

LEGAL UPDATE

Ethiopia's Critical Infrastructure Cybersecurity Framework: INSA Sets Out the Designation Standard

*Critical Infrastructure and Sectors
Designation Standard, Version 1.0
(August 2026)*



Hirko & Associates Law Office
Addis Ababa, Ethiopia



<https://hirkoandassociates.com/>



Ethiopia's Critical Infrastructure Cybersecurity Framework: INSA Sets Out the Designation Standard

Critical Infrastructure and Sectors Designation Standard, Version 1.0

I. From the Proclamation to the Designation Standard

Hirko & Associates Law Office previously published a legal update examining Ethiopia's Critical Infrastructure Cybersecurity Proclamation No. 1426/2026. That analysis considered the Proclamation's broader legal framework for protecting infrastructure whose disruption or compromise may have serious consequences for the country. The present update follows that discussion by examining the Critical Infrastructure and Sectors Designation Standard, Version 1.0, issued by the Information Network Security Administration (INSA) in August 2026 (the "Standard").

The distinction matters. A proclamation may establish the legal basis and institutional responsibilities for a regulatory framework, while a designation standard explains how the framework is intended to be applied in practice. The Standard provides a structured approach for identifying relevant sectors, assessing the criticality of infrastructure, assigning classifications, and reviewing designations over time. It therefore gives organizations a clearer basis on which to consider whether their activities, systems, facilities or services may fall within the critical infrastructure framework.

The Standard should not be read as declaring every organization operating in a listed sector to be critical infrastructure. Rather, it establishes a screening and assessment approach through which particular infrastructure may be evaluated according to its potential consequences for national security, continuity of essential services, public welfare and the wider economy. The practical question is not simply which industry an organization belongs to, but what the loss, disruption or compromise of its relevant infrastructure could mean for Ethiopia.

II. Which Sectors May Be Affected?

Part III of the Standard identifies sectors and domains that may be relevant to critical infrastructure designation. These include information and communications technology and telecommunications, financial services, energy, water and sanitation, transportation, healthcare, food and agriculture, and government services, alongside other domains that may be strategically significant or enable the operation of essential services. The Standard also recognizes the importance of infrastructure such as data centres, cloud services and national digital platforms where their functions or dependencies may have broader national implications.

The breadth of the listed sectors reflects the interdependent nature of modern infrastructure. A disruption affecting a digital service provider may have consequences

beyond that provider's direct customers. For example, interruption of a communications network, a data-hosting facility, a payment-related system or a platform used by public institutions may affect the ability of other organizations to provide services. Similarly, a failure in a physical utility may have consequences for digital systems that depend on reliable power, connectivity or water supply.

Sector eligibility is, however, only the starting point. The inclusion of a sector does not, by itself, establish that every entity within it will be designated. The Standard distinguishes between recognizing a sector as potentially relevant and determining whether specific infrastructure meets the applicable criticality threshold. This distinction is important for businesses that operate in a regulated or strategically important sector but whose individual operations may differ substantially in scale, function, substitutability and potential impact.

Organizations should therefore avoid treating sector lists as either an automatic designation or a guarantee of exclusion. The appropriate assessment will depend on the infrastructure concerned, the service it supports, the extent to which other services depend on it, and the likely consequences of a serious disruption. The Standard's approach requires attention to operational reality rather than reliance on an organization's name, business category or size alone.

III. Designation Is Based on Consequences, Not Labels

Part IV establishes a consequence-based assessment approach. The Standard directs attention to the potential effect of infrastructure failure or compromise, including implications for national security, the continuity of essential services, public and social welfare, interdependence with other infrastructure, and economic activity. These considerations place the assessment on the consequences of disruption rather than on a single technical characteristic or an organization's formal description.

This approach recognizes that criticality is contextual. A system may be technically sophisticated but have limited national consequences if it can be replaced quickly and safely. Conversely, a comparatively ordinary system may be highly consequential where public institutions, businesses or essential services depend on it and there are few practical alternatives. The assessment of interdependence is particularly significant because a disruption can spread through connected systems and produce effects beyond the infrastructure directly affected.

The Standard also contemplates consideration of risk, threats, vulnerabilities and existing controls as part of the assessment. This indicates that designation is not intended to be determined solely by the theoretical importance of an asset. The assessment framework also considers the environment in which the infrastructure operates and the factors that may affect the likelihood or consequences of disruption. The precise result will depend on the application of the Standard's methodology to the relevant facts.

The Standard sets out three designated categories based on the assessment score. Infrastructure scoring from 68 to 85, corresponding to 80–100 per cent, falls within Category I, described as Nationally Critical Infrastructure. Scores from 51 to 67, corresponding to 60–79 per cent, fall within Category II, described as Highly Critical Infrastructure. Scores from 34 to 50, corresponding to 40–59 per cent, fall within Category III, described as Significant Critical Infrastructure. Infrastructure scoring below 34, or below 40 per cent, is not designated under the stated thresholds.

These categories make the assessment framework more differentiated than a binary determination of whether infrastructure is critical or not. The classification indicates relative significance under the Standard's methodology. Organizations should not, however, infer from the category names alone that a particular set of obligations automatically applies in every case; the practical consequences must be understood in conjunction with the Proclamation, the Standard and any applicable directions or requirements issued by the competent authority.

IV. How the Designation Process Is Structured

The Standard describes a process that moves from identification and screening to detailed assessment, designation, registration and subsequent review. The stages indicate that designation is intended to follow a structured evaluation rather than arise solely from an organization's self-identification or a sector-wide assumption. Initial screening can identify infrastructure that warrants closer consideration, while detailed assessment provides the basis for determining its significance against the Standard's criteria.

For organizations that may be assessed, the process makes accurate information important. Relevant information may concern the services delivered, systems and facilities supporting those services, the number and nature of users or dependent organizations, the availability of alternatives, and the operational consequences of an interruption. The Standard's emphasis on dependencies also means that an organization may need to understand not only its own infrastructure but also its reliance on third-party providers and the extent to which other entities rely on its services.

The designation and registration stages also have practical significance for internal governance. Organizations should ensure that communications with the competent authorities are coordinated, that the information provided is consistent and supportable, and that responsibility for responding to assessment requests is assigned. Where different business units maintain separate records concerning technology, operations, risk, compliance and business continuity, an internal coordination process may be necessary to present an accurate picture of the infrastructure being assessed.

The Standard's process should not be interpreted as replacing any procedures, powers or legal requirements established by the Proclamation or other applicable instruments. Rather, it provides a designation methodology within the broader legal framework.

Where questions arise about the scope of an authority's request, the applicable deadline, the evidence required or the legal consequences of a proposed classification, the relevant provisions and any formal communication from the competent authority should be considered together.

V. Institutional Roles and Compliance Oversight

Parts II and VI address the roles of INSA, sector regulators, independent organizations and entities operating in regulated sectors. The framework therefore contemplates institutional coordination, particularly where an infrastructure operator is already subject to sector-specific supervision. For businesses in financial services, telecommunications, energy, healthcare or other regulated areas, the designation process may intersect with existing regulatory relationships and compliance obligations.

The Standard describes compliance monitoring mechanisms that may include self-assessments, reports, document reviews, on-site assessments, audits, inspections and technical evaluations. These mechanisms indicate that the framework is not limited to the initial act of designation. Monitoring may be used to evaluate whether relevant information remains accurate and whether an entity is responding appropriately to applicable requirements.

The Standard also contemplates corrective action or improvement plans and follow-up. This is significant because a designation assessment may identify areas requiring further attention, but the response should be grounded in the applicable legal requirements and any directions formally communicated by the competent authority. Organizations should maintain records of findings, assigned responsibilities, remediation steps and the status of follow-up actions, where such processes are applicable.

The existence of monitoring powers does not mean that every listed oversight measure will necessarily be used in every case. The Standard describes possible mechanisms within the framework; the selection and application of a particular measure will depend on the circumstances and the competent authority's assessment. Organizations should distinguish between a general description of the oversight framework and a specific request, finding or direction addressed to them.

VI. Designation Is Not a One-Time Determination

Part V provides for reassessment when material changes may affect an infrastructure's criticality. The examples identified in the Standard include mergers and acquisitions, changes in ownership, changes to services or systems, changes in dependencies, major incidents and changes in the threat environment. These triggers reflect the fact that the significance of infrastructure can change even where an organization's name or principal business remains the same.

A merger may consolidate services or increase the number of entities dependent on a system. A change in ownership or operating model may alter access, control or

continuity arrangements. A new service may become an important component of a wider ecosystem, while a change in third-party dependencies may create or reduce points of concentration. A major incident may also reveal vulnerabilities or operational dependencies that were not apparent during the original assessment. The Standard's approach allows these developments to be considered as part of an ongoing designation framework.

Periodic review intervals vary according to classification. The Standard provides for annual review of Category I infrastructure, review every two years for Category II, and review every three years for Category III, unless INSA determines otherwise. The intervals underline that designation is intended to remain responsive to changes in the infrastructure and its operating environment.

A review may result in reclassification, modification, suspension or de-designation, depending on the circumstances and the applicable process. Organizations should therefore avoid treating an earlier classification as permanent or assuming that a material operational change is irrelevant because no immediate incident has occurred. A disciplined change-management process should consider whether a proposed transaction, system migration, outsourcing arrangement, new service or major operational incident could affect the assumptions on which an assessment was based.

VII. What Organizations Should Consider Now

Although the Standard's application depends on the facts and the competent authority's process, potentially affected organizations can take reasonable preparatory steps. The first is to map the services and infrastructure that support essential or strategically significant functions. This should include identifying key systems, facilities, data assets, external providers and dependencies, as well as the services that would be disrupted if any of them became unavailable or compromised.

The second is to document the consequences of disruption in operational terms. A useful assessment should identify which services would stop or degrade, who would be affected, how long the organization could continue operating, whether a substitute is available, and what consequences could extend to other organizations or the public. These records should be evidence-based and periodically updated, rather than prepared only when a formal assessment is underway.

Third, organizations should review their governance arrangements. Management should know who is responsible for engagement with INSA and relevant sector regulators, who can provide accurate technical and operational information, and how legal, compliance, information-security, risk and business-continuity functions will coordinate. Where a group operates through multiple entities, it may be necessary to distinguish the systems and services of each entity while also documenting shared infrastructure and cross-entity dependencies.

Fourth, organizations should assess the quality of existing documentation concerning incident response, business continuity, recovery arrangements, third-party dependencies and significant system changes. This is not a claim that the Standard imposes a specific technical control in every circumstance; rather, these materials may help an organization explain its infrastructure, demonstrate how disruption would be managed, and respond accurately to assessment or monitoring requests.

Finally, organizations should establish a process for reconsidering potential designation implications when material changes occur. Transactions, new services, substantial changes in technology, significant incidents and changes in key providers should trigger an internal review where they may affect the criticality of infrastructure. This approach can reduce the risk that information supplied during an earlier assessment becomes incomplete or inaccurate as the organization evolves.

VIII. Legal and Commercial Significance

The Standard has potential implications beyond information technology departments. A designation assessment may require an organization to bring together legal, compliance, risk, operations, procurement, business continuity and technical teams. It may also prompt questions concerning the allocation of responsibilities between a service provider and its customers, the resilience of outsourced services, and the availability of alternatives if a critical provider becomes unavailable.

For boards and senior management, the principal governance issue is whether the organization understands the national and operational significance of the infrastructure on which its services depend. For legal and compliance teams, the task includes identifying the applicable framework, tracking formal communications from the competent authority, preserving relevant records and ensuring that internal decisions are supported by accurate information. For operational and technology teams, it includes understanding dependencies and being able to explain the consequences of interruption in a manner that can be assessed consistently.

The Standard may also be relevant to commercial planning. Organizations evaluating acquisitions, outsourcing, system migrations or new technology services should consider whether those decisions could alter the criticality of infrastructure or the dependencies associated with it. This does not mean that the Standard itself prohibits such transactions or activities. It means that material changes may affect the assessment and should be considered alongside the organization's other legal, regulatory and operational obligations.

A careful distinction should be maintained between being active in a potentially relevant sector and being formally designated. The former may make an organization relevant to screening; the latter depends on the designation process and applicable criteria. Likewise, the scoring thresholds provide a structured classification method, but the

consequences for a particular organization should not be assumed without examining the governing instruments and any formal designation or direction that applies.

IX. Conclusion

The Critical Infrastructure and Sectors Designation Standard, Version 1.0, develops the practical side of the framework established by the Critical Infrastructure Cybersecurity Proclamation No. 1426/2026. It identifies potentially relevant sectors, sets out a consequence-based assessment methodology, establishes differentiated categories, describes a designation process and provides for continuing review and compliance oversight.

For organizations operating in sectors that support essential services or nationally significant functions, the immediate priority is to understand the infrastructure they operate, the services that depend on it, and the consequences that could follow from a serious disruption. Organizations should also ensure that material changes are captured in their governance and risk processes. These steps do not presume that an organization has been designated; they help it prepare for a structured assessment and respond on an informed basis if the framework becomes applicable.

The Standard's practical effect will depend on how its methodology is applied to individual infrastructure and how it operates alongside the Proclamation and other applicable legal instruments. Organizations should therefore assess their position against the text of the Standard and any formal communications from INSA or the relevant sector regulator, rather than relying solely on general sector descriptions.

Disclaimer

This legal update is prepared by Hirko & Associates Law Office for general informational purposes only. It summarizes selected aspects of the Critical Infrastructure and Sectors Designation Standard, Version 1.0 (August 2026), and is not intended to constitute legal advice, a legal opinion on any particular organization, or a substitute for reviewing the complete Standard, the Critical Infrastructure Cybersecurity Proclamation No. 1426/2026 and other applicable laws, directives or official communications. The application and legal consequences of the framework may depend on the facts of a particular case and the position of the competent authorities.