topDNS Best Practice Series – Part II:

Applying the DTSP Safe Framework to Hosting, Registries, and Registrars: From Compliance to Operational Maturity

Webinar Readout – 4 February 2026

Introduction

As online safety laws expand globally, hosting providers, domain registries, and registrars are increasingly expected to respond to online safety issues in ways that are effective, proportionate, and legally defensible. Regulatory frameworks such as the EU Digital Services Act (DSA) establish important baseline obligations for hosting services, but they leave significant discretion in how organizations structure governance, enforcement, transparency, and continuous improvement – particularly at the infrastructure layer.

This webinar examined how DTSP's Safe Framework (ISO/IEC 25389, the first international standard for online safety) functions as a common industry reference for providing trust and safety without breaking the Internet. The Safe Framework provides a structured, role-aware approach to trust and safety that aligns with existing legal requirements while extending beyond them to support operational maturity, consistency, and accountability across jurisdictions.

Hosts and speakers

The webinar was hosted by:

- **Lars Steffen**, Head of Digital Infrastructures, Resilience & International, eco – Association of the Internet Industry
- **Thomas Rickert**, Director Names & Numbers, eco – Association of the Internet Industry

The two speakers were:

- **Farzaneh Badiei**, Head of Outreach and Engagement, Digital Trust & Safety Partnership (DTSP)
- **David Sullivan**, Executive Director, Digital Trust & Safety Partnership (DTSP)

Opening remarks

Lars Steffen opened by situating the webinar within topDNS's broader educational mission. He noted that topDNS publishes monthly abuse reports for the hosting industry – complementing the Netbeacon Institute's equivalent reports for registries and registrars – and that the initiative regularly engages with industry, including Nordic Domain Days, ICANN meetings, and CloudFest. He also flagged forthcoming topDNS events: a webinar on NIS2 directive implementation in the domain industry on 26 February, a post-ICANN meeting summary in March, and the Abuse Workshop at Nordic Domain Days in Stockholm on 26 May.

topDNS framed the session in the context of increasing regulatory and operational pressure on the Internet infrastructure ecosystem. Thomas Rickert highlighted that the EU Digital Services Act (DSA) has extra-territorial reach and introduces complex transparency reporting obligations that can be difficult to operationalize for different types of intermediaries. A recurring challenge is comparability: reporting should be meaningful across jurisdictions and intermediary roles, and should avoid asking organizations to provide information they cannot reasonably hold – for example, "content moderation" metrics for a registry operator, which has no access to hosted content.

DTSP and ISO/IEC 25389

Farzaneh Badiei introduced DTSP as a multi-stakeholder initiative launched in February 2021 to promote a safer and more trustworthy Internet through industry best practices, assessment methods, and standards. The approach is intentionally analogous to cybersecurity standards development, seeking to reduce fragmentation while supporting an open and global Internet.

David Sullivan provided a primer on international standards and described how the Safe Framework became an ISO/IEC standard via the Publicly Available Specification (PAS) process. The speakers emphasized that standards are widely used in regulation and procurement, and can help reduce regulatory fragmentation by offering a globally recognized reference point that regulators, procurers, and operators can align around. They also noted common barriers to standards adoption – principally cost and limited accessibility – and underscored that ISO/IEC 25389 is available at no cost because DTSP publishes it freely.

Assessment methodology: measuring maturity

DTSP pairs the best-practices framework with a maturity assessment methodology intended to evaluate people, process, and technology controls across five commitments: development, governance, enforcement, improvement, and transparency. The methodology includes a tailoring approach to select an assessment depth based on organizational size and scale as well as service impact and risk factors. The speakers presented this as guidance rather than a certification scheme, designed to help organizations prioritize improvements and demonstrate due diligence.

Relevance for hosting, registries, and registrars

Badiei and Sullivan highlighted the relevance of ISO/IEC 25389 for infrastructure providers across four core dimensions. First, its risk-based tailoring means the framework applies to different intermediary roles without requiring access to hosted content. Second, it supports regulatory alignment by covering compliance-oriented activities such as notice handling and transparency reporting while remaining jurisdiction-agnostic. Third, it assists with proportionality and due diligence, helping organizations document reasonable processes and resist pressure for overbroad actions that could disconnect legitimate users. Fourth, it provides a structured basis for benchmarking and internal alignment, offering a practical way to brief leadership and align teams on resourcing and operational priorities.

Q&A Highlights

Small providers and safety expectations

Lars Steffen relayed a question from Antelope Consulting, who asked whether end users of smaller providers deserve a similar level of safety regardless of the provider's size.

Sullivan argued the intent is proportional to capacity, not reduced responsibility: smaller organizations should still map practices to risks and governance, but may use lighter-weight assessments. Badiei added that right-sized benchmarks can incentivize smaller providers to adopt baseline transparency and process discipline rather than opting out due to resource constraints.

Relationship to ISO/IEC 27001 and ISO/IEC 42001

When asked about alignment with ISO/IEC 27001 (and potentially ISO/IEC 42001), Sullivan noted that DTSP deliberately published a guidance standard first, but is exploring how trust and safety practices could be attached to existing management system certifications. The discussion also recognized that information security threats and content/conduct risks are distinct but can blur in practice – as is well understood in DNS abuse contexts.

Vendor adoption and implementation support

Rickert asked whether threat intelligence providers and software vendors are incorporating the standard. DTSP explained that full membership is reserved for operators, but an Affiliate Membership tier is designed to enable broader engagement and access to implementation resources.

Key takeaways

The discussion underscored that trust and safety at the infrastructure layer cannot simply mirror content moderation models. Instead, it requires clearly defined roles, documented processes, risk-based prioritisation, and proportionate intervention mechanisms. ISO/IEC 25389 was presented as a structured method to achieve this balance while maintaining Internet interoperability.

Practical actions for participants

Participants were encouraged to map their existing abuse handling and transparency processes against the five commitments of the Safe Framework in order to identify gaps and prioritize improvements. Specific suggested steps included:

- Conduct a lightweight maturity self-assessment as a practical starting point to strengthen documentation, clarify escalation paths, and refine internal metrics.
- Adopt ISO/IEC 25389 terminology to support more structured, role-appropriate transparency reporting and improve internal data collection.

- Use the framework to brief senior leadership on trust and safety investment needs in a way that connects operational practice to internationally recognized standards.
- Contribute feedback to DTSP's forthcoming review and maintenance cycle, particularly to ensure that the needs of infrastructure intermediaries are adequately reflected.

Resources

- **DTSP Safe Framework and ISO/IEC 25389 (free access): https://dtspartnership.org/**
- **topDNS Initiative (webinars, abuse reports, events): https://topdns.eco.de/**
- **eco Association Names & Numbers: https://international.eco.de/topics/names-numbers/**
- **Netbeacon Institute (monthly abuse reports for registries and registrars): https://netbeacon.org/**