INTERNATIONAL STANDARD

ISO/IEC/IEEE 23026

First edition
2023-07

Systems and software engineering — Engineering and management of websites for systems, software and services information

Ingénierie des systèmes et du logiciel — Ingénierie et gestion de sites web pour les systèmes, logiciels et services d'information

Reference number
ISO/IEC/IEEE 23026:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO/IEC documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

This second edition cancels and replaces the first edition (ISO/IEC/IEEE 23026:2015), which has been technically revised.

The main changes are as follows:

— updates relating to enhanced technical capabilities for website design and sustainment;

— attention to threats to data privacy and website integrity;

— reorganization to present both the life cycle processes of website information for informational websites and the requirements for website features.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Continuing improvements in Internet capabilities for technical communication, and the accelerating development of new technical protocols, products and services for website development and hosting, have both simplified and complicated the engineering and management of websites. This document is intended to account for new capabilities, approaches, and interests in using websites to communicate technical information. To a large extent, use of digital communications, particularly those accessible through the Internet or intranets, has supplanted printed publications for conveying technical information. This trend applies to information for users, systems and services documentation, and operational plans, policies, and procedures.

Other factors have also affected the design and operation of websites. The increasing sophistication of information security threats to technical enterprises and their information, as well as concerns for the privacy of Internet users, have markedly complicated the process of delivering information and communication technology (ICT) information over the Web. This document therefore has increased emphasis on information security and privacy concerns.

The diversity of websites for commercial marketing and social networking purposes reflects different interests and media choices from those websites that deliver ICT reference information. This document applies primarily to websites whose purpose is to deliver information about ICT systems, software, and services. It includes increased emphasis on the human factors concerns for making information easily retrievable and usable for the intended audience. It recommends practices for websites based on World Wide Web Consortium (W3C) and related industry guidelines. It continues to address the entire life cycle of website strategy, design, engineering, testing and validation, and management and sustainment, which are the responsibility of the website owner and website provider.

Systems and software engineering — Engineering and management of websites for systems, software and services information

1 Scope

This document defines system engineering and management requirements for the life cycle of websites, including strategy, design, engineering, testing and validation, and management and sustainment for intranet and extranet environments. This document applies to those using web technology to present information and communications technology (ICT) information, such as information for users of systems and services, plans and reports for systems and software engineering projects, and documentation of policies, plans, and procedures for IT service management. This document provides requirements for website owners and website providers, managers responsible for establishing guidelines for website development and operations, website engineers, designers, developers, and operations and maintenance staff, who can be external or internal to the website owner's organization. It applies to websites for public access and for limited access, such as for users, customers, and subscribers seeking information on IT systems, products and services.

The requirements and recommendations in this document address the following aspects of usability of informational websites and ease of maintenance of managed website operations:

a) locating relevant and timely information;

b) applying information security management;

c) facilitating accessibility and ease of use;

d) providing for consistent and efficient development and maintenance practices.

This document is not particularly applicable to websites used primarily for marketing or sales, to deliver instructional material (tutorials), or to provide graphical user interfaces (GUI) for business or consumer transactional application processing. However, this document can provide useful insights for managing such sites.

This document does not address vendor and product considerations for website engineering and management. This document does not include specifications for application development tools, programming and scripting languages used for websites, metadata tags, or protocols for network communications. It does not address tools or systems used for management or storage of information content (data, documents) that can be presented on websites.

This document does not address the design and architecture of software and systems supporting the Internet.

2 Normative references

There are no normative references for this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO, IEC, and IEEE maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org

— IEEE Standards Dictionary Online: available at https://dictionary.ieee.org.

NOTE For additional terms and definitions in the field of systems and software engineering, see ISO/IEC/IEEE 24765, which is published periodically as a "snapshot" of the SEVOCAB (Systems and Software Engineering Vocabulary) database and is publicly accessible at www.computer.org/sevocab.

3.1.1
archival page
content (3.1.5) that is preserved as a record and not expected to change

Note 1 to entry: Due to technology upgrades, some archival pages cannot be readily rendered unless they are upgraded along with active pages.

3.1.2
audience
category of users sharing the same or similar characteristics and needs (e.g. purpose in using the information for users, tasks, education level, abilities, training, and experience) that determine the *content* (3.1.5), structure, and use of the intended information

Note 1 to entry: There can be different audiences for information for users (e.g. management, data entry, maintenance, engineering, business professionals).

3.1.3
breadcrumb trail
navigational aid with a displayed series of *links* (3.1.15) which lead from the *home page* (3.1.12) or another page to the current page

3.1.4
browser
application allowing a person to retrieve and read hypertext, to view the *contents* (3.1.5) of hypertext nodes [*web page* (3.1.26)], to navigate from one web page to another, and to interact with the content, such as changing the visual appearance of the displayed content

3.1.5
content
interactive or non-interactive object containing information represented by text, image, video, sound, or other media

3.1.6
cookie
small file created by the user's web *browser* (3.1.4) that is stored in and retrieved from the user's device to maintain state information, including identification of users and transaction coherency

3.1.7
extranet
intranet (3.1.14) that is accessible to authorized external users for the retrieval or exchange of information

3.1.8
faceted search
progressive search which allows users to narrow the results by selecting values for one or more attributes

3.1.9
feature
functional or non-functional distinguishing characteristic of a system, usually an enhancement to an existing system

3.1.10
frame
element that divides a *browser* (3.1.4) window into independent windows for displaying different *content* (3.1.5), or different parts of the same content (document)

3.1.11
global navigation
set of *navigation* (3.1.17) *links* (3.1.15) available on all pages of a *website* (3.1.27)

3.1.12
home page
web page (3.1.26) through which users typically enter the *website* (3.1.27), and whose *URL* (3.1.23) is typically published or linked as the main web address of the site or organization

Note 1 to entry: Types of home pages include: centre page, front page, index page, main page, start page, top page.

3.1.13
Internet
worldwide interlinked computer systems and networks connected by gateways that enable the transfer of data between them

3.1.14
intranet
managed network (3.1.16) operating within an organization with controlled and limited access

3.1.15
link
hyperlink
reference from some part of one document to some part of another document or another part of the same document

3.1.16
managed network
network or set of networks established and controlled by one or more organizations to meet specific organizational or business needs

3.1.17
navigation
process of accessing on-screen information by moving between different locations in a *website* (3.1.27) or electronic document

3.1.18
orphan page
page on a *website* (3.1.27) with no *link* (3.1.15) from any other page on the website

3.1.19
persistent URI
persistent Uniform Resource Identifier
reference that does not need to change at the *link* (3.1.15) in a document and can still reach the desired object even though that object can have changed locations

3.1.20
responsive web design
RWD
method for *web page* (3.1.26) construction to detect the user's screen size and orientation and dynamically change the layout accordingly

3.1.21
site map
textual or graphical overview of the *navigation* (3.1.17) structure of a *website* (3.1.27)

3.1.22
thumbnail
miniature image file displayed for quick identification of a larger image or video file

3.1.23
URL
Uniform Resource Locator
mechanism for identifying resources on the *Internet* (3.1.13) [such as a *web page* (3.1.26)] by specifying the address of the resource and the access protocol used

Note 1 to entry: The term as specified by the IETF is Uniform Resource Identifier (URI) of which URL is a subset.

3.1.24
user profile
set of attributes that are unique to a specific user or user group, such as job function or subscription to a service, used to control the parts of the system or *web page* (3.1.26) that users can access

3.1.25
web lead
person or group responsible to the *website owner* (3.1.28) for ongoing maintenance of the site's presentation and availability

3.1.26
web page
coherent presentation of a set of *content* (3.1.5), objects and associated interaction objects delivered to users through a *browser* (3.1.4) in accordance with *Internet* (3.1.13) protocols

Note 1 to entry: A web page can be generated dynamically from the server side, and can incorporate multimedia, applets or other elements active on either the client or server side.

3.1.27
website
collection of logically connected *web pages* (3.1.26) managed as a single entity

Note 1 to entry: A website may contain one or more subordinate websites.

3.1.28
website owner
organization responsible for the site *content* (3.1.5) and site design

Note 1 to entry: The website owner may select a supplier as the *website provider* (3.1.29) or may also be the website provider.

3.1.29
website provider
organization responsible for operation of the *website* (3.1.27) and delivery of site *content* (3.1.5) to users

Note 1 to entry: The website provider may also be the site owner, *web lead* (3.1.25), site designer, or the *Internet* (3.1.13) or cloud service provider for the site.

3.1.30
wiki
website (3.1.29) that allows a group of users to add and edit *content* (3.1.5) collaboratively

3.2 Abbreviated terms

3D	three-dimensional
AI	artificial intelligence
API	application programming interface
ARIA	Accessible Rich Internet Application
CI	configuration item
CFR	Code of Federal Regulations
CSS	cascading style sheets
CVE	common vulnerabilities and exposures
CVSS	Common Vulnerability Scoring System
DITA	Darwin Information Typing Architecture
DNS	Domain Name Service
DOI	Digital Object Identifier
DTD	Document Type Definition (for XML or SGML specifications)
FIDO	fast identity online
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GIF	Graphics Interchange Format
GUI	graphical user interface
HIPAA	Health Insurance Portability and Accountability Act
HREF	HTML reference designator
HTML	hypertext markup language
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
ICT	information and communications technology
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPR	intellectual property rights
JPEG	Joint Photographic Experts Group (image format)
JSON	Java Script Object Notation

MAC	Media Access Control
MFA	multi-factor authentication
OAUTH	open authentication
OTP	one-time password
PCI DSS	Payment Card Industry Data Security Standard
PHP	hypertext preprocesor
PICS	Platform for Internet Content Selection
PII	personally identifiable information
PIN	personal identification number
PIPEDA	Personal Information Protection and Electronic Documents Act
PNG	Portable Network Graphics
RDF	Resource Description Framework
SGML	Standard Generalized Markup Language
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	single sign-on
TCP	Transport Control Protocol
TLS	Transport Layer Security
TZD	time zone designator
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
WAI	Web Accessibility Initiative (W3C)
WCAG	Web Content Accessibility Guidelines
W3C	World Wide Web Consortium
XHTML	Extended HyperText Markup Language
XML	Extensible Markup Language

4 Planning websites

4.1 Defining the purpose, users, and context of the website

This document addresses websites that have the general purpose of providing information about ICT systems, software, or service management. Within this scope, a broad range of purposes, audience (users), and resulting types of content can be included, such as policies, plans, specifications, operating procedures and instructions (user manuals), service descriptions, service agreements, knowledge management articles, help desk scripts, test plans, technical reports, and descriptions of concepts.

When planning for the website, the website owner shall document the purpose and intended users of the website. This information may be placed in a plan, charter, or policy and represented by use cases or scenarios. It influences the decisions on what information content belongs on the website and how to organize and present the content. This governing document or another explicit statement of purpose, suitable for use by possible stakeholders, should be posted as part of the website.

A website may address one or more diverse sets of users. The users of the website can include internal management and technical staff, external customers, or the public. Thus, the website content can include general user information or procedures and specialized technical information for trained technical users. Websites may be intended for a specific group, such as internal helpdesk or external customers. Some websites may allow users to add content as part of a collaborative community or post comments in a wiki. Some sites include both technical information for existing customers and marketing presentations for prospective customers. The owner of the technical information can host some sites; other sites can run on services offered by unrelated website providers, who may have their marketing information and third-party advertisements displayed alongside the website owner's technical content. Sites can be intended for local or global use and offered in one or multiple languages.

Websites are often developed to serve several purposes and users of different technical backgrounds. Therefore, the site should be designed to allow users to understand the content's scope and functionality. The introductory pages of the site should include a description of the purpose and intended uses of the website, with links to topics accessible within one link or search which satisfies the information needs of casual users. Global navigation features and search functions should allow more technical users to access needed information quickly (see 9.2).

The effective communication of the content to the user is the primary purpose of an informational website. Ease of access to information by targeted-user communities is an example of one of the possible design goals.

The website designers should consider responsive website design to accommodate different devices. Websites may consist of static pages, system-generated pages, and dynamic pages, including user-generated content. Furthermore, any of these options may be combined to provide the intended information to the website's users. The target user community can have a wide diversity of connection speeds, display devices, or selected presentation formats within the display windows; this may establish some presentation constraints (consider displaying web pages to small screens on mobile devices).

The size and resolution of the screen should be considered in the design and usability of the website. For example, most smart phones and tablets use pop-up screen keyboards which can be too small to use without a stylus.

Website planning shall identify the target web browsers. In some cases, the website should target all major browsers. In other cases, it may be acceptable to target a small subset of browsers or a specific browser. The users should receive a clear notification if the site is not compatible with their browser.

Use of the terminology in this document is for ease of reference and is not mandatory for conformance with this document.

4.2 Establishing the informational website design and sustainment strategies

4.2.1 General

Organizational effectiveness, competitive success, and even meeting legal obligations and avoiding liabilities can depend on timely access to critical information within an organization. Website design should consider the need for timely access to information, as the Internet is used to displace other methods for information delivery. Usability testing and other methods of obtaining user feedback should be actively pursued as part of this process.

The owner of the website should consider how the company's technical and strategic direction should influence construction and feature choices that are extensible or scalable for future use. The website designer should consider performance considerations affecting the site and data store design: the

expected number and persistence of users, type and volume of information to be retrieved and viewed, and use of static or dynamic information.

Representatives of the user communities, including persons with disabilities, should be included in the design process and the ongoing evaluation of the site.

The website owner should plan to use methods and tools to collect and analyse site usage data to improve the usability of the site content.

EXAMPLE Measures, such as user comments and ratings, or trends in the number of help desk calls related to services, or software functions documented on the website.

4.2.2 Website plan

The developer of a website for information reference shall prepare a project plan, or follow an existing plan, covering the entire life cycle of the site. The life cycle includes implementation (strategy, planning, design, development, testing, and configuration), deployment, and maintenance (technical support, release management, updates, incident and problem management), and retirement.

The plan for the informational website should define when, how, and by whom specific activities are to be performed, including options and alternatives. The plan should include the following items:

a) website owner;

b) website purpose, scope, and intended user communities;

c) intended lifespan of the website and frequency of change to the content, usability and relevance of existing content;

d) applicable standards, such as CSS, and policies, including privacy, information security, risk management, and intellectual property policy;

e) applicable organizational guidance, including style guides;

f) roles and responsibilities for site development and content development;

g) roles and responsibilities for validating website content and usability, achieving performance targets, and conducting performance testing;

h) constraints on website platform or infrastructure, including programming languages;

i) schedules and resource estimates;

j) response to user support needs.

NOTE 1 Methods of user support can be handled by the web lead, help desk, a problem or incident management system, information for users, chat, or, telephone.

The website management plan shall include requirements, processes, responsibilities, and budgets for the website sustainment and maintenance, performance, stakeholder involvement, and website retirement

NOTE 2 ISO/IEC/IEEE 15289 provides additional information for plans, policies, specifications, and procedures, including project management plans, information management plans, documentation plans, information security plans, service availability and continuity plans, and system requirements specifications.

4.2.3 Website maintenance planning

Website maintenance planning should identify the source and responsibilities for the following, depending on the complexity, size and user base of the website:

a) maintenance and support organization;

b) processes and responsibilities for handling website scheduled maintenance;

c) website performance standards and measurements to assess its effectiveness for information retrieval;

d) processes and responsibilities for handling website event-triggered maintenance;

e) processes for user support, if offered;

f) process for approval of changes to content and to support software, including monitoring for changes in client or server environments that may require or warrant website re-engineering;

g) website enhancements or re-engineering;

h) verification and validation of the enhanced or re-engineered website;

i) configuration and release management;

j) security and business continuity, including risk management, failure handling and rollback;

k) periodically validating site content, such as eliminating or clearly labelling obsolete information content or discontinued services; updating the status of information or services; validating and updating links to related information;

l) periodically verifying that the website is compatible with the most recent versions of widely used browsers.

NOTE ISO/IEC/IEEE 12207 provides more information on software support processes. ISO/IEC 20000-1 addresses the supporting processes for a service management system. Both include requirements for configuration management and problem management from different perspectives. IEEE Std 828 specifies activities for configuration management.

4.2.4 Website maintenance procedures

Websites shall have incident and problem management procedures. The website owner and primary web lead shall establish procedures to:

a) report discovered errors or defects; either in the website content or in performance;

b) track errors and defects, including the severity of errors and defects;

c) prioritize correcting errors and defects;

d) correct errors and defects;

e) report the correction of errors and defects.

NOTE Maintenance procedures are detailed in Clause 8.

4.3 Establishing the privacy and security strategy

The website design should consider the needed levels of access control for the site, including whether all or some content is available to the worldwide public and some is limited to internal users such as administrators, customers or subscribers, or prospective customers who provide their contact information. Defining the different roles of website users and their need to know determines their authorized access to information.

The development plan should include the use of multifactor authentication wherever confidential data is accessed.

The website shall include its privacy policy applicable to anyone accessing the site.

There should be a policy for regular security audits (see 5.4), including access control review and action to be documented for any gap mitigation. Standard audit bodies may audit the website; and the results should be reported to the website owner and the website security lead.

There should be a plan for the classification of information according to sensitivity of the website contents. There shall be special consideration for any PII and proprietary or confidential data. Protection of PII is a complex and evolving process, subject to regulation by different governing bodies and regional requirements. Website planning shall include attention to privacy of data based on current regulations and guidelines, such as GDPR, HIPAA, PIPEDA, and PCI DSS (see 9.7).

While permissions are not required to include a link or reference to another website, appropriate permission should be obtained before including intellectual property owned by another party on a website. Legal counsel may be consulted concerning the appropriate protection and use of intellectual property contained within or offered by the website.

NOTE Additional information on data privacy is detailed in IEEE Std 7002, ISO/IEC 29100 and The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.

The security strategy should include “end-to-end” encryption of that critical data, both in transit and at rest while being stored.

Encryption protections should be periodically reviewed, based on the evolution of computer decryption capabilities.

A website owner or website provider shall have a defined security policy. The security policy should cover the following aspects:

a) roles and responsibilities as they apply to the website owner, website provider, and developers;

b) ensuring a proper balance of confidentiality, integrity and availability of all website data, to safeguard business and personal data;

c) security aspects of the website architecture and configuration, which may include having separate web, application and database servers or involve clustering, load balancing, virtualization, or cloud services;

d) operational monitoring for the detection and prevention of security incidents, and auditing, with sufficient and safe logging for unusual conditions, monitoring and alerting facilities to allow audit;

e) operational procedures to handle software defects (patches, updates) and security breaches (unauthorized access or modifications of the site);

f) authorization and authentication – including password policy when user ID/password is used in lieu of hardware token/PIN, and session management;

g) encryption, using current implementations and avoiding outdated implementations with known vulnerabilities, e.g. old TLS versions;

h) use of cookies and other amalgamations of user data;

i) coding best practices for security, including prevention of SQL injection where databases are used;

j) privacy and the handling of PII.

The security policy for website design, security controls, and development practices shall be made available to developers and support staff, for either a new development or a modification of an existing page or site.

The security policy shall cover all activities for the operation of the website, the handling and management of the data and the continuous monitoring including the assignments of roles and functions.

5 Designing and engineering websites

5.1 Design goals and website requirements

Website designers and developers, along with the business analyst, website owner, or user representative, shall prepare a design description including a prototype (or model) for a website, a context depiction, with reference to functional and non-functional requirements pertaining to performance, scalability, availability, and information security. Transition procedures may also be applied, particularly when existing content or business processes (or a business process) are being transitioned to the website. An example suited for transition requirements is transitioning safety training from a classroom to website videos.

The design process for an informational website shall include stakeholders' involvement and participation in validation throughout the website life-cycle activities: development, operations, and maintenance. To this end, website developers should identify categories of stakeholders early in the design phase so at least a representative sample of them can participate in the website development activities. The designers should consider typical access patterns for their users. This process should facilitate concurrent validation and verification of website requirements. The basis for the design description should be stakeholder requirements, which also provide a basis for validating the website design. Website developers should trace the website's functional and non-functional requirements to the website's strategic plan or charter from the website owner.

NOTE ISO/IEC/IEEE 29148 includes details of requirements engineering.

A primary consideration in website engineering is how to host the website. Typical options are self-hosting, using a website hosting service, and using a cloud platform. This decision affects the website cost, security, and staffing requirements for operations and maintenance.

The website design should be modelled or documented. An architectural diagram depicting how the website integrates into the technology ecosystem and associated infrastructure should also be included. Website design should include statements about the page formats generated, such as HTML version (and in some cases excluded functionality), version of CSS, Ajax (Asynchronous JavaScript and XML), JSON, XML and XML DTDs, graphics formats, scripting or byte code executable versions or limitations, human-language considerations (as well as character sets), bandwidth considerations, and other characteristics from this document or as identified during the design phase. The documentation should be updated based on actual experience. Specification in terms of vendor-specific products not under the control of the website owner should be avoided, along with the associated loss of product independence.

Consistency of infrastructure within related websites can simplify ongoing operation in areas such as:

— user-friendly assistant technologies to guide user inputs;

— security and efficiency of communication controls between the client and the web server;

— for stateful websites, processing of multiple requests from the same user within the same session if using multiple web servers behind a load balancer.

If a website is complex or if it implements interactive functionality, the website may be considered as a software application and engineered using standards for software development and maintenance. In these cases, one or more projects should be initiated to execute the responsibility to plan and manage the website throughout its entire life cycle from conception through retirement.

The website design should avoid the use of processes that result in irrecoverable data, except when needed for data privacy or 'do not track' requirements.

The specific modelling approach varies based on the project needs. Although website development tools can have minimal modelling, some level of modelling of the data flow, workflow and similar aspects of the website should be utilized.

If the website is hosted by a website provider, that provider may provide site documentation or specifications for available design and navigation features applicable to the web pages for an entire network, and encourage or enforce conformance to these.

Website and web page designs should be subjected to design reviews in keeping with good engineering practices. Depending on the value and expected impact of the website, additional reviews may be warranted. The design review may include evaluations of the graphical design, legal implications, cultural impacts, linguistic review, market research, accessibility and usability. The design review should span the entire range of functional objectives, technical capabilities and constraints throughout the system. The review should also address the capabilities and limitations of the target user community. The insertion of new technology into the system requires the widest range of reviewer experience. In addition, the content should be subjected to review by applicable experts and other users.

5.2 Design principles

Separation of content and presentation management is a primary design principle. The use of CSS to take care of the presentation management needs and use of content templates to take care of structure management can simplify site management.

The website should exhibit consistency of design, providing a uniform look and feel for the site. The website designer shall adopt, adapt, or develop a style guide to assist in implementing a coherent strategy.

Navigation aids, buttons, user-readable metadata in the body of the web page, such as headings (similar content), and other items commonly appearing on multiple web pages should be consistent across the site. The consistency should include the common look and feel as well as a common position on the web pages.

NOTE The website design, enforced through its metadata, can be explained in a style guide for CSS.

In situations where related organizations own related and interconnected websites, a coherent strategy should be implemented to allow consistent global navigation, search and information retrieval, security, and identification of site ownership among the related sites. Website design should consider the information structure, applying the following principles.

a) Information content is segmented into usable units (topics or chunks), neither too lengthy and complex or too short and uninformative (requiring many clicks to get to the needed topic).

b) The path to introductory and overview information is immediately evident on the website.

c) A sequence of topics leads users through more complex procedures, or from best-case or simple procedures to less-used or alternative information.

d) The general user interface guideline of ‘least clicks’ should be followed. This means reducing the number of user actions to access data or perform activities via the website.

Websites should adopt and conform to a policy regarding the separation of informational content from advertising and marketing content. If the website includes marketing material or advertising for other organizations not part of the website owner's organization, the home page shall include or link to disclosures relating to separation of editorial content and advertising, and label sponsored content and sponsored links.

5.3 Choice of devices and media

The website designer should select the types of media, such as animation, graphics, video, text, and chat dialogues, needed to best present the informational content for the intended audience. Selection of media shall include accessibility considerations for website interaction, i.e., inclusion of users with hearing, tactile or vision considerations, as further described in 9.5.

The website designer should consider avoiding technologies that are likely to be unavailable or unsupported in the foreseeable future. For example, some search tools cannot access content presented within frames.

The presentation format of a website should be independent of the information content of the website. Independence of content and format allows use of different display formats and use of different media for accessibility. Independence of content and format also simplifies site maintenance by content providers and website providers or web leads.

NOTE 1 A variety of techniques support independence of format, web publishing tools, and content, including CSS, semantic mark-up, such as XML or DITA, and functions provided through a content management system. The choice of media is influenced by the capabilities of the website provider and the user's display device (such as small-screen mobile devices).

NOTE 2 Requirements and guidance for selection of text or graphics media for information for users are provided in IEC/IEEE 82079-1 and ISO/IEC/IEEE 26514.

Comprehension and navigation are key engineering design considerations. Non-textual information (e.g. video, graphics, audio) can consume significant bandwidth, but can also provide advantages in delivering information that is easier to understand. The use of small-screen mobile devices, low bandwidth environments of some users, the inclusion of an option for text-only delivery, adaptation for the visually impaired, and delivery in multiple languages are issues that should be considered. Caching techniques can help maintain appropriate responsiveness during intermittent loss of electronic communication.

Given the ubiquitous presence of mobile devices, responsive web design (RWD) should be considered in any web design project. RWD produces output which is viewable and navigable with the devices and web software of the intended site users. It employs the use of flexible layouts (columns), scalable images, and CSS media queries. For content to be responsive to various devices and browser viewport sizes, layouts and content should adhere to the following principles.

a) Page element sizing of the site should be built with a flexible grid system that uses relative units such as percentages for width/height and the “em” scalable unit for font size.

b) Flexible images that are used in the design should be in relative units or make use of appropriate CSS (e.g. using CSS property overflow: hidden).

Different views should be enabled in different contexts by employing media queries. Media queries allow designers to build multiple layouts using the same HTML documents by selectively serving stylesheets based on the user agent’s features, such as the browser window’s size, orientation (landscape or portrait), screen resolution, and colour. Navigation elements should scale and be placed dynamically, so as not to obscure information and degrade the user's experience.

5.4 Engineering for website security

5.4.1 General

Cybersecurity has no finish line. The tactics, techniques and procedures (TTP) associated with cybersecurity breaches and attacks are constantly evolving and dynamic. Cybersecurity should be addressed on an end-to-end or zero trust basis with the principle of Cybersecurity by Design over the lifecycle of the software. Cybersecurity is integral to the development process and should not be considered as an afterthought and bolted on to the development process.

Development-security-operations (DevSecOps) integrates application and infrastructure cybersecurity seamlessly into dynamic development and operations processes and tools. The objective is to resolve cybersecurity concerns early, before the software is placed into production. The responsibilities are shared between the IT cybersecurity, development and operations teams.

NOTE 1 IEEE Std 2675 provides details of addressing DevSecOps concerns throughout the life cycle.

The site owner, website lead, and website host provider should understand the overall security requirements and design objectives for the website, including the business, legal, and regulatory requirements.

The website provider and website owner shall agree on a clear allocation of responsibilities for website security. The website lead should stay informed about potential security issues related to the website and its supporting software. Website designers, engineers, and developers should remain current on cybersecurity practices and regulations over the lifecycle of the website.

Good practices for security during website engineering and sustainment (see 9.6) include the following:

a) securing the development process associated with software code, including the secure storage of the source code and ensuring deployments are not compromised;

b) defining clear policies for deactivating deprecated devices and software (including operating systems and protocols that are end-of-life or outdated);

c) utilizing and documenting port assignments and secure protocols, and disabling unused access protocols and ports;

d) authentication, authorization, and auditing of access to website content;

e) monitoring of API access points, including errors; multiple failed attempts; large amounts of data exfiltration, which can indicate inappropriate access to sensitive information (including PII); and prohibiting execution of commands bound to the HTTP request;

f) use of security hardware and software tools on the web servers or cloud platforms.

NOTE 2 While a comprehensive guide to cybersecurity regulations and requirements is outside the scope of this document, the following is a partial list of cybersecurity references for a “Secure by Design” lifecycle approach:

— NIST Cybersecurity Framework;

— ISO/IEC 27001;

— MITRE ATT&CK Framework (https://attack.mitre.org)

5.4.2 Website operational security procedures

The website owner or website provider shall document a set of processes and procedures for regular testing of the website and for deploying patches and updates to both the software and operating environment. Updates and patches of the operational part of the website shall follow a release management procedure that identifies the deployed software. For in-house developed software, ongoing intrusion and penetration testing shall be applied to identify potential security vulnerabilities.

Because some vulnerabilities allow unauthorized persons to run malicious code and thus take over any device with a MAC and IP address, website developers and providers shall take precautions to help prevent their site from becoming a host of malicious code or other attacks. The website should include tools for the detection or prevention of lateral movement. Lateral movement is the ability of an unauthorized adversary to move beyond initial entry to the website to gain access to other protected data (such as proprietary data or PII) or other sensitive sites belonging to the website owner or accessible through the website provider's network.

For website security, the following activities should be constantly addressed, including the testing, monitoring and update of practices with respect to the application security. The website provider should have well documented processes and procedures for these topics, according to the security policy:

a) intrusion/penetration testing;

b) patching and CVE updates include a testing and release management strategy;

c) continuous monitoring for potential threats;

d) backup and data recovery exercises and procedures (see 8.5);

e) alerting the appropriate regulatory jurisdictions and authorities when breaches are detected;

f) availability of a notification list and procedures for contacting internal and external resources;

Security processes and procedures should be logged and be auditable.

5.4.3 Website security reviews and audits

Periodic reviews should be performed for conformance to security policies. Reviews may be at regularly scheduled intervals, as a result of a review-triggering event (e.g. page change), or when major architecture changes are to be implemented (e.g. expanding from an intranet to the Internet). Audits can extend to the asset, service provider, network provider, and many other functions. Regular internal audits should be performed on a periodic or random basis, as well as external audits based on service level agreements (SLA) and regulatory requirements, e.g. to validate that the network meets the defined security objectives.

Several security activities related to the website shall be reviewed or audited:

a) security of system design;

b) application code and API calls;

c) vulnerability scans;

d) intrusion and penetration testing;

e) system log files;

f) unauthorized access, including lateral movements in the network;

g) data integrity including backups;

h) exfiltration of PII and other sensitive data;

In preparation for an external audit, the system operator should collect sufficient monitoring data. This enables the audit process to use timely actionable and adequate information to determine systems issues as well as for a forensic audit in the event of a system breach. Periodic reviews and audits include scanning authentication and authorization records, definitions, and databases for the required minimum privileges, out-of-date users, and strength of credentials from posted user IDs with password information.

A qualified person associated with the website owner should assess the adequacy of the security indicators and security protection for the page and should subject each page with a security designation to a review before the page is initially placed on the Internet. The review should consider both the code for the page and the displayed page.

5.5 Engineering for performance, scalability, and sustainability

5.5.1 General

Web pages, websites, website content, and web projects have a lifetime, i.e. a life cycle. Often the end point of a website is indefinite while the website is being developed, but typically the website will change due to new technology, security threats, organizational changes, management policy for periodic re-evaluation, or changes in demand for its content. The website owner and developer shall estimate the duration of the life cycle or plan for a life cycle extending as far ahead as technical planning is defined. The website owner and developer shall design for website management and sustainment during its active life cycle. The website lead shall support the execution of the lifecycle planning.

The website owner, working with the website designer, should define clear performance expectations for various use cases of the website. The performance requirements should be confirmed with acceptable performance test results. Many websites are dynamic, with frequent progressively elaborated updates. The website designer should implement within the overall design the capability for easily and readily updating content while also considering flexibility for readily re-engineering the website to leverage technological advances and innovation.

The website design should take into consideration the potential technical changes, changes in standards, regulatory changes, policy changes, security, business continuity, financial issues, user input, and organizational aspects that affect information content, protection, designation, or access.

Dynamic websites usually mean the web page and the contents of the web pages are displayed based on user authorizations. To do this, the web pages must use the objects to display proper data for the user. The objects are not static HTML code; typically, they use programming languages such as Java, C#, PHP, or JavaScript that generate code.

The website engineer should consider the characteristics of the client and server environment, or cloud service, and its impact on access to the presented material by the target-user community. Plans should include contingencies for technical obsolescence and growth.

Resilience, backup and redundancy shall be planned to meet availability requirements, service level agreements, and regulatory requirements, including failover or disaster recovery and mitigation requirements. Such considerations should include corrective action for website breaches, such as undesired intrusion that results in altering website content, and loss of website hosting mechanisms including the communication services linking the website with ancillary interfaces including its users.

The designer shall document the targeted computing environments for the website for future sustainment. The selection of implementation tools (e.g. cloud services, servers, generators, and release levels or versions of HTML, CSS, XML, and scripting) shall be based on the evaluation of the target client communities and plans for site maintenance.

5.5.2 Selecting technical formats and standards to use for the website

5.5.2.1 General

The website designer shall allow website access by devices and software prevalent in the target user community.

The website designer should consider the legacy and anticipated evolution of the users' target environment, as well as likely changes in technology, website maintainability or extensions to the website.

NOTE 1 The rate of adoption of new technology at the consumer level often exceeds that of industry and the public sector.

EXAMPLE 1 Devices can include the following:

— wireless and mobile devices;

— smart TV and virtual reality devices with web interfaces;

— interfacing devices for user accessibility such as braille display units;

— access-specific or text-only devices;

— vehicular interfacing devices including display units;

— interfacing devices including display and administrative units for controls, appliances, and IoT devices and bots.

Website designers should avoid designing the website for one specific browser, because it can render improperly in other browsers. Website designers should apply similar web layouts across multiple platforms to provide consistency while helping to minimize confusion and frustration of users.

Site designers should avoid over-specifying websites to avoid web link obsolescence. In general, the greater the specificity, the more likely the link will become outdated. On the other hand, a more generalized website address can force the user to click through several layers to get to the precise website needed. The site designer should exercise judgment between over-specifying the website link or forcing the user to do extensive searching once connected to the site in question.

Designers should consider hardware (including firmware) and software compatibility. Considerations should include screen display area (which can be quite small), communication latency, i.e. satellite links, wireless channel bandwidth, and limited (or non-existent) local cache.

The website infrastructure, including communications bandwidth and cost considerations shall meet performance needs for response time.

EXAMPLE 2 Limited bandwidth and "per minute" tariffs are common on an international basis and in the dynamic mobile and radio communications environments.

Protocols or protocol subsets for supporting mobile and IoT devices may require additional consideration in selection of target protocols.

Websites may monitor client browsers and capabilities as a basis for consideration of ongoing environmental configuration (and documentation) changes or updates. Website designers should also configure the website for compatibility with accessibility tools (see 9.5).

The technology and standards related to the development of websites changes rapidly over time with innovation including the development of new versions, and changes in technology (including browsers). Designers should consider portability of legacy code and all associated valid metadata having the capability to make use of cloud web services and apps. For integrity, external and internal metadata including DAM (digital asset management), XMP (extensible metadata platform) and news exchanges where applicable should be periodically validated. Support for older formats is eventually deprecated within browsers, so websites that are developed using older technologies should be updated or risk becoming inaccessible, insecure, or unusable for their audience. Therefore, designers should investigate and select formats and technologies that are currently well supported and likely to retain viable future support. Portability to different standards should also be an important consideration. Upward compatibility is particularly important for areas with changing standards, such as AI and multimedia formats.

NOTE 2 Standards and recommendations for HTML, XML, and other data formats are maintained by W3C.

5.5.2.2 HTML versions

The version of HTML, and the features within that version of HTML, should be selected based on the client environment of the target-user community and the source content management system. For example, frames are incompatible not only with old browsers, but also with some types of output devices like voice synthesizers or (line) tactile displays. Such features should be given critical evaluation in the design phase. Removal of an architectural feature like frames can require significant redesign. Web page developers should be familiar with XML and evaluate whether it is needed to incorporate XML into a website.

XML objects only contain the data to be displayed or received in the web GUI. XML does not prescribe how the data are displayed. XSL defines the web GUI layout. For communications between the client and web server, a common data format is JSON.

5.5.2.3 Cascading style sheets

Web pages shall separate the presentation from the content, to the extent that it is feasible.

The trade-off between accommodating a greater range of target-client browsers using page-specific characteristics and the maintenance advantage of page-independent presentation offered by style sheets shall be included in website design.

Web page generation tools should support CSS as an external style sheet, only using site-developer specified/selected ‘class’ (or ‘id’) attributes and avoiding the ‘important(!)’ designation so end-users can apply their own style sheets to match their preferences or requirements.

The decision to use CSS should include evaluation of the capability of target user environments.

A simple example is using colour in web pages. Explicit incorporation of colour is one option; style sheet incorporation of colour is another. The same colour scheme can be applied to a diverse set of pages in a consistent way using a style sheet, reducing coding and maintenance effort. A change to the common style sheet, rather than changes to the many pages using that plan, can accomplish a change in the colour scheme. Moreover, specific user communities may want or need to override the colour selection put forward by the design (e.g. visual impairments), which is viable with a mechanism such as cascading style sheets.

Similarly, if hard-copy printing of a page is desirable, the CSS printer presentation style should be included.

5.5.3 Bandwidth efficiencies

The first bytes (including <head> bytes) have the most impact on network overhead. TCP operates with a “slow start,” awaiting an acknowledgment of initial packets sent before initiating a full sequence of transmissions. This avoids congestion of the net that may be directed to a nonresponsive site. This makes the data transferred first from the server, and initial elements of the page (e.g. <head>) more critical in response time and network loading. Data in the <head> sequence should be focused to minimize overhead and provide essential data to the client. Since the HTML format calls for all metadata to be in the <head> section, the developer should test changes in code in order to maximize bandwidth efficiencies.

The system design should consider newer protocols that are more efficient and effective where there are situations of limited bandwidth or network issues that have poor transmission. Networks that have significant delays, such as satellite communications networks or latency-sensitive, near real-time applications, can benefit from more efficient protocols.

EXAMPLE 1 One newer protocol is QTCP which enables senders to gradually learn the optimal congestion control policy in an on-line manner. QTCP does not need hard-coded rules and can therefore generalize to a variety of different networking scenarios.

There can be significant overhead in loading pages generated from some website applications and from unused CSS. Tags expected in the head section of a web page including minimal overhead would include: 'title', 'link' (to style sheets), 'meta' (as designated in Dublin Core plus 'keyword', 'description', or "http-equiv"), 'base', 'script', 'object'. Where extended sets of metadata, style or scripts are included, the 'link' element should be used to reduce 'in page' overhead. Relevant information about the metadata should be indicated with the 'profile' attribute of the 'head' tag.

To facilitate indexing presentation of a collection of related pages, the “initial” page in all of the pages should include the “link” element.

EXAMPLE 2 <link rel="start" type="text/html" href="first_page.htm" title ="whatever the title of this set should be" />

5.5.4 Document type declaration

Static web pages have initial lines with <Content-Type>, which may also be applied to dynamically generated web pages. <!DOCTYPE.> indicates the DTD applicable for this page. XHTML pages should have the initial <?xml version=”1.0” ?> declaration, and for HTML consistency may need to include both HTML and XHTML head elements. The incorporation of extraneous data at this point is poor web page engineering.

5.5.5 Description metatag

The Description metatag may be used to provide guidance to search engines on what to present users in the search response (e.g. <meta name="description" content="response" />). W3C guidance defines and recommends usage for Description metatags. Search engines often display the first few lines of a web page to help searchers to identify the sites they want. Some engines display the metatag description attribute instead. This display can persist long after the actual web page has been deleted. Therefore, for specific information to be visible, its placement near the top of the page can help. If information is to be invisible, then early page placement should be avoided (for various reasons search engines may be displaying pages that the designer did not intend to have publicly available). Finally, to assure old information is not presented by search engines, it may be necessary to replace the page with a "no longer available" message page for an extended period of time to provide for search engine replacement of the earlier data (resubmission may also be useful).

5.5.6 XML considerations

XML provides mechanisms for delineating document structure in ways that are responsive to business objectives. A well-formed HTML document is one instance of an XML document. XML provides for new tags that can be content specific, and facilitate automated processing of content. Within the HTML environment, XML-type structures should be designated with the id and class attributes, and potentially the and elements.

Within an HTML 4.0 document, id is defined as being unique, and can be used as an anchor for fragment links, whereas class can be duplicated many times within a document. Both id and class can be used to distinguish a page segment for style sheet presentation control (developers should verify that usage of 'class' and 'id' for style specification work for the targeted range of browsers).

For HTML5, the rules applying to class and id attributes are very similar. The website developer should plan for the accommodation of a range of browsers identified in the target user community client environment during the design planning process. This can be accomplished by identification of browser types and delivery of different sets of pages based on this, or by ensuring that the critical information content for a page can be effectively presented by the full range of browsers. Browser and version-specific dependencies should be avoided.

5.5.7 Image formats, image compression and video

During content negotiation with the server, the server may identify that the client can accept compressed content. Compression of static pages reduces site and network overhead. Delivery of compressed dynamic pages can be a useful trade-off to deliver content to the client with the least connection overhead.

Encrypted data cannot be compressed, so if data is also to be encrypted, it should be compressed first.

Similar formatting of images into efficient formats, such as JPEG, PNG, or GIF, can also provide timely response to clients that can accept these more efficient formats. The smallest acceptable image should be transferred to the client. The client's selection of data formats can be critical to client-side applications and should be respected when possible. Thumbnails, which are miniature pictures of an original that is scaled down, should also be provided for large size images.

The website design should also include considerations for video communication, associated video communication protocol, and the operability of the various video types.

5.5.8 Server technology independence

Depending on the target audience and the desired sophistication of the pages, a web page may make use of server-side capabilities such as server side include (SSI), active server page (asp.net), or other capabilities. It is desirable, whenever possible, to produce pages that are platform-independent and do not depend on server settings or capabilities. For example, avoid links to a directory in a relative reference. Instead point to the file within the directory. For example, <a href="detail/"> should be

<a href="detail/index.htm">. The default file can vary from server to server; pages that reference directories are not portable from one server to another.

Because more server code is treated as comments by browsers, these pages can be usable across a wide range of servers even though their appearance can change.

The ultimate goal is to allow pages, whenever possible, to be moved from server to server, used in cloud services and even be moved onto transportable media devices for distribution without suffering from broken links.

5.5.9 Designing for performance and scale

5.5.9.1 Scripting and executable considerations

Client-side execution such as scripting may be refused by clients. Part of the design process shall include documenting when, if ever, such facilities may be used. The design process shall include documenting when, if ever, scripting is being used.

If a site requires scripts for some features, then the server shall notify the user that downloading of scripts is required. Selection of specific tools or versions of implementations shall be considered in both the context of the target-client environments and the life cycle management of the website.

Because client environments may disable client execution or scripting for security reasons, servers should be able to deliver information without scripting on the client. Where possible, standards-based environments that are independent of the user's processor, operating system, and browser should be developed.

5.5.9.2 Server and client-side executable code

Executable code from scripting languages is widely used and supported by most recent browsers. Scripts can operate on the server side using, for example, the common gateway interface (CGI), or on the client side through scripts embedded in the page or applets. However, not all browsers support client-side scripts and users may turn off both Java and client-side scripting. This can be a matter of corporate security policy, or to reduce the distraction of intrusive dynamic elements. The W3C stipulates that any web page using client-side scripts is required to provide the same functionality on the page without the scripts to be considered accessible.

NOTE 1 See Techniques and Failures for Web Content Accessibility Guidelines 2.0 at www.w3.org.

Dynamic page creation should be focused on server-side scripting/programming. This facilitates end-user accessibility, the range of target devices, and security.

NOTE 2 Persons accessing pages using non-visual means can have trouble identifying dynamic page changes and become frustrated with scanning duplicate content to identify changes.

5.5.9.3 Database management system considerations

Databases used in web environments enable the data persistence or dynamic update and integrity of the site. Databases may be used in the presentation of website content, in collecting tracking information and in the management of the website. Most website management tools use database environments to organize and manage resources. The website designer and provider should consider the responsibilities and tools to define the architecture for centralized, local, and distributed databases.

Database performance is commonly a primary constraint on the website performance. The website designers should carefully consider data design and database security, implementation, host, maintenance, backup and restore as key points of website engineering.

Database management systems should be selected so that data can be used, exchanged or distributed to different platforms without significant changes in configuration and web programming, and in consideration of anticipated traffic and website growth with the scalability of the database and host

environment. Associated reporting or report generation needs including ad-hoc reporting desired by the website user should also be considered. Database engineers should consider data access and security needs for encryption of data.

6 Testing and evaluating websites

6.1 Test planning

Test planning includes the procedures and methods for the tests to prove the website system meets the requirement specifications. Developers, testing staff, and quality assurance (QA) engineers follow the test plan and perform testing and evaluating tasks using the auto-test software or manual testing. The test coverage and choice of tests shall be planned in consideration of the risk to site users and the website owner of untested but defective features. Types of testing in the test plan may include:

a) functionality tests of the website;

b) positive and negative test plans for GUI controls, especially for the web control objects, such as textbox, checkbox, ratio box, list control, dropdown list, and address bar;

c) robustness of the website against the possible common failures and critical use cases;

d) content protection, especially protection of controlled information, from malicious readings and changes;

e) viewing web pages on a variety of displays and with different resolutions and colour settings to validate that the web page content remains readable and legible;

f) cross-browser support: of different browsers with different rendering engines to parse and display the contents embedded in the HTML/CSS;

g) website scalability and responsiveness which meet the peak load requirement in each defined use case;

h) security testing against common hacker and malware attacks.

Test cases should be created based on the test plan. All test cases shall be executable; and test results shall clearly show whether the related website features meet the requirement. The comparison of the test results and the requirements indicates whether the website system has passed the test case, or not. The final evaluation results of the websites are decided based on all test results in the test cases.

NOTE 1 ISO/IEC/IEEE 29119-1 describes software test planning and testing concepts and can be applied to website testing. Other parts in the ISO/IEC/IEEE 29119 series cover test procedures and test documentation.

NOTE 2 Taking into consideration the different perspectives of different users, ISO/IEC 25010 provides guidance and a framework for discerning quality requirements within the context of different user perspectives. The document contains a quality in use system model with a number of characteristics that covers the human-computer interaction systems in use. For measuring and evaluating system quality, it provides consistent terminology for reference during system testing. For reporting usability test results, see ISO/IEC TR 25060.

NOTE 3 ISO/IEC 25020 provides the criteria for selecting software quality measures and quality measure elements along with the issues affecting the reliability or validity of measures. It provides a guideline and a framework for measuring quality requirements and evaluation of software products.

6.2 Testing for usability

6.2.1 General

The website in development should be tested and evaluated for effective human-computer interaction.

The website owner and primary web lead shall establish the methods, processes, and procedures to test the site for usability. The website developer (which can include architect, designer, or QA) shall develop criteria for evaluating website usability by analysing the target-user community and information to be retrieved. The website developer or testing team shall prepare test cases to evaluate the user interaction with the website.

New site versions should be tested before being released for general use. Development testing shall be conducted as part of the implementation process. Validation should be pursued in at least two distinct phases: development testing and operational testing.

Testing for usability may include the following:

a) accessibility of the site to a range of differently abled users;

b) testing by users or user representatives for acceptable results in terms of response time and relevant information retrieved from the site;

c) ability to print web pages in usable format.

NOTE ISO/IEC/IEEE 26513 contains details regarding usability testing for sites containing information for users.

6.2.2 Validation of markup language and accessibility conformance

Many development tools have validation support embedded in the coding environment. Submission of web pages to external validation tools shall be done in a way that is consistent with the proprietary nature of the information content. Web pages should be submitted for either internal or external validation of HTML or XML for DTD conformance and WCAG 2.0 compliance using tools such as the W3C Markup Validation Service http://validator.w3.org.

6.2.3 Operational validation

Even though no changes have been made to a website, its operations may change due to changes elsewhere in the network. Therefore, links identified within the website and external resources used within the website (such as data feeds, pictures, videos, and frames) should be validated and updated on a regular basis.

The validation process is in addition to live broken link error handling that should be included inside the HTML code, scripts, and other website elements. Using web analytics tools supports statistical measurement and evaluation of website performance and success of conversion rates (the percentage of users who take a desired action on the website). Analysis of daily unique hits, monthly page views, and browser statistics can support the following:

a) correction of invalid links, either changed to a currently valid link or removed from the site;

b) identification of orphan pages and a decision to remove the page, link to the home page, or to leave the page (possibly due to external traffic to the page from a different user profile);

c) affirmation that resources such as images, videos, and other site content are still valid and a decision to replace or remove references to unavailable resources;

d) verification that links have not been “hijacked” and link to the intended information;

e) verification that different protocols such as HTTP, HTTPS, FTP, and others are working properly and have updated certificates, authentication controls or other validation methods.

Site documentation for websites presenting ICT information shall have an identified set of measures to evaluate whether the website is meeting its goals. The plan shall include the set of measures to be collected and analysed, the methods that are used for the evaluation, and the acceptance criteria for approval of the website design.

Website assessments shall be done on the objects (text, graphics, layout, navigation, multimedia) as delivered to typical client devices, and not assuming that generation tools can convert the source accurately.

The website tester shall check for errors in text and links on static as well as dynamically generated pages.

Common user interface characteristics can be evaluated by inspection, such as visibility of system status.

Simplistic "hit rate" measures may be insufficient unless web pages for low-bandwidth or text-only users are being compared to equivalent web pages. A representative measure is the time or the number of keystrokes required of the user community to arrive at the desired end page.

QA should be part of site planning and development. The project plan should indicate specific tools and processes to be used during implementation to assure the quality objectives are met.

Web pages should be subjected to proofreading and QA. Proofreading should involve the use of the full range of browsers, screen resolutions, and browser window sizes and shapes.

The QA process should validate that the presentation meets all the objectives and requirements of this document and other applicable standards. It should also validate the user requirements.

6.2.4 Active links

External links shall be tested before and after each system release.

The website owner or provider shall periodically test external links to verify that all links are still active. Automatic review of links, which can use metadata, can help to quickly identify targets that are not valid anymore; and human review of links may validate that the correct content is linked. Use of persistent URIs helps to avoid some of the problems created by these references.

Links that go to pages with critical information should provide indication of the last verification date, e.g. Mfield (<linkverified>, <... class="linkverified">).

6.2.5 Dead links

Care should be taken that all web links are up-to-date. Dead, inactive, or missing links severely detract from the utility of a website. Websites demand periodic maintenance so that that links are current. Automated tools exist that check the existence, if not veracity, of web links.

6.3 Testing for performance and resilience

Performance tests, scalability and load tests, and stability tests are important for supporting site usability and responsiveness. Auto-test software is available for performance testing. These tests can be performed using the script languages on command lines, such as JavaScript, Power Shell, or Python. The use of script languages allows for flexibility to change the auto-test application behaviours.

The website tester shall test performance capabilities of the website, simulating the anticipated peak load to be supported when the site is in operation. The evaluation shall include the anticipated client environments of these target-user communities. Diversity of browsers in use, complementary capabilities (e.g. script, byte code, graphics), and the bandwidth of connectivity shall be included in this environmental evaluation.

The performance tests shall include the tests of the website's resilience, especially in the case of changes in server-side resources. Performance tests should include the test cases that measure the average response time when some resources, e.g., servers, are unavailable. Resilience tests should also include the website system robustness when parts of the resources fail.

6.4 Testing for security

Website system security tests and evaluations are essential because the systems can be vulnerable to cybercriminals and hackers. Depending on how the website is hosted, most security problems can be handled by the platform or cloud service provider. Website owners and hosts have more extensive security concerns when they host the websites.

Websites should use https protocol instead of http.

The website system shall be tested for vulnerability to security malware and hacker attacks. For website security testing and evaluating, the following should be confirmed, as applicable for the content and intended audience of the website.

a) Login controls and user credentials such as two-step login functions, are active.

b) User passwords are never stored in raw text format.

c) "Forget username or password" functions are working.

d) User personal identification information is protected from improper use.

e) Restricted pages require user login.

f) No restricted information shows up in general user sessions.

g) Only the data in the incoming requests are used; no command coming from outside is executed, especially when the website system uses XML DTD.

h) XML data structures are defined by XSD. All XML data have their XSD.

i) Common hacker attacks are tested with the website security features.

j) No SQL script is bound in the //https request if the website system connects to the database.

7 Managing the website

7.1 Website roles and responsibilities

The roles in Table 1 shall be involved in website management and engineering. The roles may be combined and delivered by one person taking into account workload and competence. In applying this document, one person can assume many roles, and one role can be held by numerous individuals or subgroups within the organization. There are no requirements for independence of roles in this document. For these roles, it is not necessary to have one unique team member each. It is feasible that one person may be competent to serve multiple roles, so that the website team size can vary depending on the organizational processes, roles and staff.

Organizations shall designate a web lead (or project leader where website is part of a project) with responsibility and accountability for achieving the objectives of website management.

Table 1 — Website management and engineering roles

Role	Function
Website owner	Source of website content and requirements. Can be supported by the business analyst
Site provider	Provider of the site address and the infrastructure to host the website
Content manager	Controls and manages content of the website manually or through a content management tool
Web designer/developer	Creates the layout and functions for the GUI, data interfaces, and website software
Web lead	Manages activities related to website development, operation, and maintenance

Table 1 *(continued)*

Role	Function
Privacy lead	Oversees compliance with applicable privacy requirements and regulations for protection of collected, shared, stored, and revealed personal information
Quality reviewer	Reviews activities performed for website development, management and maintenance
Tech support	Supports website application software, infrastructure, and users
Security manager	Manages and oversees security protocols and procedures for the website
User	Uses the website to retrieve information

7.2 Control of information content

Effective websites are designed to minimize the sustainment effort needed to change the website content. A change in content can be due to changes in organizational strategy and policy, technology, standards, information and status updates, or errors and defects. Changes in policies (e.g. organizational, regulatory, and legislative) and stakeholder needs can lead to changes in information content or access controls. Change management of website is a core task for the control of information content.

The website owner, web lead, and website provider shall establish the methods, processes, and procedures to control changes and keep the site content current or labelled as to applicability.

NOTE 1 Some web pages are applicable to particular versions, regions, languages, or platforms.

Individuals shall be designated with responsibility to develop, maintain and review the updated content, approve updates, and release updated content into operation.

The website owner and web lead shall establish the requirements and procedures to handle outdated (no longer current) content. The requirements and procedures shall include:

a) how to identify when content is no longer current, for example, the product being discussed on the web page is no longer manufactured, is no longer sold or has been substantially changed;

b) how to notify users that the content is no longer current; this may include on page notification, email, or other means;

c) who to actively notify that the content is no longer current; this may include notification to web leads of inbound links that the content is outdated and, if applicable, a link to the current content;

d) how to handle out-dated content; this may include permanent archival, time based archival with eventual removal, or complete and permanent removal; see 8.5.2.

Daily website management is typically the operation team's work. They handle the website product updates day-by-day. The operation team also monitors the website performance and the users' feedback. They also summarize the website running statuses and report to the management team. They can also suggest feature changes of the website for the next version. They may also perform a product website rollback when the new version has serious problems.

NOTE 2 The procedures can assign responsibility to individuals to update page or site content as needed, allow a select set of people to make comments or maintain an online conversation, such as in a blog environment, or schedule updates with version controls.

7.3 Managing security

Website security should be managed and reviewed in regular intervals. The website host and website lead should regularly review (or set automated tools to review) and notify website server and firewall logs of unauthorized access or probable breach. The security of the content management system itself should be reviewed regularly as well. For instance, the codebase should be regularly reviewed for code-related security breaches. For transaction-intensive websites, vulnerability and penetration testing should be carried out in a defined time schedule.

An updated printed copy of security processes and procedures shall be available offline for all security operators.

8 Sustaining the website

8.1 General

Website maintenance, including updates, should be planned, executed, monitored and controlled to keep a website functional, accurate, current and accessible. The website provider should plan for maintenance to include procedures for scheduled (preventive) and unscheduled (corrective, event-triggered) maintenance.

8.2 Continuous delivery, content validation, and versioning

The provider should have governance processes set for regular review of the design and currency of the content. Proper change management and configuration management processes should be defined with appropriate tools and clearly communicated among the maintenance team to facilitate seamless content update, versioning and delivery. Different types of changes are possible, e.g. content, graphics, structure, and addition or deletion of web pages. The governance process should cover all such changes.

In addition to manual change management, the automation of change management, testing and content delivery may be planned. An update schedule should be prepared and published.

When major changes are going to be made to websites, these changes should include timely notification to the users. This notice should assist users in knowing that they can expect a change and maintain their confidence in the website content. When action is required by the user, a clear, concise and easily understood message is recommended. An example is: “You need to change your password; an unauthorized or unknown device tried to access your account.”

When the site is undergoing maintenance, visitors should be made aware that the site is unavailable or operating with limited services, and the expected date and time when full service will be restored.

A website can include notable complexity, particularly if the site implements interactive functionality or involves multiple developers or organizations. Particularly in complex cases, a software maintenance process of versions and version release should be adopted. This provides a disciplined basis for the maintenance activity. A specific state of the website can be clearly identified and assumed if required (e.g. in case of a restore from backup, see 8.5.1).

Site versions should be readily displayed or referenceable via the site.

Furthermore, the web lead or project manager of the site should consider the following.

a) The website should maintain accountability and audit trail for all changes made to the scripting, framework, structure, and code.

b) A source code control system may be used to coordinate code changes, especially when multiple developers are involved.

c) Separate modification timestamps should be provided for content updates and for scripting, framework, structure, and code changes. The timestamps aid in identifying pages where testing or debugging should be focused and allow proper versioning.

d) If style sheets are not available, the website design should use an alternate method for indicating page classifications. Style sheets may be used to indicate obsolete pages or other classifications (e.g. “draft,” “superseded,” “confidential”, “sample”) as watermark.

e) An alternate method for accessibility to users with need for special assistance should be included.

NOTE The following standards can be relevant, assisting all parties and stakeholders involved to establish appropriate change management and configuration management processes as well as managing the full life cycle of the implementation of the website.

— IEEE Std 828 describes change management and configuration management processes and how they are accomplished as well as roles and responsibilities for activities, timeline and required resources. These guidelines support implementing continuous delivery and content validation.

— IEEE Std 2675 describes the processes, activities, and tasks that comprise the life cycle of software systems. These processes, activities, and tasks can be applied to the full life cycle of software systems, products, and services, including conception, development, production, utilization, support, and retirement.

— ISO/IEC/IEEE 26531 describes requirements for efficient development and management of information content produced throughout the life cycle of a system and software product.

8.3 Handling disconnects

8.3.1 General

The consistency of the website's links should be checked on a regular basis. All page links of the complete site should be either auto checked or manually randomly checked with a defined frequency. A non-reachable or non-existent page (a 404 error) should be reported to the maintenance team and a proper informative error page should be shown to the website visitor with possible means to search the site or offer documents and references with similar URLs.

8.3.2 Site or page relocation

Changes in client or server environments can require or warrant site modification or re-engineering (e.g. the shift from desktop to mobile devices, the shift from central data to cloud computing, the discontinuation of a hosting service or program), but should not affect or change the way the site is accessed.

A website shall be reachable under a site-specific DNS A, AAAA (address) or CNAME (canonical name) record, e.g. "https://site.domain.com". Part of the site maintenance procedures shall include verifying that the appropriate registration for the DNS remains current. Site-specific names should not include a specific machine name, location name, physical IP addresses, or other element that is likely to change with time.

Documents of enduring relevance should be provided with URLs that are similarly enduring. For example, the path coded in a URL should not mirror the transitory organization of the website. The organization of the website may change; the URL to access enduring documents should not.

Relative URLs and host relative URL servers can use the "redirect" capability of either HTTP or server scripting to return the right page to the user. This can be used to accommodate changes in page location. Relative URLs allow for:

— migration of pages within a site;

— maintenance of a replica or development version;

— consistent digital signature/integrity validation.

8.3.3 Redirection

Servers should respond to attempts to access invalid links within an existing site by redirecting such requests to a defined working page with an explanation of the error and some navigational hints.

Redirection or refresh of a page shall not inhibit a user's ability to navigate to prior pages. Users shall be allowed to return to the page from which they initiated a link.

Redirection may be initiated by a server to provide better response to user request. Redirection for better performance shall be transparent to the user. For example, a containerized cluster can redirect the request to another pod or node, but this doesn't redirect to a different URL.

Reasons for applying redirection resulting from site maintenance include:

— page location changes;

— catch directory changes and direct request to the correct URI;

— accepting and resolving mistyped URIs;

— eliminating case dependencies in URIs;

— adjustment for differences in object name extensions, e.g. htm/html, jpg/jpeg;

— common spelling errors that may be site-specific;

— providing default for attempts to access directories;

— delivering selected web pages to client from a selection list;

— accommodating language preference;

— accommodating text-only preference.

Redirection has the advantage of providing back the corrected URI so that bookmarking occurs with the current version. The designer should consider the value of having directions for users to implement the redirection manually, when appropriate.

8.4 Security monitoring and measurement

The persons actively monitoring for messages should direct the message to the persons assigned the responsibility for responding to the message. A website may have multiple web leads responsible for independent subsets of the website. In this case, the persons monitoring for messages should direct the message to the appropriate internal web lead.

After a website is launched or significantly modified, the owner and website provider shall regularly monitor the site's security attributes and assess security risks (see 9.6.2).

The following should be included in a risk assessment:

a) development framework used to develop the site;

b) any underlying databases;

c) access vectors – is the site exposed to the Internet or is it only internally accessible;

d) existing and new security protections, such as firewalls or host-based security systems, or prediction of threats, e.g. identified through artificial intelligence analysis of user behaviour singularity or traffic analysis singularity;

e) analysis of the security metrics and trends.

8.5 Backups and archiving

8.5.1 Backups

Website information and configuration settings shall be backed up and stored on a regular basis so that they can be restored or archived as approved. A backup and archival policy should be defined and communicated to the relevant stakeholders. Backup procedures shall include tasks and responsibilities before the backup, during the backup, after the backup and during restorations (e.g. disaster recovery).

Backups and restores should have a documented set of procedures and storage based on the importance of the data to the organization and the risk to the data owners. Access to the backup systems should be restricted to authorized users. Access to the backup should be monitored and logged for unauthorized or unusual activities. Data that is critical should be also backed up with offsite, off network "air-gapped" media.

Continuous automated backups may be accomplished by the use of continually mirrored or redundant sites rather than by periodic backups. Major releases of the website versions shall receive a full backup.

Backup procedures should be specified using automatic backup mechanisms when feasible. Identification of the backup should include website identification, date and time information, responsible party identification, and other relevant information to restore the website on another machine. Backup procedures should specify the service responsible for storage of the backup copies.

Backup content supporting the website should include code, data and databases, multimedia resources, and other files that contain the website and make the website functional. The backup content shall also include appropriate architectural system diagrams and dictionaries (including database dictionaries) as well as pertinent documentation.

Security of the backups shall meet or exceed that of the backed-up website. Security of backups may include encryption of the backup and offsite storage. Multiple offsite locations or redundant cloud hosting, each with its own backup copy, may be appropriate. A backup that is not connected to the usual network can protect data and websites in the event of a catastrophic disaster or ransomware attack.

The website provider shall periodically verify that websites can be successfully restored from backup, or that dynamic content can be regenerated. The checks can be automated or performed manually by simulating restoration to verify its integrity. The website operating procedures should be available from an offsite location. The website provider shall inform the website user of the length of time required to reactivate the website from a complete loss of service.

Restoration of the information methods, processes and procedures should consider the backup media retrieval and the backup media usage. These methods, processes and procedures may be different for different situations, e.g. retrieval may be different for a partial or a complete retrieval. The reason for the retrieval may also cause use of a different set of methods, processes, and procedures. For instance, retrieval due to unintended site destruction, security breach, or a natural disaster each may require a different set of methods, processes and procedures.

8.5.2 Archiving

At the end of a site's life, for historical, business, or legal reasons the site may be archived in various ways:

a) kept in its current state and annotated to indicate the dates or versions of the system for which it was applicable;

b) reduced to a minimum of informational pages;

c) if the site is obsolete, removed but kept in a retrievable state.

If there is no need for archiving, the site may be permanently removed.

In case of partial or permanent removal, the site contents can be archived in the form of the most recent backup. References to the removed site should also be removed from search engines and directories as well as referencing web pages. Any links to other sites should also be considered, such as notifying the other sites.

A formal decommissioning process should be established involving relevant stakeholders and including consideration of appropriate notification of site users and legal considerations.

9 Website features

9.1 Web page components

9.1.1 General

Websites shall have at minimum the home page, website owner details, required contact information, page titles, website content, and site features for information discovery and retrieval.

The website shall have a defined structure for organization of its information content and functions. A well-organized site structure can also simplify maintenance and sustainment of the site as information is added or archived in the future.

The website structure should reflect the information-seeking tasks that can be performed by the users, allowing them to readily understand the site's organization and find the needed information, such as instructions for tasks to be performed. The structure should be visible on every page, such as through menus, tabs, or display of higher-level pages in a breadcrumb trail. When the users' task is primarily to find technical information, the site structure should reflect the logical organization of the enterprise or the products, services, systems, procedures and instructions, or concepts to be presented. The site organization should place frequently used information where it is readily accessible (one click) from the main website page (home page). Frequently used features like search, and site login, logout, and registration (as applicable) should also be readily visible on the home page. Page content should identify the likely frequency of changes and last updates.

The structure of a website may be hierarchical or flat. Subordinate websites may be separately managed. Such management should reflect the applicable policies of the organization. Websites are not implicitly hierarchical. Figure 1 illustrates a hierarchical information architecture for related websites.

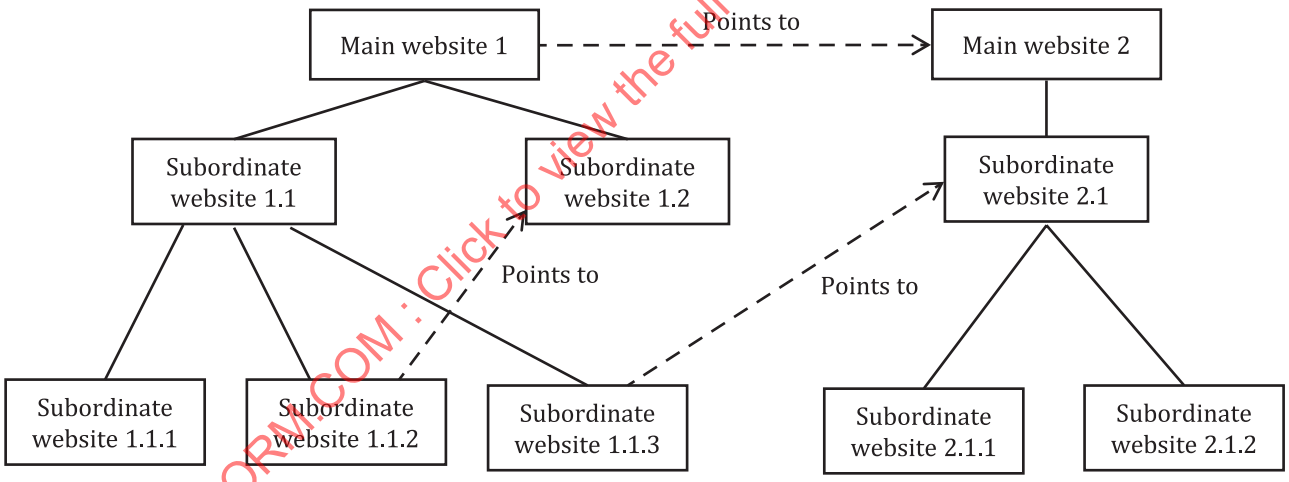

Figure 1 — Example of website information architecture

A site map document or illustration may be created for URLs and metadata for those URLs. The site map may be labelled as a site map and tested for usability with accessibility-compatible website readers.

The segmentation of content into pages for display may follow a choice of principles for ease of use. Windows and browsers can easily scroll and zoom to accommodate various amounts of content. Extended text presented on a single page is more easily comprehended when headings identify topics on the page. Very long pages, which typically require scrolling several times to view all the content, should display links to headings at the top of the page, serving as a table of contents. Important or summarized content should appear at the top of the web page, with less important or detailed content accessible through scrolling.

The orientation of the device, landscape or portrait, should be considered in the design of content. The location of data that needs to be entered by users should not be hidden when data is required to be entered. The ability to easily navigate the web page will vary depending on the capabilities of the device.

The use of popup notifications should be designed to minimize annoyances.

Default files for compliance to legal regulation or policy, copyright information, contact information, style sheets, and other site-specific data may be created for a site or inherited from a broader organizational context.

9.1.2 Website home page

A website shall include a home page. The home page shall provide a comprehensive view and links to the types of information available on the site.

Websites that are part of a larger site construct shall contain a link to that overall site's home page. The home page shall either contain, or provide links to:

a) “top-level pages” (home pages) for this site;

b) purpose of the site and intended users or tasks the website supports;

c) disclosures of the site owner and the responsible web lead (site maintainer);

d) terms and conditions of use;

e) privacy and information-sharing policy, including cookie policy and identity-capturing policy, in compliance with legal and regulatory requirements;

f) applicable intellectual property considerations (copyright, trademark, etc.) (see 9.7.5);

g) dates of last content update for this home page or policy pages indicated by this page;

h) third-party plug-in download site, if needed.

The home page should include a search tool to assist access to specific information. Since some users have low bandwidth connectivity, the home page for a site should load quickly (e.g. within 5 s).

The home page may also contain:

— search services for the site;

— any brands applicable to the site (logos or marks of certification or affiliation);

— other statements about the site owner;

— information about new content on the website;

— if the site is owned by a subdivision of a parent organization, information on the functions of the parent organization and a link to its website, if any.

Since the home page may be loaded on a variety of devices, its graphic files should be resized to minimize the time to load, and its graphics should contain height/width tags and alt tags so that a user can quickly identify the content of the page. Reusing graphics will have a positive impact on the overall performance. For the same purpose, multimedia and other large files such as audio and video should be designed and tagged to load after other lighter content elements of the page, such as text and images, have already loaded.

9.1.3 Identifying the website and its owner

The identity of the website and the website owner shall be accurately and legibly displayed on the home page or other directly linked pages (e.g. "About" page). The website shall indicate the sources

of its information that are not owned by the website owner. See 9.7.5 regarding intellectual property considerations. The site shall contain a statement of policy for redress (correction) of inaccurate information found on the website and contact information whereby the website owner and web lead of the website can be reached.

Identifying the website may include a page with descriptive information about the site owner and contact information, supplemented by banners or logos. The website should indicate whether the site is applicable for one country or internationally. Users can thus evaluate the credibility of the information presented and identify potential sources of bias.

NOTE In some jurisdictions, contact and website ownership details are legally required.

The site should contain contact information for the site owner, the web lead, and the website provider. The contact information should indicate whether and how quickly users can expect a reply to their attempted contact.

The site may include contact information relevant to legal rights or recourse in the event of difficulties with site-provided information (warranty).

Contact information may be Internet based and should include telephone numbers or physical addresses.

9.1.4 Page title, header, and headings

Every web page shall display a distinct descriptive title. The web page title shall include useful and distinctive indication of the contents.

The web page title should be placed in a consistent location and presented in a consistent style for pages of the same type in the website. The title should be chosen carefully, considering its role in search engine indexing, query responses, window title bar, and in bookmark labels. If structured consistently, it may also improve the orientation of the user in the site.

Web pages should contain only essential header data.

EXAMPLE Non-essential header data include, for example, links to external sites, where the link can frequently change.

Heading data should provide useful information for meeting the service objectives for the target-user community.

The value of the Content-Length entity-header indicates the size of the message body. This field should be populated with a decimal value greater than or equal to zero, whenever the size can be determined (e.g. Content-Length = 2342).

9.2 Site navigation

9.2.1 General

Navigation features shall enable information users to go to the following locations from every page in the site:

a) back: to return to the section/page most recently linked from;

b) next: next logical topic/page in the sequence of topics (if any);

c) previous: logical topic/page just prior to the one being viewed (if any);

d) home page or top-level menu;

e) table of contents (if any), list of topics, or keyword index (if any).

Navigation functions like "back" which are relevant to the user's location and path through the website are called contextual navigation. Navigation functions that are specific to the page being viewed, like

next and previous, are called local navigation. Global navigation features, applicable on all pages of the website, include home, search and index.

A URL pointing to a directory shall have a clearly identifiable page for further information, such as a default file (as set in a server) or a meaningful directory listing for the user community.

Navigation features guide users to information by indicating the locations to which users may move from their current location. Commonly used features for website navigation include links displayed in tabs, menus, page headers and footers; bookmarks; cross references; navigational icons; and buttons. The website designer should include labels or explanations of unusual, flexible, or complicated navigational features. For informational websites, the user should be able to click on text or a graphic without the website unexpectedly displaying different information.

The web page should display where the topic is in the hierarchy or where the current topic fits into the total structure (a breadcrumb trail or path of navigation links from the home page). This feature is particularly useful for users who have arrived at a page through an external link or search function, without going through the site's home page. A website that has multi-level menus should allow selection from choices in two levels of the menu, aiding comprehension of the information structure.

NOTE Users can access information more readily from a larger number of specific menu choices than from a small number of non-specific high-level pages.

The main navigation links should remain visible when the user scrolls through a long page, or readily accessible (such as by a "Top of Page" link on a long page). If an embedded active object is used, then it should have a description that can be read by accessibility-compliant readers.

Except for required statements of policies and terms of use, and login pages, the user should be able to navigate away from any page to another page in the site without entering data. The site may provide notices and require assent when the user is leaving the site and navigating to an external site where content is not controlled by the current site owners. The user should also be able to navigate away from the site without entering data.

The location and appearance of navigation aids on the various pages of an Intranet should be consistent. For example, the navigation aid to move the user to the site home page should always be located in the same page position as defined by the high-level design of the website. This also applies to the relative location and appearance of other navigation elements such as “Top of Page,” “last 25 items” or “next 25 items.”

Tables of contents or site maps should be provided for large sites to aid users seeking an overview of the contents.

Speed and ease of access to information on web pages should be improved by reducing the number of clicks on the information access paths.

The name of the default page for a directory access is defined in the server configuration. The default page can be named default.htm, index.html, or home.html, although disclosure of default page names can be a security risk. The primary navigation environment should be presented when the default name within a directory is used. The Redirect header tag can be used to manage navigation.

Site navigation patterns should be re-evaluated based on user access patterns, collected over time, or navigation graphs (charts showing links between pages).

The web pages should allow the user to log off at any point, rather than having to go back to the home page.

9.2.2 Links

9.2.2.1 General

Links between related topics shall be bidirectional, so that whichever topic the users access first, they can jump to the related information on the other topic.

Textual link anchors shall provide a clear indication of the destination of the link. Links to “under construction” or inactive pages should not be displayed to users.

EXAMPLE Rather than using "Click here", use "More troubleshooting tips" onscreen or in a mouse-over pop-up.

Links should provide information that the user expects in one jump, rather than requiring that the user follow one or more additional links to reach the required information.

Links should be easily recognizable by users, such as by underlining and color-coding. The style sheet should indicate that links should display in a different colour after they have been selected.

9.2.2.2 Absolute and relative links

Links within a website should be relative to the linking page, and not to the site root. Sites may wish to establish a reference point for relative references, e.g. a top-level directory, and use <BASE HREF= ... /> to establish the reference point. Use of the BASE tag can complicate site relocation. Links to external websites and site pages intended for external reference should provide persistent URIs. DOIs, as defined by the DOI Foundation, may be used as persistent URIs.

The class designation “duplicate link” should be used to designate additional navigational links which duplicate one on the page. One instance should not be designated a duplicate link. This allows style sheets to hide these redundant and distracting links from users (especially for aural presentation).

9.2.2.3 Links to protected websites

Links to protected websites and pages should indicate that the website is password-protected or requires a subscription or registration. This annotation may be color-coded for maximum effect, to alert the user to the restrictive nature of the website.

9.2.3 Offsite warning

To assure that the seamless nature of the web does not mislead the user about the source of the content, the website shall display clear notifications before a user navigates from a site to other sites. Users shall have the choice to accept or reject leaving the website. The website should provide users with an alternate way of locating the information, in case the external link has been broken or the destination removed. Security software should notify the user if the new site is suspect and provide appropriate cautions. Offsite links that download large files or videos should be clearly marked as such, including the file format and file size.

The notification may point out a change of security domains, or links that lead offsite may be tagged with “<a ...class="offsite">” as a method for creating a CSS controlled visual distinction. Depending on the situation, browsers may use this information to implement specific policies, such as managing the history information or cookies, blocking transfer, presenting the link with some warning icon, or presenting the user with some “leaving this site” warning.

As an alternative, “<... Class="onsite">” may be used to indicate links that are known to be appropriate for seamless transition. With the use of this approach, browsers should implement the “offsite” action for links that do not include this attribute.

9.2.4 Usage tracking and cookies

The project plan shall document the decision to use, or not use, cookies; and the implementation shall be consistent with this plan.

The use of cookies shall be described and the user given an option of receiving these cookies as an explicit action. Websites that use cookies, web beacons, or other technologies which collect information on customer usage shall have a privacy statement available from their home page or general information pages that explains their use of such technology. Websites shall disclose if usage of prior site information is collected and if information is shared with other organizations. If cookies are

required and the required cookies are not received, the site shall provide relevant feedback to the user as an error message (testing for this is not easily automated).

Additional information on security and privacy aspects of cookies is in 9.6.5.3.

It may be useful to use cookies to maintain state between page accesses. Tools can be used to verify that use of cookies is intended for a given site.

9.2.5 Frames

Frames shall identify the source and ownership of frame contents. Frame presentation of third-party content shall indicate the source and ownership of the content.

The _blank target, or other means of creating new windows, shall not interfere with the user's ability to return to their page history.

Various methods can be used to encapsulate graphics or other page elements on a page that are transparent to the user. If design includes the use of frames, then provision should be made for the user community to choose a no-frame implementation of the same content. This choice should be considered in the maintenance plan as well.

NOTE This design choice relates to requirement 22(j) of US 36 CFR 1194, commonly called Section 508 (www.section508.gov).

To avoid being "encapsulated", it is appropriate to include a <base target="_top" /> HEAD entry to force linked pages to acquire the full, original window. Scripting may be used to detect encapsulation and reloading the current content into the _top frame.

9.3 Search and indexing

9.3.1 General

Websites shall include an index or a list of keywords or topics of all pages relevant to the target audience. The site index shall be available in plain text format for accessibility. Websites with more than twenty static text pages, or with dynamic content, shall offer a keyword or full text search function.

A site may have more than one such index if there are distinct target audiences. Indexed information should be limited by user access privileges. Indexing in the html using sequential numbering of pages can result in easily guessed URLs and provide unexpected access to restricted information. This may require restricting access to the index or excluding restricted information from the index.

The developers of the website should implement measures with the goal of rejecting malicious queries that result in unauthorized bulk retrievals of the database or damage the site. SQL injection is an example of such malicious inquiries (see 9.6.4). Although full protection can never be guaranteed, robust actions can repel many common attacks.

NOTE See the ISO/IEC TR 24772 series.

The website shall display a response if no search results were identified for a query.

If the website displays results in preferential position, due to payments or sponsorship to the site owner or site provider, those sponsored results shall be labelled and visibly distinguished from other results, such as by text font or background shading.

If the search results contain references to an external website, such site references shall be clearly identified as being external to the website, such as by opening in a new tab or through a link to the external site.

The entry field for search should be sized to allow for display of a typical query. The search function may suggest corrected spellings for search data.

The search results should be presented in sufficient detail that the user can determine their relevance. The website should allow the user to sort search results in a useful way, such as by date, relevance, or alphabetically.

Users can become frustrated while waiting for retrieval of multiple pages of search results, rather than scrolling through an extended set of results retrieved all at once. Website designers should allow users to select how many results to retrieve when searching, within performance limits.

Website owners should consider the implications of referencing web pages beyond the maintained responsibility of the site. Such web pages vary in availability, size, style, consistency, accessibility, correctness, timeliness, human language, or other requirements of the managed site. A similar distinction is applicable to any pages indexed which are not managed web pages adhering to the site's guidelines. Contractual arrangements with the site provider may be applied to address requirements of the managed site. Maintenance of bibliographies of offsite references may also be appropriate.

Users can expect site index/search results to access internal content and not content from outside the site. If search engines are linking to external content, users should be warned that external references can link to non-relevant and non-secure content.

9.3.2 Search filtering

Faceted search and browsing by category may be offered when a large number of results are retrieved. Complex websites may offer an advanced search function that allows the user to further specify the search criteria or filter search results. The website should provide search options, such as contains the following words, exact match, spelling correction, or similar information.

9.3.3 Keywords

Web pages shall present keywords in priority or alphabetical order and without duplication.

EXAMPLE <meta name="keywords" content="keyword1, keyword2" />).

"Full text" searches usually exclude commonly used words (stop words), such as articles and prepositions. Unless a site offers full text search of its contents, search engines should include a limited number of keywords when indexing pages.

9.3.4 Metadata for indexing

Web pages shall incorporate appropriate metadata to provide for accurate cataloguing and indexing of pages for the environment in which the web pages are accessible. Web pages shall not provide duplicate data to search engines or indexing systems, other than divergent spellings or grammatical forms.

Header elements should include data needed for web page processing (link, style, script) or page indexing (title, meta/keywords, meta/description, PICS, and Dublin Core items.) Where more than four metatags are included, the use of link to profiles should be used. Links to style sheets and script files should also be used to facilitate reuse as well as off-loading network overhead.

NOTE 1 The Dublin Core DTD Metadata was developed by the library sciences community, and is applicable to general purpose web page indexing, see http://dublincore.org/specifications/.

NOTE 2 The DITA specification is specific to metadata tagging of topic-oriented information and document types.

NOTE 3 In some applications metadata can be recorded as part of the properties for the web page.

NOTE 4 The W3C PICS enables labels (metadata) to be associated with Internet content.

9.3.5 Flushing search engines

Search engines may store part or all of indexed pages. As a result, the previous content of a web page can be presented, even after a page has been updated, and incorrect or deleted material can continue

to be available. The use of the “description” metatag provides a level of control over what is presented. The information incorporated in the “description,” early in the web page creation should take this into account. Resubmission to search engines may facilitate replacement of these references.

Inclusion of sensitive data should be considered in this context. Efforts to eliminate data errors or expired pages may require replacement with other content at that URI and re-indexing of that content to flush out archival caches. Sensitive pages should use Cache-Control HTTP header to instruct browsers and proxies not to cache the page (e.g. Cache-Control: no-cache) associated with the content. Also, the page may include a metatag for cache-control (e.g. <meta http-equiv=”Cache-Control” content=”no-cache” />) associated within the content. Digital signature or fingerprinting of pages to assure content integrity can reduce risks of user modification of sensitive data; however, it is not possible to take action to assure the elimination of all copies of specific content.

9.4 Presentation of information

9.4.1 Presentation of text

Text presented on web pages should be legible. Placement, formatting, the font, background and text colour, and font size determine the legibility of the text on the website. The website design should support the use of common browser tools to enlarge text or shorten line lengths and page width. The web browser should provide scroll and zoom capabilities.

The use of topical headings, short sentences (fewer than 15 words), short paragraphs, and restricted vocabulary can support reading comprehension for text on websites. For legibility, fonts with simple letterforms, large x-height and large counters have a much more discernible shape. Extended text in ALL-CAPITAL letters, text type size outside the 9 to 12-point range, very short lines and very long lines all make text harder to read.

NOTE ISO/IEC/IEEE 26514 covers style and format for instructional and informative text.

Lack of contrast between text colour and background colour (such as dark blue or dark red text on black background, or white text on white background) results in illegible text which is still visible to automated searches and text readers. This practice is not recommended.

Where feasible, automatic population of repetitive user information is recommended to help avoid rekeying information and reduce potential errors.

The layout should be similar over different devices and operating systems, if feasible. If data is required to be entered, it should be easy to locate. For example, boxes that need to be checked should employ appropriate contrast to indicate the state. If the device supports cut and paste between applications, the web page should provide this capability to minimize the user having to rekey data.

9.4.2 Graphic images

Graphic elements shall contain declared height/width display size, permitting the immediate allocation of page layout for these and concurrent rendering.

For security purposes, firewalls and gateways can convert or block certain data types. Hence, the client does not receive the expected graphic.

The alt attribute shall be used to label a graphic and facilitate understanding of the content of graphics by persons who are not displaying graphics with their browsers. This also facilitates indexing.

The use of consistent style sheets can reduce page size and provide for reuse of style for subsequent pages. Reuse of images, as opposed to use of new images, can reduce download time by taking advantage of local caching.

Alt attribute descriptions should start with unique information, for example, “home button” rather than “button for home page,” and use functional descriptions where applicable. Longdesc can be used to provide detailed information about graphical content where it is warranted.

Multiple graphic images at the server should be considered, providing for lower bandwidth connections, or user choice. A potential convention is to have a thumbnail graphic delivered, which is also a link to a higher resolution graphic as an option for the user community. Caching can improve performance with attention to cache state management.

Software tools can improve performance and response time of graphic images in in low bandwidth networks by improving client and server-side processing. These tools in conjunction with caching can yield significant performance improvements.

Where a server can deliver images in multiple formats, image URIs should not include a specific format name structure, e.g. xxx.gif. To allow for content negotiation with users and to minimize overhead in response, a diverse set of image formats should be provided.

Images should not be used to bypass HTML limitations or provide “style” control. Where available, CSS should be used. If email addresses are presented in images, they should be presented in a form that is accessible as text, but discourages their harvesting by robots, for example, by spelling out "at" and "dot" and including spaces.

Graphic presentation rather than written text may be chosen for certain languages, cultures, or disciplines.

Images shall not be used to present text in an alternative style. This is disruptive to text-only browsers, it limits accessibility and global applicability, and it can have a negative impact on performance.

Sites should support common image formats such as JPEG, PNG, and GIF for compatibility, and seek to deliver the least overhead image acceptable to the client. For animated images, network motion graphics (NMG) should be supported. Scripting or client-side executable languages may be used as a more efficient means of providing the required functionality. Animated GIF images can display incorrectly or be deprecated in newer system environments and should be avoided.

To facilitate access by older browsers that do not support longdesc, the website designer may also provide an anchor link to that same data (longdesc takes a URI as its value).

9.4.3 Animations, 3D, sound, video

The user shall be able to control dynamic media objects (audio or video) by starting, pausing, restarting, and stopping them. The website shall indicate that selecting a link will launch audio or video content.

If presentation of dynamic media requires the use of specific client software, the website should provide information on the requisite media player and where it may be obtained or downloaded from a trusted source, such as one hosted and maintained by the supplier of the media player software.

Each animation, 3D, sound and video should have a description that can be read by accessibility-compliant readers (alt attribute).

Blinking or repeating animations are generally a distraction in the presentation of ICT information and should be avoided unless inherent in the information.

If media is being played with audio, consideration should be given to pause the media being played. Audio levels should be able to be adjusted including muting from the player in the browser where feasible versus using the main computer settings.

NOTE Animations that represent system processing or real-time event presentations can be uncontrollable by the user.

9.4.4 Use of colour in websites

The website shall not present information solely by the use of colour, unless no target users of the site can be colour-impaired.

Designers of web pages should avoid colour combinations that cause problems for individuals with colour impairment in its various forms. Designers of website should avoid using these colour pairs for background/foreground of text, or of any objects (e.g. links, borders or icons) which need to be differentiated by colour: red and black and bright shades of red and green, blue and orange, green and magenta, cyan and yellow, magenta and blue, yellow and orange, and green and blue.

Backgrounds should be lighter shades than text. The use of reverse combinations (e.g. white or yellow text on black or dark blue background) is less legible and should be avoided in extended text on informational websites. Reverse combinations may be used for banners or titles.

Check boxes and buttons should change colour with sufficient contrast to indicate that they have been selected. Greyed colour is often used to indicate website processing when an option cannot be selected.

NOTE Some development environments can check for colour contrast issues.

9.4.5 Time-sensitive content

Website design shall include a clear way to identify the areas changed without the need for navigating the whole site.

A web page shall include a page date as an RMfield (<pagedate>, or <. class="pagedate">). This indicates the most recent date when a change considered being of value to the target-user communities has occurred. Each web page shall include an expiration date as an Mfield or RMfield (<expirationdate>, or <…class="expirationdate">). This date indicates the earliest date that the page information may be deleted.

If time is included, the time zone shall be specified. Because local time in this context can be ambiguous, time-zone designators should be included (UTC or UTC-offset) when indicating the time.

Website design may segment information content by creation, expiration, or revision date and incorporate this into the overall website design. Some information has a limited useful life. Stock quotes, telephone directories, product specifications, organizational charters, and archival background information change at different rates. The nature of the information and the need of the user to have "current" or historical information affect the contents of web pages, as well as the methods used to deliver and annotate these pages.

EXAMPLE A website contains information on several versions of a software or hardware product, some of which are no longer actively maintained by the original manufacturer, but for which assistance is available from a wider user community. A website for a program contains specifications which were applicable at the time of when the contract was signed.

The segmentation should be at the page level. A policy for the expiration of the changed-pages list should be described. Date and time information may be displayed by default or on request.

The page information may be changed during this period, but the type of information presented on the page should remain constant or the user redirected to the new location of the information.

The expiration date serves several functions:

— a basis for automated deletion or archiving of the page;

— an indication that can be used by pages linking to this page of its expected life span

— a basis for exclusion of the page from indexing or search query processes.

The value "archival" may be used to indicate that the page contents are not expected to change; some form of persistent URI should be considered for archival pages where ongoing reference is expected.

Web pages should include applicable dates from this list:

a) date of creation, represented as an Mfield (<datecreated>, <… class="datecreated">), which is used to indicate when the content was created;

b) date of last modification, represented as an Mfield (<datemodified>, <... class="datemodified">). Changes in this date may occur without substantive changes in the content of the page (Mfield is suggested since this date is considered only to be of use in page management, but not for target-user communities);

c) content date, represented as an Mfield or RMfield (<contentdate>, <... class="contentdate">), which is used to indicate that the content was current as of this date; this does not always reflect changes in content from a previous content date;

d) date of next content review, represented as an Mfield or RMfield (<nextupdate>, <... class="nextupdate">), is used to indicate when a review is scheduled; substantive changes can occur prior to this date, and some form of user notification may be needed in certain business situations (see 6.2.4);

e) date of retirement, represented as an Mfield or RMfield (<dateretired>, <... class="date retired"> may be used to indicate when a page has been archived and is no longer considered active; organizations with requirements for archiving some or all information may want to include use of this date in their website project plan.

Content expiration or content review dates should reflect the expected rate of change for the content. Website maintenance tools should use these dates. These dates can be expected to be different from the cache expiration date. An automated notification should be sent to the content owner before or when content expires, so it can be updated in a timely manner.

When a user launches a website and receives notification that a newer version or update is available, unless the update is essential for security or operational reasons, the user should be given an option of when to apply it.

If the purpose of the above dates is for internal maintenance rather than use by the target-user community, it may be appropriate to maintain the information independently from the page content.

All dates should be presented with four-digit years.

Designers should use ISO 8601-1 as a reference. This document recommends the date format: YYYY-MM-DD (all digits) for dates. Where needed, dates may include time and time-zone, based upon UTC. HH:MM:SS should be 24-hour format if it has to be machine-readable.

ISO 8601-1 recommends the following time zone designation (TZD) format:

YYYY-MM-DDThh:mm:ssTZD

where:

YYYY is year

MM is month (01 to 12)

DD is day (01 to 31)

The letter “T” is required if time is specified

hh is hour (00 to 23)

mm is minute (00 to 59)

ss is second (00 to 59) (decimal fractional extensions may be incorporated)

TZD is the time-zone designator

the value should be “Z” for UTC

or +hh:mm for positive (east) displacement from UTC

or –hh:mm for negative (west) displacement from UTC

This format should be used in any machine-readable fields where date is included in the field. For date independent (time only) machine readable fields, the time subset should be used.

9.4.6 Printing from websites

Web pages consume energy for viewing as well as printing resources. The website owner should take into account organizational or industry green (eco-friendly) guidelines related to usage of colour, fonts and background for web page viewing and printing. Energy conservation should be part of the design criteria when the web content will be accessed from mobile devices operating on batteries. Environmental protection should be part of the design criteria when the web content will be printed. Colours, fonts and backgrounds that can save energy and printing should be considered.

To reduce printing to paper, web pages with printable content should provide an alternate way to render and output the content to an electronic postscript file or an email message.

Web pages that need to collect information from the users through forms should implement online fillable forms instead of printed forms.

When a web page print function is required, the website should provide a print-friendly version of the page, with streamlined content optimized for printing.

9.5 Accessibility

The target-user community evaluation shall take into account the likely existence (or future existence) of individuals who will need to access the information or services of the site and who are blind, deaf, or have limited sight, colour blindness, mobility impairments, audio impairments, or require other special considerations, as well as ergonomic requirements for general ease-of-access and ease-of-use for users. Typical changes for accessibility include the capability to zoom in or convert text to audio (text to speech).

Website design shall accommodate requirements for users to access content on small-screen or mobile devices or to print content. In view of the needs of search engines and differently abled users, the website shall provide a text equivalent or label for graphical, video, and audio content. Data entry can be supported by cut and paste. Geolocation can use context sensitive data or applications on the users' device, if the user provides permission.

Non-text media, such as graphical images, audio, or video, shall have alternative text descriptions.

The design process shall include consideration of conformance to the WCAG Level A, Level Double-A, or Level Triple A of the W3C WAI. See https://www.w3.org/WAI/WCAG2AA-Conformance.

Web page text to background luminance-contrast shall exceed 33 % (better than 67 % recommended). The web page text shall provide adequate contrast to be viewable over a wide range of lighting, from dim to bright sunny conditions.

Web pages shall not include flashing or blinking objects which have a blinking frequency or flicker rate greater than 2 Hz without consideration for photosensitive epilepsy impact.

NOTE 1 Frequency greater than 55 Hz is acceptable under US 36 CFR 1194.22(j).

Timeouts or refresh should be used with care to assure users have enough time to understand and interact with pages correctly. Where timeout is applied, a mechanism shall be provided to allow a user to indicate more time is required.

Forms shall use label and tab index designations to allow persons using assistive technology to access the fields and functionality required to complete and submit the forms.

Web pages shall use the TABINDEX attribute in conjunction with the A, BUTTON, INPUT, TEXTAREA, and OBJECT element and any input control where this provides a logical sequencing to access these elements.

Where a set of pages contain common initial links or duplicate links, TABINDEX shall be used to present unique links for this page first. To allow the user to avoid duplicate links, TABINDEX shall be used to present duplicates after all links have been sequenced once, and a 'refresh' link provided to reset the series without traversing the duplicates. For forms that have more than one logical section, for example, personal information, billing information, ship-to information, FIELDSET and LEGEND elements shall be used to identify these sections.

Form fields should have associated LABEL elements (affects TEXTAREA, SELECT, and INPUT fields of type TEXT, PASSWORD, CHECKBOX, email, number, date, RADIO, and FILE) or use Web Accessibility Initiative Accessible Rich Internet Application (WAI ARIA) techniques.

Repetitive navigation links should be assigned a TABINDEX value of zero (which should result in these being presented at the end of the tabbing sequence).

Web pages where the primary page content does not start immediately in the BODY element should define a DIV element with the attribute ID="content" to enclose the primary content in HTML4, or should use the <article> tag in HTML5. This facilitates access for users of restricted or special browsers, such as those used by the visually impaired.

The user should have the alternative of selecting a text-only page, without style sheets or frames.

The website should be accessible from different devices, such as mobile phones, tablets, or personal computers, at resolutions depending on target-user needs. Websites should have techniques to identify different platforms and, browsers and may have compatible versions for site access.

The World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG 2.1) identifies four principles of website accessibility as follows: perceivable, operable, understandable, and robust.

Web authors should apply parsers and validators to validate that specifications or parameters are set for content, CSS, and accessibility related details. Archived content should be periodically reviewed for usability with current standard tools and platforms.

Legal requirements for access vary by jurisdiction. Practical considerations may change as web-based information becomes either "mission critical" within an organization or displaces other forms of communication with target-user community individuals. Information about current guidelines and related initiatives from the W3C can be found at https://www.w3.org/WAI.

Use of the 216 "Web safe" colours is recommended. These colours are selected, in hexadecimal format, with RGB values that consist of any valid combination of 00, 33, 66, 99, CC or FF only. The intent is to improve legibility by avoiding light text on light backgrounds or dark text on dark backgrounds.

NOTE 2 IEC 61966-2-1 provides a specification of the sRBG colour space used in almost all websites.

Specification of all possible TABINDEX elements may be necessary to assure proper browser sequencing. Sequencing should be verified with target browsers.

Web pages should use the ACCESSKEY attribute with the BUTTON, INPUT, and TEXTAREA tags to initiate the related functions. ACCESSKEY should be considered for initiating link operations with the A and AREA tags as well. When specified, ACCESSKEY designators should be made visible to users and given a distinguishing style (which should be done with CSS class/style designations) to facilitate user awareness. ACCESSKEY designations should avoid overlap with browser and operating system defined shortcuts.

NOTE 3 Browsers and assistive technologies do not have a common set of shortcut key (accesskey) assignments.

Pages should use a common look and feel, including the location of a common set of navigation buttons. The first link on a page should be a link to the unique content of this page and be identified with alt text

such as ‘skip navigation’ or ‘skip to content'. This initial link may need to be a 1x1 pixel image that is not visible to users operating on a visual basis, but will be presented to individuals using audio or Braille output where avoiding the repeated information is important.

9.6 Website security

9.6.1 Overall security considerations

Control of website security needs to be an “end-to-end” process and cannot be bolted on as an afterthought. The overall design of a website encompasses the system architecture, security policy, security of the website code during development, operational security including monitoring and auditing, access control, and data security.

Website security is implemented through the system architecture, the code and software applications, the underlying operating system, the Internet or intranet as infrastructure, and machine-to-machine interfaces. Website security encompasses electronic appliances and other consumer products with a networking capability (Internet of Things), which can be monitored to retrieve information. Such networkable devices have a MAC address and get an IP address on a home or enterprise network environment, and so become subject to security vulnerabilities. Additional security issues can be created through the way the live environment is configured.

Network configurations are becoming more complex as website hosting is transitioned to the cloud or to hybrid configurations with cloud, virtual, and physical host configurations. A network can contain many different components from several vendors, including servers, authentication and authorization systems, load balancers, intrusion detection systems, firewalls, session border controllers, web application firewall and other systems. The detailed design of the network and the security of the Internet can be very complex and is outside the scope of this document.

For websites that have no requirement to communicate with external systems and users, micro-segmentation should be used to isolate their workloads and enhance their security.

For the protection of PII and other sensitive information as outlined in section 4.4 and other parts of this document the site operator shall use encryption for the website, the login, and the database.

Operational security depends on control of human access and data integrity. Each of these aspects should be thoroughly analysed, designed and implemented as well as continuously monitored and audited to help ensure the orderly and intended operation of the website and contribute to the overall management of risk.

NOTE Controls as defined in ISO/IEC 27001 can be used as guidance or requirements. Specific documented vulnerabilities that can affect websites are detailed in the CVE numbered vulnerabilities https://www.cvedetails.com/index.php. Common web vulnerabilities from design and coding are listed in the Open Web Application Security Project (OWASP) Top 10 https://owasp.org/www-project-top-ten. For off-the-shelf software, sites like CERT (https://www.sei.cmu.edu/about/divisions/cert) can be consulted, to help avoid publicly available zero-day exploits as well as to keep the software up-to-date with manufacturers' patches and updates.

9.6.2 Website security monitoring and measurement

Websites shall have monitoring, detection, and instrumentation to provide alerts for unauthorized or suspicious transactions. The external ingress and egress points shall be well defined with the ability to monitor incoming and outgoing traffic as well as devices on the network. This is especially relevant for remote access, such as virtual private networks (VPN) for remote workers and vendors.

A security information and event management (SIEM) framework should be utilized. The SIEM should provide the website provider with records of the activities within their IT environment as well as safe logging for unusual conditions, monitoring and alerting facilities.

Security metrics may include the following:

a) tracking the number of security incidents;

b) costs associated with resolving security incidents, including potential impacts to the reputation of the website owner and website provider;

c) mean time to discover a security incident;

d) mean time to resolve a security incident;

e) number of vulnerabilities discovered;

f) CVE score for each vulnerability computed using the CVSS (https://www.first.org/cvss);

g) mean time to address a vulnerability;

h) number of security patches;

i) mean time to patch;

j) total number of CIs;

k) number of CIs with approved change requests;

l) number of CIs where approved change requests were implemented during the period;

m) number of CIs where approved change requests were not implemented during the period;

n) number of CIs where, based on automated configuration audits, the version number of the CI differed between two successive audits.

9.6.3 Web page security designations

Security designations or characteristics shall be included on the page. These may use one of the following RDF standards:

a) RDF tags based on the Dublin core metadata initiative https://www.dublincore.org/specifications/dublin-core/dc-rdf;

b) the W3C standard RDFa Core 1.1 https://www.w3.org/TR/rdfa-core.

The exact wording of the designation varies in different organizations and can have legal implications (which vary by country). Typical security "banners" include:

— XYZ Corp. Confidential

— Internal Use Only

— Public Information

Declaration of security designation is insufficient to provide security control. Site design should include evaluation of passwords, encryption, and other techniques to provide additional security controls.

Pages without appropriate security designations can be implicitly public information (even though protected by copyright) or lacking in essential legal protections, depending on the legal jurisdictions from which they may be accessible.

Pages should avoid "welcome to" or any similar language, as that can be considered by some legal authorities as an open-ended invitation to attackers. Instead, the pages may have a narrative description about the business or the page in question.

Web pages should include similar banners in a way that is consistent with the associated community. Collaboration can permit sharing of confidential information, and such pages may carry corporate-specific banners; or collaboration can generate confidential information within the collaboration and have designations specific to that arrangement.

9.6.4 Security of the website code

An in-house software development process is continuous and should be secured throughout. Additional diligence throughout the code development helps ensure that the source code applications and APIs have not been compromised or tampered with.

Common vulnerabilities include SQL injection, cross site scripting (XSS), broken authentication and session management, insecure direct object references, cross site request forgery, security misconfiguration, insecure cryptographic storage, failure to restrict URL access, insufficient transport layer protection, and invalid redirects and forwards. The overall posture should address the latest threats that are identified from periodic testing, CVE updates and other trusted resources.

The functional correctness of the software should be tested against known errors, weaknesses and common vulnerabilities. Using repeated automated tests can catch vulnerabilities earlier in the process (see 6.4).

NOTE 1 IEEE Std 2675 provides additional advice on continuous testing during DevOps processes.

A software bill of materials (SBOM) that lists all of the software components being used in a website should be maintained for use in keeping software updated and in tracing the source of problems and vulnerabilities.

NOTE 2 The NTIA (National Telecommunication and Information Administration) Survey of Existing SBOM Formats and Standards provides more information on the SBOM.

https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf

Particular attention should be employed when using open-source software. Open source software is widely used in websites of all sizes and criticality. It can be more rigorously and widely tested than proprietary products. Selection of open source software from a source that is considered to be trusted is recommended. The website developers should take care to retest new functionality for its suitability and possible security vulnerabilities.

Many open source and cloud-based tools offer infrastructure as code (IaC) and vulnerability scanning capabilities, including the following:

— automated scanning of dependencies, system health and vulnerabilities:
  — code and container;
  — CVSS CVE;
  — computer security;
  — viruses;
— code reviews, audits and hardening;
— validation that code libraries are current;
— code signing at end of compile and validation of code on device to avoid code tampering;
— securing the code in a vault at the end of a compile;
— runtime protection.

9.6.5 Website access and authentication

9.6.5.1 General

Non-public information may be proprietary, sensitive, or classified information or PII. Users shall be required to identify themselves through an authentication process for all non-public information of the website. Stronger authentication should be used for sites that store PII associated with the users, financial or medical information, information for use in recovering from emergencies, or other confidential or sensitive information.

A zero-trust architecture (ZTA) should be adopted for all critical applications.

NOTE NIST Special Publication 800-207 addresses the framework for ZTA.

The home page, if it is accessible to the public, or the login page should clearly indicate if access to parts or the entire site is restricted and who to contact to request or reactivate access. Access to the website may be granted through automated procedures.

9.6.5.2 Authentication

Access should be granted through a policy decision point (PDP) and corresponding policy enforcement point (PEP). An intrusion detection system (IDS) and denial of service (DoS) detection and prevention system should be configured in front of the PEP.

Many technologies can be used for user authentication, including the following:

— password managers;

— password-less sign on;

— hardware tokens;

— software tokens;

— MFA (multi-factor authentication);

— OTP (one-time password),

— FIDO-2 (fast identity online);

— OAUTH (open authentication);

— PINs (personal identification number),

— digital IDs – users, devices, and computers;

— SSOs (single sign-on);

— challenge questions – do not use information that can be discovered on the Internet;

— AI based on user typical activities;

— biometrics;

— machine identity;

— validation using software applications.

The following are sample guidelines to produce stronger passwords.

a) User ID should be eight (8) characters or longer and should not be an email address as this is one half of the login information.

b) Passwords should be at least eight characters with at least one of each type of symbol. Stronger passwords should have sixteen or more characters, including at least two of each type of character:

   1) upper case symbols (A to Z);

   2) lower case symbols (a to z);

   3) numbers (0 to 9);

   4) special symbols (such as ?!#$%& or ~).

c) Passwords should be random in nature and not easily compromised. For example, an easily guessed password such as letters and numbers in sequence like ABC1234 should be rejected.

d) The application provider should scan the passwords on the dark web for possible compromise.

e) Phrases can be used, as well as a password manager to provide a more secure random password.

Designers should avoid the use of email addresses for user identification, and instead use a unique ID that is not easy to crack. SMS (short message service) messages are not suitable for secure MFA; however, the use of SMS messages provides additional protection over just using User ID and Passwords.

Digital signature and other fingerprinting mechanisms may be applied for page integrity and website authentication. These are separate processes which need to be distinguished as digital identity versus digitally signed documents.

In case there are a defined number of consecutive unsuccessful attempts, for example, greater than three, to login with incorrect credentials, access by the user shall be locked out for a defined interval. The account user shall be notified for each set of attempts from a suspicious device. Data on the unsuccessful login should be captured, including details on the device, location, number of attempts and time. This is in case the device or account has been taken over or compromised. Before the user accesses their account, they should be required to acknowledge this information.

For the user, an alternate backup “out-of-band” alternative notification should be available if feasible. Furthermore, if the user is notified to contact an organization, a verifiable trusted contact method such as a number on a previously received card or account statement should be available.

To avoid unnecessary inconvenience for a preauthorized user, the lock-out period may be overwritten if a subsequent attempt is made with the correct credentials and from an IP or machine ID from where the last successful login happened. Once a user is logged in, they should be notified to review their account activity as well as recovery and notification info. The user should be periodically prompted to see if there have been added data that are not the user's valid accounts. If there is significant inactivity in an application on a device, there should be a time limit set when it is disabled so it can’t be hijacked or compromised. The user can re-enable and log in when necessary. There should be additional security measures, e.g. security questions or image interpretation, for users who are logging in after a certain duration as defined in the security policy, e.g. 90 days, or using devices other than what they use normally. Website administrators should provide users advanced notice of the date by which their passwords need to be changed to avoid inactivation of their accounts.

Passwords should always be transmitted over secure transport and stored in one way hashed encrypted format. Recommended secure transport protocols are current versions of TLS or Datagram TLS (DTLS).

NOTE Use of SSL is deprecated but can be needed for integration with legacy applications.

Website developers should consider implementing single sign-on if use cases suggest scenarios where the user will have to access multiple independent but related systems to perform a specified task or set of tasks. The most recent supported protocols should be utilized where feasible.

In implementing single sign-on, developers should avoid exchanging hard-coded passwords between systems, as these can be easily discovered and used as a medium of attack.

9.6.5.3 Cookies for security and authentication

Cookies simplify functions such as user personalization and tracking and facilitate easier access to applications. The user should be allowed to opt-in to the use of cookies based on the privacy regulations in effect in the appropriate jurisdictions. The user should be informed, upon initial access to the site, what information is stored in the cookie, the consequences of opting out of using cookies, and how cookie information is used between sessions. Cookies should be set with an indicator to be deleted at the end of a session if not used for auto-login feature. Use of cookies between page accesses should only be done if the same page is accessed multiple times during a single session.

Cookies track whether a user is logged in and under what name. They also streamline login information, so users don't have to repeatedly enter site passwords. For further user account protection, cookies should be periodically released or have a maximum lifetime to request reauthentication.

Use of third-party cookies (from analytics, scripts, and images, or if the cookie includes any external content) can lead to inadvertent insertion of malware from the website logged onto. Use of third-party cookies is deprecated and shall require permission from the user. If the user is redirected and returns to the website, the user should be revalidated; and the website should not rely on cookies alone, as browsers and systems can be hijacked.

9.6.5.4 Authorization

Role-based access control (RBAC) and least privilege shall be applied and periodically reviewed to restrict who does modifications and deployments.

Once an end user is properly authenticated, a set of access rights to pages and data is associated with the user, according to the user profile or user role. User access rights should be granted according to the principle of least privilege, the minimum level to perform an authorized tasks and activities. User actions to change or remove the web page or its data, or to retrieve unauthorized content, should be logged and analysed. Log data is needed if inappropriate activity is detected, including attempts to move laterally in a network that the user is not authorized to access. As an escalation, alerts can be triggered to notify the relevant parties of the inappropriate activity.

All data input by a user shall be security checked (e.g. data within expected range) prior to initial use of that data.

Authorization should consider permitted access to each page of the site and the associated metadata, not just the home page. Role-based authorization should be used whenever certain classes of users are allowed access to certain pages or sections of the website.

If authorization information is retained between visits, the user should be advised on what information is retained, in what form (e.g. via the use of cookies), and for how long.

9.7 Data management

9.7.1 General

Data management is essential for websites providing technical information. It involves maintaining the integrity of the data, data encryption, data privacy, and protection of IPR.

9.7.2 Website information integrity

An organization shall take reasonable steps to determine that data on its website is reliable for its intended use, accurate, complete, and current.

When it is necessary to assure the material presented is original and has not been altered, e.g. when posting price data or other data that is secured for legal or business reasons, the data should be digitally signed; and this digital signature should be easily verifiable by the end user. Numerous types