent, this improves the usability and accessibility of web content.
Government organisation action: None.
Developer action: Ensure that all changes of context are triggered only by a specific action on the part of the user. Further, that action is the one that usually causes changes in context, such as clicking on a link or pressing a submit button. Actions that simply move the focus to an element must not cause a change of context.
Reference: WCAG 2.1 - 3.2.1
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behaviour before using the component. 5.2.41

Benefits: It helps users with visual and cognitive disabilities by providing additional cues to detect changes of context, reducing the chances of disorientation and enhancing their ability to use the content. Users who are unable to detect changes of context are less likely to become disoriented while navigating a site, making the content more accessible to a wider range of users.
Government organisation action: None.
Developer action: Provide a submit button to initiate a change of context or if change in context occurs provide information to users about what will happen when a change to a form control results in a change of context
Reference: WCAG 2.1 - 3.2.2
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user. 5.2.42

Benefits: This is particularly helpful for individuals with low vision who use screen magnification or visual cues to navigate the website. Ensuring that repeated components occur in the same order on each page of a website helps users with cognitive limitations, intellectual disabilities and those who are blind to become comfortable with the website's structure and easily find what they are looking for.
Government organisation action: None.
Developer action: Ensure presenting components that are repeated in web pages in the same relative order each time they appear. Other components can be inserted between them, but their relative order is not changed. Similarly in navigational components links or programmatic references must be presented inside a navigational component in the same relative order each time the navigational component is repeated. Other links can be removed or inserted between the existing ones, for example to allow navigation inside a subsection of a set of Web pages, but the relative order is not changed.
Reference: WCAG 2.1 - 3.2.3
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: Components that have the same functionality within a set of Web pages are identified consistently. 5.2.43

Benefits: This will help people who use screen readers to navigate and operate a website more easily, as they rely on their familiarity with functions that may appear on different pages. It also benefits people with cognitive limitations and those who have difficulty reading or detecting text alternatives. Consistent labelling and text alternatives enable people to find desired functions on other pages if they are present, interact with non-text content in a consistent way and have a more predictable and consistent experience while navigating a website.
Government organisation action: None.
Developer action: Apply consistent labels on user interface components (i.e., elements, links, JavaScript objects, etc.) that have the same function e.g., A Web page has a form field at the top of the page labelled "Search". On the bottom of the page is another form field which provides the same function. It is also labelled "Search."
Reference: WCAG 2.1 - 3.2.4
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text. 5.2.44

Benefits: This helps users, including those who are blind or have cognitive or learning disabilities, to understand that an error has occurred and how to correct it. By providing text-based error messages, users who cannot perceive visual cues, such as colour or icons, are also able to understand the error message. This improves the accessibility of web forms and makes them more usable for a wider range of users.
Government organisation action: None.
Developer action: Error must be identified to the user in text. It is perfectly acceptable to indicate the error in other ways such as image, colour etc, in addition to the text description.
Reference: WCAG 2.1 - 3.3.1
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.



Statement: Labels or instructions are provided when content requires user input. 5.2.45

Benefits: This benefits user, especially those with disabilities, by providing clear and unambiguous instructions that help them enter information correctly and avoid incomplete or incorrect form submissions. The goal is to provide enough information for users to accomplish tasks without undue confusion or navigation, without cluttering the page with unnecessary information.
Government organisation action: None.
Developer action: Developers must present instructions or labels that identify the controls in a form so that users know what input data is expected. In the case of radio buttons, checkboxes, combo boxes, or similar controls that provide users with options, each option must have an appropriate label. Instructions or labels may also specify data formats for data entry fields, especially if they are out of the customary formats or if there are specific rules for correct input. Developers may also make such instructions available to users only when the individual control has focus, especially when instructions are long and verbose.
Reference: WCAG 2.1 - 3.3.2
Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/ Accessibility plug-in/Web Accessibility tool to check the conformity of this checkpoint.

Statement: If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardise the security or purpose of the content. 5.2.46

Benefits: This will help users with disabilities to understand how to correct errors and fill in forms successfully. Providing information about how to correct input errors can benefit users with learning disabilities, visual impairments and motion impairments by making it easier for them to understand the nature of the error and how to correct it and reducing the number of times they need to change an input value. This improves the overall accessibility and usability of it or application for a wider range of users.
Government organisation action: None.
Developer action: Provide text descriptions to identify required fields that were not completed while submitting a form or provide the correct format if the values entered in a field have an incorrect format.
Reference: WCAG 2.1 - 3.3.3
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

Statement: For webpages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: 5.2.47

(a) Submissions are reversible;
(b) Data entered by the user is checked for input errors and the user is provided with an opportunity to correct them; and
(c) A mechanism is available for reviewing, confirming, and correcting information before finalising the submission.

Benefits: This benefits users with disabilities who may be more likely to make mistakes due to reading or motor impairments and helps prevent costly errors that could result in financial loss or data loss. By providing safeguards to avoid serious consequences, this success criterion improves the accessibility and usability of it or application for all users, not just those with disabilities.
Government organisation action: None.
Developer action: Provide safeguards as above to avoid serious consequences resulting from mistakes helps users with all disabilities who may be more likely to make mistakes.
Reference: WCAG 2.1 - 3.3.4
Evaluator action: The evaluator will test it manually to check the conformity of this checkpoint.

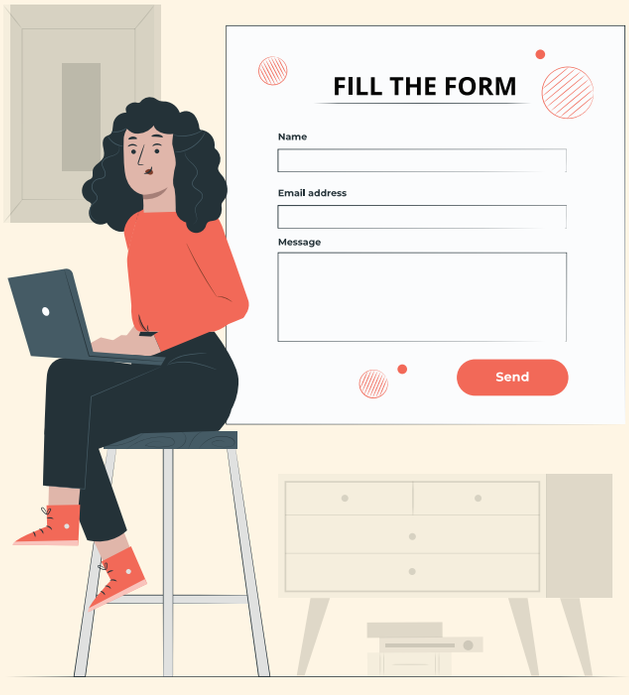
Statement: In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes and any IDs are unique, except where the specifications allow these features. 5.2.48

Benefits: This will help prevent different user agents from rendering the content differently or being unable to parse it, which can lead to accessibility issues for users with disabilities. By requiring that web content be correctly structured, with complete start and end tags and proper nesting, this helps ensure that assistive technologies can parse the content accurately and without crashing, which improves the accessibility and usability of the website or application for all users.
Government organisation action: None.

Government organisation action: None.
Developer action: Developers must validate the markup to ensure that it is as per the standards
Reference: WCAG 2.1 - 4.1.1
Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/ Accessibility plug-in/Web Accessibility tool to check the conformity of this checkpoint.

Statement: For all user interface components (including but not limited to form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies. 5.2.49

Benefits: This ensures that user interface controls in web content can be accurately interpreted and controlled by assistive technologies. By providing role, state and value information for all user interface components, people with disabilities who use assistive technology such as screen readers or speech recognition software can more easily access and navigate web content. This can improve their overall user experience and help them more fully participate in online activities.
Government organisation action: None.
Developer action: Developers who develop or script their own user interface components must provide role, state and value information on all such components
Reference: WCAG 2.1 - 4.1.2
Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/ Accessibility plug-in/Web Accessibility tool/ Assistive Technology to check the conformity of this checkpoint.



Statement: In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus. 5.2.50

Benefits: It benefits blind and low vision users of assistive technologies by enabling compatibility with screen readers and may also benefit users with cognitive disabilities. Properly assigning roles or properties to status messages allows for possible future uses and personalization opportunities, while also providing additional information to users without affecting their current point of regard. Additionally, assistive technologies may choose to delay, suppress, or transform such messages based on the user's preferences.

Government organisation action: None.

Developer action: The status message provides information to the user on the success or results of an action, on the waiting state of an application, on the progress of a process, or on the existence of errors; the message is not delivered via a change in context.

Reference: WCAG 2.1– 4.1.3

Evaluator action: The evaluator will test it manually and by using the Accessibility extension to browser/ Accessibility plug-in/Web Accessibility tool/ Assistive Technology to check the conformity of this checkpoint.







Cybersecurity 5.3

Protecting web resources from unauthorised use, access, changes, destruction, or disruption is generally termed as “Website Security” or “Secured Website”.

Sometimes web resources become unavailable due to denial-of-service attacks or display modified information on the webpages. Millions of passwords, email addresses and credit card details have been leaked into the public domain exposing web users to both personal embarrassment and financial risks. The purpose of Website Security is to prevent such risks.

Website Security requires vigilance in all aspects starting from design, coding and implementation to testing and deployment. Organisations should implement appropriate security majors, defences and countermeasures to protect web resources against malfunctioning, phishing, cyber-crimes or cyberattacks to avoid

data loss of the organisations or users.
The government organisation will ensure and monitor that the host service provider and the developer adhere to the industry best security practices and guidelines such as ISO 27001, OWASP ASVS, OWASP Top 10 vulnerabilities and CIS benchmarks as per the prevailing security policy. Following guidelines are to secure web resources & associated infrastructure:

Statement: Website, web application, web portal or mobile app have been Security Audited and an Audit Clearance certificate has been issued by NIC/ STQC/ STQC empanelled laboratory/CERT -In empanelled laboratory before hosting in production environment. 5.3.1

Benefits: The goal of securing a website, web application, web portal or mobile app is to maintain the confidentiality, integrity and availability of information and services. This goal is accomplished through the implementation of best security practices in design, development and deployment. Attacks could cause both personal embarrassment and financial risks.
Government organisation action: It should be ensured that the website, web application, web portal or mobile app don't have any security risks as identified by the latest OWASP Top 10 vulnerability list. The design and development agency or the developers should follow industry best practices such as OWASP ASVS and OWASP MAVS.
Developer action: Securing critical web resources is more important than ever as the focus of attackers has steadily moved towards the application layer and they are exploiting the weaknesses in the code.

A. Securing Code

(a) Ensure that all websites, web applications, web portals or mobile apps and their respective CMS, 3rd party plugins, codes, etc. are updated to the latest vers ions.

Note: Every day, there are countless websites/apps compromised due to outdated software. Potential hackers and bots are scanning websites/apps to attack. Updates are vital to the health and security of the website/app. If the website's software or applications are not up-to-date, the website/app is not secure. Take all software and plugin update requests seriously. Updates often contain security enhancements and vulnerability repairs. Check the

website/app for updates or add an update notification plugin. Some platforms allow automatic updates, which is another option to ensure website/app security. Longer the wait to update, lesser the secure. Keeping the website/app up-to-date and its components should be on top priority.

(b) All passwords, connection strings, tokens, keys, etc. should be encrypted with salted hash. There should not be any plain passwords stored in config files or source code or in a database.

(c) All exceptions should be handled appropriately. Custom error pages should be displayed for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception.

(d) HTTP Response Headers should be obscured.

(e) Cookies should be secure and HTTP only.

(f) Configure captcha for login pages.

(g) Directory traversal should be disabled. In case of any specific attempt by a user to access a portion of the code by typing the URL path (ex: www.xxx.gov.in/js/custom.js) then the same should be redirected to a custom error page.

(h) All default user names and IIS/Apache pages (like admin, default.aspx, index.aspx, etc.) should be renamed. The access URL for the admin panel/CMS, should also be renamed.

(i) The Web Server processes should not be running under Administrator or Root user Account. A dedicated User account with limited privileges should be used for the Web Server Processes.

Note: Not every webmaster knows which web server they use. Use a website scanner like Site Check to check the website for known malware, viruses, blacklisting status, website errors and more. The more one knows about the current state of website security, it's better as it gives time to fix the issues before any harm comes to it.

(j) If the web or mobile app is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channels.

(k) Enforce strong password management policy, secure password recovery mechanisms and multi-factor authentication (MFA) for user login to website, web application or web portal infrastructure.

(l) Implement role-based access control and minimal privilege policy for users as per need from the system.

(m) Establish the secure coding practices document based on leading practices such as OWASP for code development. Below is an indicative checklist that can be considered for secure code development:

(i) Input Validation

(ii) Authentication & Password Management

(iii) Session Management

(iv) Access Control
(v) Cryptographic Practices
(vi) Error Handling & Logging
(vii) Data Protection
(viii) Communication Security
(ix) System Configuration
(x) Database Security
(xi) File Management
(xii) Memory Management

(n) Implement logging functionality and periodically auditing the web logs for suspicious activity.

(o) Configure website, web application or web portal caching to optimize resource availability.

(p) Sanitise user input at both the client end and the server end with both syntactical as well as a semantic approach.

(q) The technology to be implemented should be chosen after careful consideration. Various client-side Active Content Technologies are available e.g., Java scripts etc. Each has its own strengths and weaknesses along with an associated risk.

(r) Disable the root user access to run the code on Linux/Unix hosts.

(s) Use explicit path names when invoking external programs and not rely on the PATH environment value.

B. Securing databases: Database being the core of any application and/or organisation and is used to store large amounts of highly sensitive and personal information. Therefore, appropriate technical controls should be in place to safeguard the databases and information stored in them. The following are the guidelines for securing databases:

(a) Implement strong encryption and key management mechanism for the information both at rest and transit.

(b) Implement strong hashing and salting algorithms to store passwords in the database.

(c) Use secure credentials for database access. Remove or change all default database administrative passwords.

(d) Utilise strong passwords//phrases or implement multi-factor authentication.

(e) Disable unnecessary accounts such as orphaned accounts, unused accounts, generic and service accounts.

(f) Enable access to the database only from the Web Server on a whitelisted port and it should not be assigned publicly accessible IP.

(g) TLS should be enabled in databases for secure communications between web servers and databases.

(h) Create admin restrictions, such as by controlling privileged access on what users can do in a database.

(i) The application should use the lowest possible level of privilege when accessing the database.

(j) Turn on node checking to verify applications and users.

(k) Turn off all unnecessary database functionality (e.g., unnecessary stored procedures or services, utility packages, install only the minimum set of features and options required (surface area reduction)

(l) Enforce a strict access control policy and introduce role-based access control (RBAC) privileges.

(m) Enable audit trail logs on the database servers.

(n) Ensure appropriate logging and monitoring of database logs.

(o) Consider fine grained record/row level auditing based on the sensitivity of data.

(p) Implement a backup solution to store data and system configurations from the website, web application or web portal that should be backed up periodically.

Note: One of the best methods to keep a website/app safe is to have a good backup solution and the user should have more than one data backup. Each of these two backups is crucial to recovering a website after a major security incident occurs. There are several different solutions one can use to help recover damaged or lost files. Keep the website information off-site. Do not store the backups on the same server as of the website; they are as vulnerable to attacks too. Choose to keep the website backup on a home computer or hard drive. Find an off-site place to store the data and to protect it from hardware failures, hacks and viruses. Another option is to back up the website in the cloud. It makes storing data easy and allows access to information from anywhere. Besides choosing where to back up the website, one must consider automating them. Use a solution where one can schedule the website/app backups. It has to be ensured that the solution has a reliable recovery system. Be redundant in the backup process — backup the backups. By doing this, one can recover files from any point before the hack or virus occurs.

(q) Keep the backup media file in safe custody and access to it should be restricted and logged.

(r) Conduct periodic auditing of Web Application - at least once in a year or as and when any changes are done in the source code, whichever is earlier.

(s) Report any web application-related security incidents observed to NIC-CERT & CERT-In immediately at Incident Response Helpdesk:

NIC-CERT: incident@nic-cert.nic.in

CERT-In: incident@cert-in.org.in

Toll free phone: CERT-In - +91-1800-11-4949

Evaluator action: The evaluator shall check that the website/ web application/ web portal/ mobile app under evaluation has a valid security audit certificate issued by NIC/STQC/STQC empanelled laboratory/ Cert-IN empanelled laboratory fulfilling Cert-IN requirements.

Statement: Hosting Environment has been secured for ensuring confidentiality, integrity and availability (CIA). 5.3.2

Benefits: The goal of securing a hosting environment is to maintain the confidentiality, integrity and availability of information resources leading to successful operations. This goal is accomplished through the implementation of security controls. Hosting service providers should follow industry best practices for securing the hosting environment. Attacks could cause both personal embarrassment and financial risks. Secure hosting as well as doing regular backups save the time and money put into the site.

Government organisation action: Think of a website's domain name as a street address. Now, think of the web host as the plot of "real estate" where the website exists online. As one would research a plot of land to build a house, it needs to examine potential web hosts to find the right one. Many hosts provide server security features that better protect a website and its data.

A. There are certain mandatory aspects to check for when choosing a hosting service provider (HSP):

(a) Ensure the hosting of the web infrastructure within geographical boundaries of India.

(b) The government organisation to ensure the HSP is providing data centre, business continuity plan and disaster recovery environments with state-of-the-art secure infrastructure configured in high availability (HA) mode for hosting the websites, web applications, web portals or mobile apps and their respective CMS.

(c) Conduct periodic drills of disaster recovery environment - at least once in a year.

(d) HSP to ensure that the servers are protected against environmental, physical and cyber threats.

(e) Ensure the HSP has implemented all security controls of the Data Centre including physical security and appropriate access control mechanisms.

(f) Servers, Network devices used to host the website should be hardened with latest security patches and periodic Vulnerability Assessment (VA) and Penetration Testing (PT) followed by corrective actions should be performed as per the security policy.

(g) Ensure the HSP of the hosting environment has deployed and configured a Web Application Firewall (WAF), which is hardened with latest security patches and is available for use by the government organisation on demand.

> **Note:** It sits between the website server and the data connection. The purpose is to read every bit of data that passes through it to protect the site. Most WAFs are cloud-based and are a plug-and-play service. The cloud service is a gateway to all incoming traffic that blocks all hacking attempts. It also filters out other types of unwanted traffic, like spammers and malicious bots.

(h) Enable and maintain logs of the ICT infrastructure for a rolling period of 180 days as per CERT-In directions.

(i) Regularly monitor and conduct review of alerts and logs

(j) HSP should also ensure:

(i) Web host offer a Secure File Transfer Protocol (SFTP);

(ii) FTP use by unknown users is disabled; and

(iii) It uses a rootkit scanner.

(k) HSP should ensure to secure the containerized environments, if applicable.

Note: Containerized Workloads are much more complex than traditional workloads. Production environments deploy massive amounts of containers. Security experts and administrators need to secure more components in a containerized environment than they would in traditional deployments. Container security involves the implementation and maintenance of security controls that protect containers and the underlying infrastructure. Integrating security into the development pipeline can help ensure that all components are secured from the initial development phase and until the end of their lifecycle.

B. Best practices should be used to protect the containerized environments:

(a) Each library and tool pulled into the image poses a potential threat. To mitigate these threats, one need to include the application within the container image. This should be a statically compiled binary that contains all required dependencies.

(b) Remove all components the application does not need. For example, remove the “sed” and “awk” binaries, which are present by default on any UNIX system. This can help reduce the attack surface.

(c) If the image is not created from scratch, only trustworthy images should be taken. Public image repositories, such as Docker Hub, can be used by anyone and may contain malware or misconfigurations.

(d) If there is a private registry, the system administrator has to establish access controls that define exactly who can access and publish images and who cannot perform such actions.

(e) Signatures help track images to the people who signed them. This makes it difficult to substitute the signed image for a compromised one. The Docker Content Trust mechanism provides information about signing images. Notary - an open-source tool can help sign and verify images.

(f) Vulnerability scanners are designed to identify known vulnerabilities. These tools can help find critical vulnerabilities and detect critical threats. Scanners can be used on a continuous basis to ensure that the registries do not contain critical vulnerabilities.

(g) Secure the target environment – by hardening the underlying host operating system. It can also be established that the firewall and VPC rules or create special accounts that limit access.

(h) Use an orchestration platform – These systems usually provide secure API endpoints as well as role-based access control (RBAC), which can help minimise the risk of unauthorised access.
(i) Use immutable deployments – This involves creating an instance image during the build steps. The deployment can then use this image to create new instances. To update the application, new images should be created, spin up new instances and then destroy the old ones.
(j) Create separate virtual networks for the containers – This introduces a level of isolation that can reduce the attack surface.
(k) Apply the principle of least privilege – Allow connectivity only between containers that truly need it.
(l) Expose only the ports that serve the application – Do not expose any other ports, except for SSH. Apply this principle to containers as well as the underlying machines.
(m) Use TLS to secure communication between services – This process encrypts traffic and ensures only authorised endpoints are allowed.
(n) Use the Docker Image policy plugin – This plugin is designed to prevent any process from pulling images that were not previously allow-listed.
(o) Enable TLS everywhere – enable TLS for all supported components to defend against traffic sniffing and authenticate identities at both ends of each connection.
(p) Use a service mesh architecture – Service meshes are networks of persistent encrypted connections between high-performance sidecar proxies. They provide traffic monitoring, management and policy enforcement without affecting microservices.
(q) Use OPA – Open Policy Agent (OPA) enforces custom policies on a Kubernetes object without reconfiguring or recompiling the Kubernetes API server.
(r) Apply network policies – The default Kubernetes networking permits all traffic between pods, but can be restricted with a network policy.
(s) Implement private networks – Deploy each Kubernetes worker and master node on a private subnet to secure the connections to corporate networks, make nodes unreachable from the public Internet and minimise overall attack surface.
(t) Keep the etcd cluster separate – Use a firewall to protect the etcd cluster, which stores state and secret information and requires special protection compared to other Kubernetes components.
(u) Ensure the regular rotation of encryption keys – Regularly rotating encryption keys and certificates helps minimise the blast radius of an attack that compromises keys.
(v) Use static analysis for YAML – Statically analyse where pod security policies deny access to API servers. This should be part of the development workflow because it helps identify the organisation's risk tolerance and conformity requirements.
(w) Manage secrets – Integrate clusters using a secret management system to ensure application pods automatically receive all secrets and passwords needed at runtime (based on the app roles

associated with each pod).

(x) Check the code – Scan the code and use static analysis to ensure automation security. Source code must be scanned for all application code in Kubernetes to identify vulnerabilities and hard-coded errors.

(y) Use RBAC policies based on the principle of least privilege – Role-based access control (RBAC) helps manage access policies at a granular level to protect resources. A centralised authentication and authorization system like single sign-on throughout the organisation makes onboarding and offboarding easier.

Developer action: Following activities are to be ensured by the developer, which in this case would mean its system administrator, or/and DevOps:

(a) Restrict the admin access and implement the principle of least privilege and disable unnecessary accounts and privileges;

(b) Disable all unnecessary ports opened on the web server, i.e., deny all access by default;

(c) Remove default, temporary or guest accounts from the web server; and

(d) Change the default login credentials and implement strong password enforcement with password expiration policy on the web server.

> **Note:** With there being so many websites/apps, databases and programs needing passwords, it is hard to keep track. A lot of people end up using the same password in all places, to remember their login information. But this is a significant security mistake. Create a unique password for every new login request. Come up with complicated, random and difficult to guess passwords. Then, store them outside the website directory. For example, a 14-character combination of letters and numbers may be used as a password. The password may be stored in an offline file, a smartphone, or a different computer. When CMS prompts the user to log in, the user must choose a smart password. The user should refrain from using personal information in the password. The user should not use her/his birthday or a pet's name and it should not be guessable. After every three months or sooner, the password may be changed. Smart passwords are long and should be at least 12 characters. Besides numbers and letters, a password should also include symbols. The uppercase and lowercase letters may be alternated. The same password should not be repeated and nor should it be shared with others. The system administrators should ensure that organisation employees change their passwords frequently.

(e) Whitelist the application in use and disable the unused features or modules.

(f) Use of Secure FTP (SFTP) to transfer files over an encrypted channel.

(g) Disable Hypertext Transfer Protocol (HTTP) and enforce Hypertext Transfer Protocol Secure (HTTPS) & HTTP Strict Transport Security (HSTS). To keep a website safe, it needs a secure URL. If a

user uses their private information to access a site, it should use HTTPS, not HTTP, to deliver it.

Note: HTTPS (Hypertext Transfer Protocol Secure) is a protocol used to provide security over the Internet. HTTPS prevents interceptions and interruptions from occurring while the content is in transit. To create a secure online connection, a website also needs an SSL Certificate. If the website asks visitors to register, sign-up, or make a transaction of any kind, the connection must be encrypted. SSL (Secure Sockets Layer) is another necessary website protocol. This transfers visitor's personal information between the website and the database. SSL encrypts information to prevent it from others reading it while in transit. It denies those without proper authority the ability to access the data, as well. GlobalSign is an example of an SSL certificate that works with most websites.

(h) Mandatorily use a valid SSL Certificate on all websites. The SSL Certificate should use at least 2048-bit SHA 256 encryption or higher.

(i) Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry.

(j) Configure the HTTP Service banner so that Web Server and Operating System type & version will not be disclosed.

(k) The configuration files of the Web Server must be protected by the Web Server process. One can find them in the root web directory. Web server configuration files permit to administer server rules. This includes directives to improve website security. There are different file types used with every server, following may be referred for their usage:

(i) Apache web servers use the .htaccess;

(ii) Nginx servers use nginx.conf; and

(iii) Microsoft IIS servers use web.config.

(l) Open source/Freeware software should be used with due diligence.

(m) Remove or disable all superfluous drivers, services and software.

(n) Remove or replace obsolete software libraries.

(o) Remove or replace outdated security level protocols.

(p) Limit unauthorised or unauthenticated or administrative privileged user access to the system.

Note: Initially, one may feel comfortable giving several high-level employees access to a website. Administrative privileges are given thinking those would be used carefully. Although this is the ideal situation, it is not always the case. Unfortunately, employees do not think about website security when logging into the Servers or the CMS. Instead, their thoughts are on the task at hand. If they make a mistake or overlook an issue, this can result in a significant security issue. It is vital to access employees before giving website access. Find out if they have experience using the CMS and if they know what to look for to avoid a security breach.

Educate every CMS user about the importance of passwords and software updates. Tell them all the ways they can help maintain the website's safety. To keep track of who has access to CMS and their administrative settings, make a record and update it often. Employees come and go. One of the best ways to prevent security issues is to have a physical record of who does what with the website. Be sensible when it comes to user access.

(q) Implement encryption for the transmission of all sensitive information. This should include TLS for protecting the connection. Disable weak cyphers (SSLv2, SSlv3, 3DES, RC4, TLS v1.0, v1.1).

(r) Periodically review logs for suspicious activity like authentication, user access activity & changes and privilege elevation & usage.

(s) Implementation of network segmentation and segregation to limit the impact of network intrusion.

(t) There should be no active concurrent sessions of the web server.

(u) Ensure servers, frameworks and system components are running the latest approved version and have all patches issued for the version in use.

(v) Isolate development environments from the production network and provide access only to authorised development and test groups.

(w) Implement a software change control system to manage and record changes to the code both in development and production.

(x) Establish practice of hardening web servers and conduct the periodic secure configuration review of the same.

(y) The most common attacks against websites are entirely automated. What many attack bots rely on is for users to have their CMS settings on default. After choosing a CMS, change default settings immediately. Changes help prevent a large number of attacks from occurring. CMS settings can include adjusting control comments, user visibility and permissions e.g., default setting change using 'file permissions.' Permissions can be changed to specify who can do what to a file. Each file has three permissions and a number that represents every permission:

(i) 'Read' (4): View the file contents.

(ii) 'Write' (2): Change the file contents.

(iii) 'Execute' (1): Run the program file or script.

(iv) To clarify, to allow multiple permissions, add the numbers together e.g., to allow read (4) and write (2), set the user permission to (6.) Along with the default file permission settings, there are three user types:

(I) Owner – Often, the creator of the file, but ownership can be changed. Only one user can be the owner at a time.

(II) Group – Each file is assigned to a group. Users who are part of that specific group will gain access to the permissions of the group.

(III) Public – Everyone else.

(z) Customise users and their permission settings. Do not keep the default settings as is, otherwise it shall run into website security issues at some point.

Evaluator action: The evaluator shall check to ensure that the Government organisation actions are being complied.

Statement: Website has the Security Policy, Privacy Policy and the Contingency Management Plan clearly defined policies and plans approved by the government organisation. 5.3.3

Benefits: Having clearly defined policies helps ensure efficient management of the website/app and its content throughout the life cycle of the website.

Government organisation action: Clearly define and approve the website/app related policies listed above. Web Information Manager must ensure their implementation throughout the website/app life cycle.

Developer action: Citizen-facing policies like copyright policy, privacy policy and terms and conditions must be published on the website.

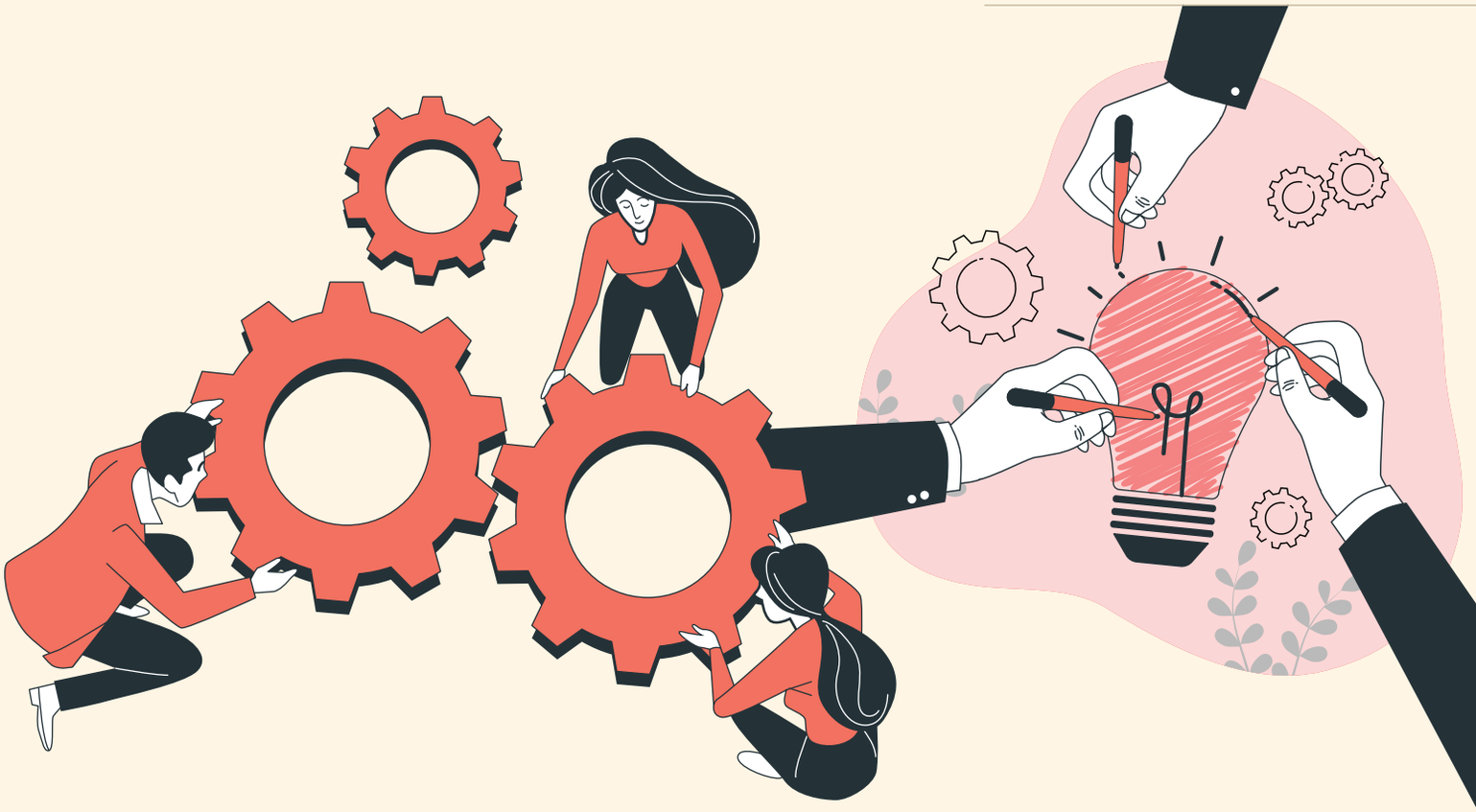
Evaluator action: The evaluator will:

(a) Compare during the backend audit the policies given in WQM and those available at the website/app for consistency.

(b) Check the implementation of these policies by examining the documented records generated by the implementation.







Lifecycle management 5.4

Statement: The government organisation has nominated a Web Information Manager (WIM) as defined in the guidelines. 5.4.1

Benefit: WIM can ensure a proper flow of content to the website/app and ensure that content quality and user satisfaction issues are taken care of. WIM will achieve this by coordinating with the various groups within the government organisation and undertaking multiple activities with regard to the Indian Government website being maintained by her/him. For instance, formulating policies for content management to update authentic content and manage it through the entire life cycle, e.g., creation, moderation, approval, publishing and archival getting the website certified for guidelines conformity and ensuring conformity throughout its lifecycle.

Government organisation action: The government organisation must appoint a WIM who must be a senior official not below the rank of a Joint Secretary (JS).

Developer action: Display complete contact details of the WIM on the website, so that visitors could contact him/her in case of some queries or requirements.

Evaluator action: The evaluator will check the website for WIM details and will compare the same with the WIM details in Website Quality Manual (WQM). Further during the backend audit the evaluator will interview WIM to assess his/ her awareness and competence regarding the responsibilities

Statement: It has been ensured that all stationery of the government organisations as well as advertisements/public messages issued by the concerned organisation prominently display the URL of the website. 5.4.2

Benefit: By mentioning the URL prominently on all stationery and publicity material of the government organisation, the Website can be promoted to attract visitors who may benefit from the information and services being delivered by the government organisation.

Government organisation action: The government organisations must ensure publishing of government website URL prominently on all stationery and publicity materials such as letterheads, visiting cards, publicity material such as brochures, pamphlets and documents such as the annual report etc; advertisements, press releases, tender notifications etc. issued in the newspapers/ audio-visual media. Also, ensure publishing regular and updated news related to the Government and in the interest of the citizens to attract citizens.

Developer action: Promote government websites/apps by linking with other government websites/apps as well as international websites. Provision may be provided on the website/apps to send regular updates on the website/app through an electronic newsletter to registered and interested users.

Evaluator action: The evaluator will check during the backend audit by examining the stationery (e.g., letterhead, tender document, email signature, Visiting Cards, Publicity material such as Brochures, Pamphlets and documents such as the Annual Report etc; Advertisements, Press Releases, Tender Notifications etc.) conformity with this.

Statement: Website has the following clearly defined policies and plans approved by the Web Information Manager (WIM): 5.4.3

(a) **Copyright Policy**
(b) **Content Contribution, Moderation & Approval (CMAP) policy**
(c) **Content Archival (CAP) policy**
(d) **Content Review (CRP) policy**
(e) **Hyper linking Policy**
(f) **Terms & Conditions**
(g) **Website Monitoring Plan**

Benefit: Having clearly defined policies helps ensure efficient management of the website and its content throughout the life cycle of the website.

Government organisation action: Clearly define and approve the website related policies listed above. WIM must ensure their implementation throughout the website life cycle

Developer action: Citizen-facing policies like copyright policy, privacy policy and terms and conditions must be published on the website.

Evaluator action: The evaluator will:

(a) Compare during the backend audit the policies given in WQM and those available at the website for consistency; and

(b) Check the implementation of these policies by examining the documented records generated by the implementation.

Statement: The mechanism is in place to check the accuracy of Hyperlinked Content and clear indications are given when a link leads out to a non-government website. 5.4.4

Benefit: Hyperlinking content across different websites/apps can occasionally cause ambiguity in the mind of the visitors about the owner of a particular portion of content and whom to be contacted in case of any query. Therefore, it helps to verify content accuracy before linking to an external website and thereafter clearly indicating when a visitor is being led to an external website.

Government organisation action: Define the Hyperlinking policy, duly approved by the WIM. Check the accuracy of the linked content regularly.

Developer action: Ensure alert mechanism to notify the visitor when clicking any link will lead to an external website

Evaluator action: The evaluator will check that:

(a) The policy defined in WQM is consistent with that available on the website; and

(b) The mechanism is completely and correctly defined in WQM and the same has been implemented by examining the documented records generated by the implementation.

Statement: It is ensured through content moderation and approval policy that Website content is free from offensive/ discriminatory language. 5.4.5

Benefit: Content that is free from offensive/discriminatory language helps in promoting inclusivity and enhances the user experience, attracting visitors to frequent the website/app for information and services they gain from.

Government organisation action: Any information in text, visual or any other media which may

offend/harm the National sentiments as well as security and integrity of the country must be avoided on the website. The government organisations must designate the officials who will implement the content moderation and approval policy (content creator, moderator and/or approver) as required.

Developer action: Ensure CMS has an in-built workflow for content moderation and approval.

Evaluator action: The evaluator will check that:

(a) The policy defined in WQM provides commitment to ensure that the website content is free from offensive/ discriminatory language.

(b) Developer action has been implemented.

(c) Randomly picked contents fulfil the policy.

Statement: Documents/pages in multiple languages are updated simultaneously. 5.4.6

Benefit: Helps avoid inconsistencies, at any point, between the various language versions, thus offering visitors the same content in multiple languages.

Government organisation action: Translate all content simultaneously.

Developer action: Ensure mechanism for publishing content in multiple languages and to display the status of non-translated content.

Evaluator action: The evaluator shall check the website contents manually to see conformity with this.

Statement: Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors. 5.4.7

Benefit: Presence of broken links and page not found errors will frustrate the visitors and reduce the trust level of citizens

Government organisation action: Define the Hyperlinking policy, duly approved by the Web Information Manager

Developer action: Ensure that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the website immediately upon discovery. Use appropriate technology tools available for convenient discovery of broken links.

Evaluator action: The evaluator shall check that the mechanism is completely and correctly defined in the WQM and verify the implementation by examining the documented records

generated by the implementation of the mechanism. Further the evaluator shall also test the website using the tool to check broken links on the website.

Statement: There are no links to 'under construction' pages. 5.4.8

Benefit: Visitors have a better experience when they find content versus experiencing "under construction" pages that convey a negative impression.
Government organisation action: Avoid any "under construction" pages as much as possible. Also, the government organisation must provide a date in case the content is event based i.e., Republic Day speech of President
Developer action: Avoid publishing any pages with "under construction" / "work in progress"
Evaluator action: The evaluator shall manually test the website for this checkpoint.

Statement: Documents are provided either in HTML or other accessible formats. 5.4.9

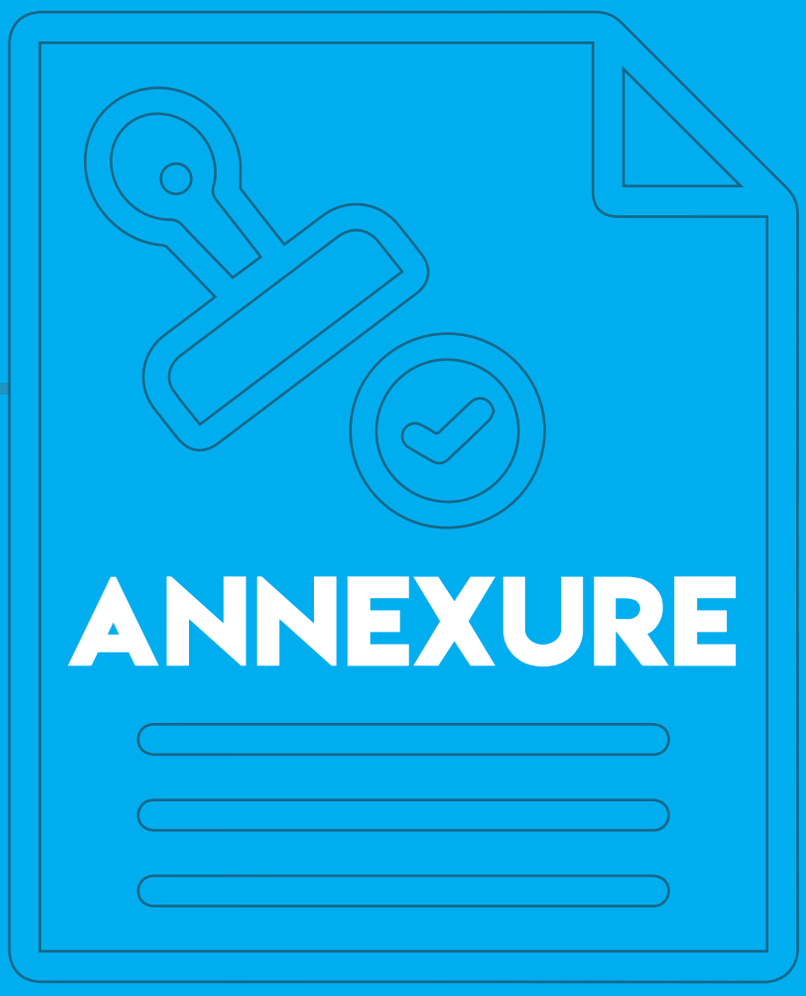
Benefit: Enhanced accessibility for all website visitors, especially the visually challenged who should be able to use assistive technologies to read the accessible format documents.
Government organisation action: The government organisations must ensure that the accessible version of all scanned documents is made available
Developer action: Ensure uploading of documents in HTML or other accessible formats.
Evaluator action: The evaluator shall manually test the website for this checkpoint.

Statement: Website/app is bilingual with a prominent language selection link and uses Unicode characters. 5.4.10

Benefit: India is a country with diverse cultures and as many as 22 languages. This will enable wider use of websites/apps by the rich Indian demographics, a large part which is more comfortable in regional languages versus English.
Government organisation action: Provide resources to translate all content. If difficult, determine which content is widely accessed by visitors and translate those sections to regional language.
Developer action: Ensure use of Unicode character set for regional language content and thorough testing to ensure access by all and no loss of layout.
Evaluator action: The evaluator shall manually and through tool test the website for this checkpoint.

GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES AND APPS



ANNEXURE

Annexure I

Committee composition

Annexure II

Matrix for checking conformity

Annexure III

Important terms

Committee Composition

The National Informatics Centre has taken the initiative to develop guidelines for the National Portal of India Project. These guidelines were created after extensive consultation with representatives from various Indian government organisations at both the central and state levels, as well as established guidelines from other countries and international bodies such as ISO and W3C.

The current version of the guidelines has made several significant improvements. It includes upgraded accessibility guidelines to ensure that websites and apps can be used by the widest possible audience. A new chapter on security has been added to help prevent cyber threats and protect user data. Furthermore, the guidelines have been organised in a stakeholder-wise manner, providing separate views for developers, owner organisation - web information managers and stakeholders.

Revised by:

Ms. Alka Mishra	**Scientist-G, NIC - Chairperson**
Dr. (Ms.) Seema Khanna	**Scientist-G, NIC**
Sh. A. K. Upadhyaya	**Scientist-G, STQC**
Sh. Durga Prasad Misra	**Scientist-F, NIC**
Sh. Pankaj Sharma	**Scientist-E, Indian Computer Emergency Response Team**
Ms. Shilpi Kapoor	**Chief Executive Officer, BarrierBreak**
Dr. Nirmita Narasimhan	**Programme Director Saksham & Policy Fellow, LirneAsia**
Shri Lokesh Joshi	**Scientist-F, NIC - Member Convener**





Matrix to check conformity

S/N	Quality Guidelines:	Risks Addressed
1	Association to Government is demonstrated using Emblem/Logo in proper ratio and colour, prominently displayed on the homepage/homescreen of the website/app.	Q8
2	Ownership information is displayed on thehomepage/ homescreen and on all important entry pages/screens of the website/app and each subsequent page/screen is a standalone entity in terms of ownership, navigation and context of content.	Q8
3	Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned.	Q3
4	Due permissions have been obtained for publishing any content protected by copyright.	Q3
5	Homepage/homescreen of website displays the last updated/reviewed date.	Q7
6	Complete information including title, size, format and usage instructions is provided for all downloadable material.	Q7
7	Statement: With respect to each, Circular, Notification, Document, Form, Scheme, Service and Recruitment notice, the following should be clearly listed on the Website: (a) Complete title (b) Language (if other than English) (c) Purpose/procedure to apply (as applicable) (d) Validity (if applicable)	Q7
8	All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are removed from the website and/or placed into the archives as per the archival policy.	Q7

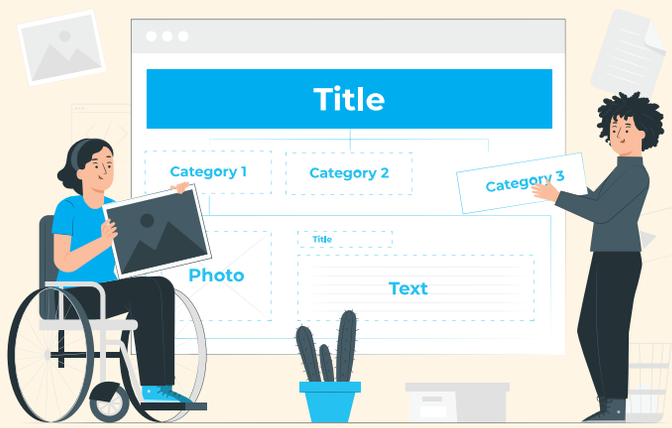
9	All information about the government organisation, useful for the citizen and other stakeholders, is present in the 'About Us' section and a mechanism is in place to keep the information up to date.	Q6, Q7
10	Website has a 'Contact Us' page providing complete contact details of important functionaries in the government organisation and this is linked from the homepage/homescreen and all relevant places on the website/app.	Q6, Q7
11	Feedback is collected through online forms and a mechanism is in place to ensure timely response to feedback/queries received through the website.	Q10
12	Website provides a prominent link to the 'National Portal' from the homepage and subsequent pages belonging to the National Portal load in the new browser window.	Q7
13	The website has been tested on multiple browsers. Hindi/Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout).	Q9
14	The website has a readily available Help section linked from all pages of the website.	Q6, Q7
15	Website uses Cascading Style Sheets (CSS) to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes.	Q9
16	Website is readable even when style sheets are switched off or not loaded.	Q9
17	Proper page title and language attribute along with metadata for page like keywords and description are appropriately included.	Q9
18	Minimum content as prescribed in the guidelines is present on the homepage/homescreen and all subsequent pages/screens.	Q6, Q7

19	Data tables have been provided with necessary tags/markup.	Q9
20	Content of the web page prints correctly on an A4 size paper	Q9
21	API integration with key government platforms (India Portal, DigiLocker, Aadhaar, Single-Sign-On, MyGov, Data Platform, MyScheme) and similar websites of the government organisation must be enabled for seamless exchange of Information and data.	Q7, Q8, Q10
22	The government organisation must ensure a consistent user experience and visual identities across all its websites/apps.	Q1, Q4, Q9
23	Websites/apps must provide integration with popular social media.	Q1, Q3, Q5, Q7
24	Website is in the nic.in or gov.in domain. Educational Institutions and Research and Academic Institutions, which are eligible for registration under 'gov.in' may use 'edu.in', 'res.in' or 'ac.in' domains.	Q8
25	The language is free from spelling and grammatical errors.	Q7, Q9



S/N	Accessibility Guidelines:	Reference	Risks Addressed
1	All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below.	WCAG 2.1 – 1.1.1	A1
2	For pre-recorded audio-only and pre-recorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labelled as such: (a) Pre-recorded Audio-only: An alternative for time-based media is provided that presents equivalent information for pre-recorded audio-only content. (b) Pre-recorded Video-only: Either an alternative for time-based media or an audio track is provided that presents equivalent information for pre-recorded video-only content.	WCAG 2.1 – 1.2.1	A1
3	Captions are provided for all pre-recorded audio content in synchronised media, except when the media is a media alternative for text and is clearly labelled as such.	WCAG 2.1 – 1.2.2	A1
4	An alternative for time-based media or audio description of the pre-recorded video content is provided for synchronised media, except when the media is a media alternative for text and is clearly labelled as such.	WCAG 2.1 – 1.2.3	A1
5	Captions are provided for all live audio content in synchronised media.	WCAG 2.1 – 1.2.4	A1
6	Audio description is provided for all pre-recorded video content in synchronised media.	WCAG 2.1 – 1.2.5	A1
7	Information, structure and relationships conveyed through presentation can be programmatically determined or are available in text.	WCAG 2.1 – 1.3.1	A6, A9

8	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	WCAG 2.1 - 1.3.2	A6, A9
9	Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, colour, size, visual location, orientation, or sound.	WCAG 2.1 - 1.3.3	A1, A2, A3, A4
10	Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.	WCAG 2.1 -1.3.4	A4, A5
11	The purpose of each input field collecting information about the user can be programmatically determined when: (a) The input field serves a purpose identified in the Input Purposes for User Interface Components section; and (b) The content is implemented using technologies with support for identifying the expected meaning for form input data.	WCAG 2.1-1.3.5	A6
12	Colour is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	WCAG 2.1 - 1.4.1	A1
13	If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level.	WCAG 2.1 - 1.4.2	A4, A5



14	The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: (a) Large Text: (18 pt. or 14 pt. bold) Large-scale text and images of large-scale text have a contrast ratio of at least 3:1. (b) Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. (c) Logotypes: Text that is part of a logo or brand name has no contrast requirement.	WCAG 2.1 - 1.4.3	A1
15	Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality.	WCAG 2.1 - 1.4.4	A1, A4
16	If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text except for the following: (a) Customizable: The image of text can be visually customised to the user's requirements. (b) Essential: A particular presentation of text is essential to the information being conveyed.	WCAG 2 1 - 1.4.5	A1
17	(a) Content can be presented without loss of information or functionality and without requiring scrolling in two dimensions for: (b) Vertical scrolling content at a width equivalent to 320 CSS pixels. (c) Horizontal scrolling content at a height equivalent to 256 CSS pixels. (d) Except for parts of the content which require a two-dimensional layout for usage or meaning.	WCAG 2.1-1.4.10	A6

18	The visual presentation of the following has a contrast ratio of at least 3:1 against adjacent colour(s): (a) User Interface Components: Visual information required to identify user interface components and states, except for inactive components or where the appearance of the component is determined by the user agent and not modified by the author. (b) Graphical Objects: Parts of graphics required to understand the content, except when a particular presentation of graphics is essential to the information being conveyed.	WCAG 2.1- 1.4.11	A6
19	In content implemented using markup languages that support the following text style properties, no loss of content or functionality occurs by setting all of the following and by changing no other style property: (a) Line height (line spacing) to at least 1.5 times the font size. (b) Spacing following paragraphs to at least 2 times the font size. (c) Letter spacing (tracking) to at least 0.12 times the font size. (d) Word spacing to at least 0.16 times the font size. (e) Exception: Human languages and scripts that do not make use of one or more of these text style properties in written text can conform using only the properties that exist for that combination of language and script.	WCAG 2.1- 1.4.12	A6



20	Where receiving and then removing pointer hover or keyboard focus triggers additional content to become visible and then hidden, the following are true: (a) Dismissible: A mechanism is available to dismiss the additional content without moving pointer hover or keyboard focus unless the additional content communicates an input error or does not obscure or replace other content. (b) Hover-able: If pointer hover can trigger the additional content, then the pointer can be moved over the additional content without the additional content disappearing. (c) Persistent: The additional content remains visible until the hover or focus trigger is removed, the user dismisses it, or its information is no longer valid.	WCAG 2.1-1.4.13	A4, A5, A6
21	All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints.	WCAG 2.1 - 2.1.1	A5
22	If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away.	WCAG 2.1 - 2.1.2	A5





23	If a keyboard shortcut is implemented in content using only letter (including upper- and lower-case letters), punctuation, number, or symbol characters, then at least one of the following is true: (a) Turn off: A mechanism is available to turn the shortcut off. (b) Remap: A mechanism is available to remap the shortcut to include one or more non-printable keyboard keys (e.g., Ctrl, Alt). (c) Active only on focus: The keyboard shortcut for a user interface component is only active when that component has focus.	WCAG 2.1 – 2.1.4	A5
24	For each time limit that is set by the content, at least one of the following is true: (a) Turn off: The user is allowed to turn off the time limit before encountering it; or Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or (b) Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the spacebar") and the user is allowed to extend the time limit at least ten times; or (c) Real-time Exception: The time limit is a required part of a real-time event (for example, an auction) and no alternative to the time limit is possible; or (d) Essential Exception: The time limit is essential and extending it would invalidate the activity; or (e) 20 Hour Exception: The time limit is longer than 20 hours.	WCAG 2.1 – 2.2.1	A4

25	For moving, blinking, scrolling, or auto-updating information, all of the following are true: (a) Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and (b) Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential.	WCAG 2.1 - 2.2.2	A2, A4
26	Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds.	WCAG 2.1 - 2.3.1	A2
27	A mechanism is available to bypass blocks of content that are repeated on multiple Web pages.	WCAG 2.1 - 2.4.1	A6
28	Web pages have titles that describe the topic or purpose.	WCAG 2.1 - 2.4.2	A6
29	If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability.	WCAG 2.1 - 2.4.3	A6
30	The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general.	WCAG 2.1 - 2.4.4	A6

31	More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process.	WCAG 2.1 - 2.4.5	A6
32	Headings and labels describe topic or purpose.	WCAG 2.1 - 2.4.6	A6, A9
33	Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible.	WCAG 2.1 - 2.4.7	A4
34	All functionality that uses multipoint or path-based gestures for operation can be operated with a single pointer without a path-based gesture, unless a multipoint or path-based gesture is essential.	WCAG 2.1-2.5.1	A4
35	For functionality that can be operated using a single pointer, at least one of the following is true: (a) No Down-Event: The down-event of the pointer is not used to execute any part of the function. (b) Abort or Undo: Completion of the function is on the up-event and a mechanism is available to abort the function before completion or to undo the function after completion. (c) Up Reversal: The up-event reverses any outcome of the preceding down-event. (d) Essential: Completing the function on the down-event is essential.	WCAG 2.1- 2.5.2	A4
36	For user interface components with labels that include text or images of text, the name contains the text that is presented visually.	WCAG 2.1- 2.5.3	A9





37	Functionality that can be operated by device motion or user motion can also be operated by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: (a) Supported Interface: The motion is used to operate functionality through an accessibility supported interface. (b) Essential: The motion is essential for the function and doing so would invalidate the activity. (c) Functionality that can be operated by device motion or user motion must also be operable by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: (d) Supported Interface: The motion is used to operate functionality through an accessibility supported interface. (e) Essential: The motion is essential for the function and doing so would invalidate the activity.	WCAG 2.1- 2.5.4	A5
38	The default human language of each Web page can be programmatically determined.	WCAG 2.1 – 3.1.1	A1, A6, A7
39	The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language and words or phrases that have become part of the vernacular of the immediately surrounding text.	WCAG 2.1 – 3.1.2	A1, A6, A7
40	When any user interface component receives focus, it does not initiate a change of context.	WCAG 2.1 – 3.2.1	A6
41	Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behaviour before using the component.	WCAG 2.1 – 3.2.2	A6

42	Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user.	WCAG 2.1 – 3.2.3	A6
43	Components that have the same functionality within a set of Web pages are identified consistently.	WCAG 2.1 – 3.2.4	A6
44	If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.	WCAG 2.1 – 3.3.1	A6
45	Labels or instructions are provided when content requires user input.	WCAG 2.1 – 3.3.2	A9
46	If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardise the security or purpose of the content.	WCAG 2.1 – 3.3.3	A4, A6
47	For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: (a) Reversible: Submissions are reversible. (b) Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. (c) Confirmed: A mechanism is available for reviewing, confirming and correcting information before finalising the submission.	WCAG 2.1 – 3.3.4	A8

48	In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes and any IDs are unique, except where the specifications allow these features.	WCAG 2.1 – 4.1.1	A6
49	For all user interface components (including but not limited to form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.	WCAG 2.1 – 4.1.2	A6
50	In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus.	WCAG 2.1– 4.1.3	A6





S/N	Security Guidelines	Risks Addressed
1	Ensure that the website, web application, web portal or mobile app is Security Audited and an Audit Clearance certificate is issued by NIC, STQC or a CERT-In empanelled vendor before hosting in production environment.	S1- S15
2	Hosting Environment must be secured for ensuring confidentiality, integrity and availability (CIA).	S1- S15
3	Website has the Security Policy, Privacy Policy and the Contingency Management Plan clearly defined policies and plans approved by the government organisation.	S1- S15



S/N	Lifecycle Management Guidelines	Risks Addressed
1	The government organisation has nominated a WIM as defined in the guidelines.	Q1
2	It has been ensured that all stationery of the government organisation as well as advertisements/public messages issued by the government organisation concerned prominently display the URL of the web site.	Q2
3	Website has the following clearly defined policies and plans approved by the WIM. (a) Copyright Policy (b) Content Contribution, Moderation and Approval (CMAP) policy (c) Content Archival (CAP) policy (d) Content Review (CRP) policy (e) Hyper linking Policy (f) Privacy Policy (g) Terms & Conditions (h) Website Monitoring Plan. (i) Contingency Management Plan (j) Security Policy	Q3, Q4, Q5, Q7
4	The mechanism is in place to check the accuracy of Hyperlinked Content and clear indications are given when a link leads out to a non-government website.	Q4
5	It is ensured through content moderation and approval policy that Website content is free from offensive/discriminatory language.	Q7
6	Documents/Pages in multiple languages are updated simultaneously.	Q7
7	Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors.	Q7
8	There are no links to 'under construction' pages.	Q7
9	Documents are provided either in HTML or other accessible formats.	Q9
10	Website is bilingual with a prominent language selection link and uses Unicode characters.	Q9, Q6, Q7

Important terms

Abbreviations:	
NIC	National Informatics Centre
UT	Union Territory
UUU	Usable, User-Centric and Universally Accessible
ISO	International Organisation for Standardization
WCAG	Web Content Accessibility Guidelines
STQC	Standardization Testing & Quality Certification
ICT	Information and Communications Technology
GIGW	Guidelines for Indian Government Websites and Apps
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
XSS	Cross-Site Scripting
DOM	Document Object Model
CMS	Content Management System
NPI	National Portal of India
CSS	Cascading Style Sheets
UI	User Interface
URL	Uniform Resource Locator
ALT	Alternative Text

Important terms

Abbreviations:	
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
HTML	Hypertext Markup Language
OCR	Optical Character Recognition
PDF	Portable Document Format
ID	Identification
FTP	File Transfer Protocol
WAF	Web Application Firewall
DMZ	Demilitarized Zone
IDPS	Intrusion Detection and Prevention System
HSTS	HTTP Strict Transport Security
SSL	Secure Sockets Layer
IIS	Internet Information Services
SSL	Secure Sockets Layer
DES	Data Encryption Standard
3DES	Triple Data Encryption Standard
RC	Rivest Cipher
SHA	Secure Hash Algorithm
API	Application Programming Interface

Important terms

Abbreviations:	
MFA	Multi-Factor Authentication
OWASP	Open Web Application Security Project
PATH	Personal Access Token Holder
IP	Internet Protocol
RBAC	Role-Based Access Control
UNIX	Universal Operating System
VPC	Virtual Private Cloud
SSH	Secure Shell
OPA	Open Policy Agent
YAML	Yet Another Markup Language
SSO	Single Sign-On
CERT-In	Indian Computer Emergency Response Team
WIM	Web Information Manager
JS	Joint Secretary
WQM	Website Quality Manual
CMAP	Content Contribution, Moderation & Approval policy
CAP	Content Archival (CAP) policy
CRP	Content Review (CRP) policy

Web Information Manager

The success of any endeavour depends upon the backing of a strong and enthusiastic team. In case of a Government website, the role of a Website management team assumes paramount importance in ensuring its credibility amongst its patrons.

Departments MUST appoint a **Web Information Manager (WIM)** whose role shall be to ensure that there is a proper flow of content to the site and that content quality and user satisfaction issues are taken care of. To achieve this WIM has to coordinate with the various groups within the Department and undertake the following activities with regard to the Indian Government website being maintained by her/him.

- Formulation of policies concerning management of content on the web through its entire life cycle viz. Creation, Moderation, Approval, Publishing and Archival. Ensuring that all content on the website is always authentic, up-to-date and obsolete information or services are removed.

- Set a mechanism for periodically validating links to related information. An automated report can provide a list of broken links on the site, which can be immediately corrected.

- Getting the website certified for Guideline Compliance and ensuring that it remains compliant throughout its lifecycle.

- Web Information Manager is overall responsible for quality and quantity of information and services on the website. The complete contact details of the Web Information Manager should be displayed on the website, so that the visitor could contact him/her in case of some queries or requirements.

- Since the websites receive a significant amount of feedback/query mails from the visitors, it is the responsibility of the Web Information Manager to either reply to all of them himself/her self or designate someone to regularly check and respond to the feedback/query mails.

Besides the Web Information Manager, a Technical Team should also be appointed for every Indian Government website whose responsibilities would be:

- Regular monitoring of website for Performance, Security and Availability.
- Ensuring compliance with policies (organisational, regulatory, legislative, etc.) that may require changes in website content, architecture, and security.
- Periodic security audit of the website in line with major revisions.
- Analysis of traffic on website and provide feedback to management.

GIGW

GIGW 3.0

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES

For any feedback on these guidelines contact us at:

Web Technology Division
National Informatics Centre
A- Block, CGO Complex, Lodhi Road, New Delhi – 110003

Email: webguidelines@nic.in