2024 Annual Report

SIDN For confidence online

2024 Contents

Loek Bakker, *CTO SIDN* Roelof Meijer, *CEO SIDN*

Global interconnection is the internet's strength

Foreword

The internet is a largely invisible network of more than 70,000 interlinked networks, which connects people all around the world. Thanks to the internet, we have unlimited scope for working together, plus access to a vast body of information and (vital) digital services, ranging from financial and government services to health care and education. We hope that the benefits of the internet and cooperation within our sector will continue despite the international conflicts and (geopolitical) tensions the world is experiencing. And we hope that we here in the Netherlands and people elsewhere will remain committed to that ideal as a counterpoint to the negative influences that drive people apart. So that global interconnection always remains the internet's strength.

Strategic decisions for a secure and stable .nl

A reliable Domain Name System (DNS) and domain registration system (DRS) for .nl are our top priority. They are central to our mission of promoting problem-free, opportunity-rich digital living for everyone. In 2024, much of our attention was focused on the new Hello Registry registration platform that we're developing from the existing Fury platform with our strategic partner CIRA. The main task that occupied us was preparing for the migration of .nl, .amsterdam, .politie and .aw to Hello Registry.

Another prominent feature of our year was the process that followed the announcement that we were proposing to partially migrate our registration system infrastructure to the public cloud service operated by Amazon Web Services (AWS) in Europe. The choice of AWS as cloud service provider gave rise to concerns regarding the Netherlands' digital autonomy. We well understand those concerns, because the debate regarding our nation's lack of digital autonomy is increasingly urgent and intense. Geopolitical developments and the situation described in the Draghi Report and Clingendael Report underscore the importance of increasing the strategic digital autonomy of both the Netherlands and Europe.

At the moment, however, no Dutch or European cloud service provider can fully satisfy either SIDN's technical and functional criteria, or our legal and organisational requirements. That was the conclusion of an analysis carried out for us by Eraneos in 2023. And backed up by a quick scan of the Dutch and European cloud services markets that the Ministry of Economic Affairs (EZ) commissioned last year. In 2024, we also arranged a Data Protection Impact Assessment (DPIA), and the General Intelligence and Security Service (AIVD) performed a risk analysis.

The findings of the 2 procedures confirmed that our decision-making process had been as thorough and rational as could be expected, and that we had put the reliability and availability of the .nl domain first. In early 2025, on the basis of the quick scan, the DPIA and the risk analysis, the government gave us the conditional green light to go ahead with a modified plan for migration of the .nl registration system to the AWS public cloud.

Having taken advice from the General Intelligence and Security Service (AIVD), we intend to implement a number of important measures to ensure that .nl's availability does not depend on AWS. Central to those safeguards is using a Dutch service provider to host the database for the zone file. That database serves as the primary, authoritative and trusted source for the generation, signing and publication of the zone file via a Dutch service provider without using AWS. The planned measures will reduce our dependence on AWS and safeguard our (digital) autonomy.

On the remainder of the migration pathway, we will be guided by the lessons learnt, and maintain close dialogue with our stakeholders. The .nl domain - and its domain registration system - will always be operated by us and tied to the Netherlands, ensuring the constant availability of .nl and the security of our data.

› Read more about our choice to use the public cloud, the government's stance and the DPIA.

The .nl domain will always be operated by us and tied to the Netherlands.

Collaborating across borders and boundaries

It's vital that we keep working together on the basis of trust, knowledge and understanding towards shared objectives. From fighting internet abuse to safeguarding the vital digital infrastructure. The current international landscape and the political and public interest in our services emphasise the societal importance of our resilience and a strong .nl ecosystem. As well as the importance of an internet that is open, secure and accessible to everyone, everywhere.

Our colleagues at SIDN Labs therefore work with universities, research centres and other partners on applied technical research aimed at improving the internet infrastructure. In the Netherlands and beyond. And, over the last 10 years, through SIDN Fund, we've supported more than 400 innovative projects that contribute to a strong internet for all.

We also participate in various international associations, including CENTR, DNS-OARC, IETF and ICANN. In addition, we sponsor or give expert assistance to organisations that campaign for a stronger and more secure internet, such as the Internet Security Platform. In the interest of an open and secure digital future for all, we provided input

Over the last 10 years, SIDN Fund has supported more than 400 projects.

through the Ministry of Economic Affairs to the UN Global Digital Compact, formally adopted by world leaders in September 2024. The Compact is to serve as a route map for global collaboration amongst member states and other actors with a view to utilising the opportunities provided by technology and bridging the digital divide.

Developments in the domain name market

Developments in the Dutch and global domain name markets also commanded a lot of our attention in 2024. With a market share of 61 per cent in 2024, .nl leads the Dutch market. Next comes .com, which has a 26 per cent share. After modest growth in the early part of 2024, .nl experienced 3 successive quarters of contraction for the first time in its history. By the end of the year, there were almost 6.2 million .nl domain names. A considerable proportion of those names are not yet, or are no longer, in active use. We're therefore working with the .nl registrars to reinforce the brand preference for .nl, and to promote the active use of domain names. After all, .nl is the domain of and for the Netherlands, and one of the most secure in the world.

Indeed, stagnation and contraction are evident throughout the domain name industry. Of the gTLDs introduced since 2013, only a few hundred have secured modest international success, and none are widely used in the Netherlands. We don't expect the new application window that ICANN is planning for 2026 and beyond to bring significant change, because the market is very different from what it was a few years ago. Increasing use of artificial intelligence (AI) in the form of ChatGPT, Microsoft Copilot and DeepSeek means less reliance on traditional search engines. While it's not clear whether that's depressing demand for domain names, it is the case that domain names are less visible in AI-driven search results. Meanwhile, investment in Web3.0 TLDs (blockchain domains) began declining in 2024 from the peak seen a few years ago. Web3.0 TLDs are increasingly seeking integration with traditional DNS TLDs. We're therefore inclined to see that development as more of an opportunity than a threat.

Outlook for 2025

A stable, constantly available and secure .nl remains our top priority. In 2025, we'll therefore go on working to make the infrastructure that supports .nl even more resilient. We'll also continue preparing for the partial migration of our technical infrastructure to the cloud. The preparations will be informed by the lessons already learnt, and we'll engage with the government, the Registrars' Association (RA) and other stakeholders.

A unified SIDN-CIRA team will take forward development of the new Hello Registry registration platform, and we'll continue preparing for its adoption. Encouraging the active use of .nl domain names and discouraging cancellations will remain important focuses. As will tackling abuse in the .nl zone, for which we plan to establish an anti-abuse working group with registrars in 2025. Security will remain top of mind, and we certainly won't confine ourselves to compliance with ISO 27001:2022, NIS2 and the like.

In 2025, we will once again draw motivation and strength from collaboration on communal and societal values. The important work of SIDN Labs and SIDN Fund will continue, and we'll invest further in an inspiring and sustainable working environment that promotes collaboration, personal development and knowledge-sharing. So that SIDN's highly committed workforce can go on excelling in their pursuit of a secure, stable and globally prominent .nl, and an open network of networks that connects people all around the globe.

This annual report describes how we work with our partners for a secure, stable, resilient and autonomous .nl. We hope you enjoy reading about the highlights of our year, what we learnt in 2024, and what we're planning for 2025.

Roelof Meijer, *CEO*
Loek Bakker, *CTO*

Our key figures

6,169,270

More than 6.1 million .nl domain names (on 31 Dec 2024)

We work with more than 1,100 .nl registrars

I ♥ .nl
39 year

The .nl domain is 39 years old

We have a team of 99 personnel

1996

SIDN has operated .nl for 29 years

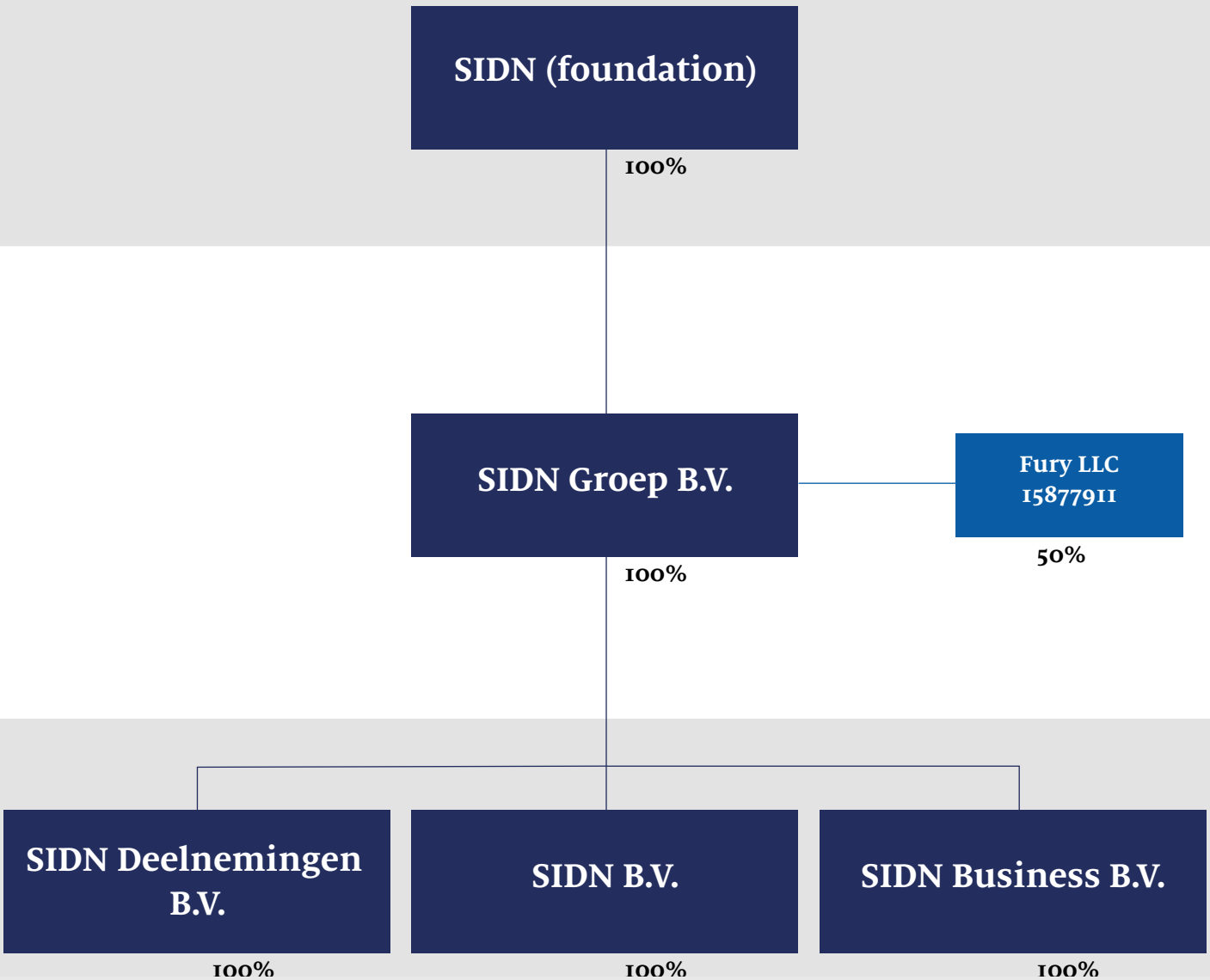
Over 60 per cent of .nl domains are DNSSEC-enabled

Problem-free, opportunity-rich digital living for everyone

1 About SIDN

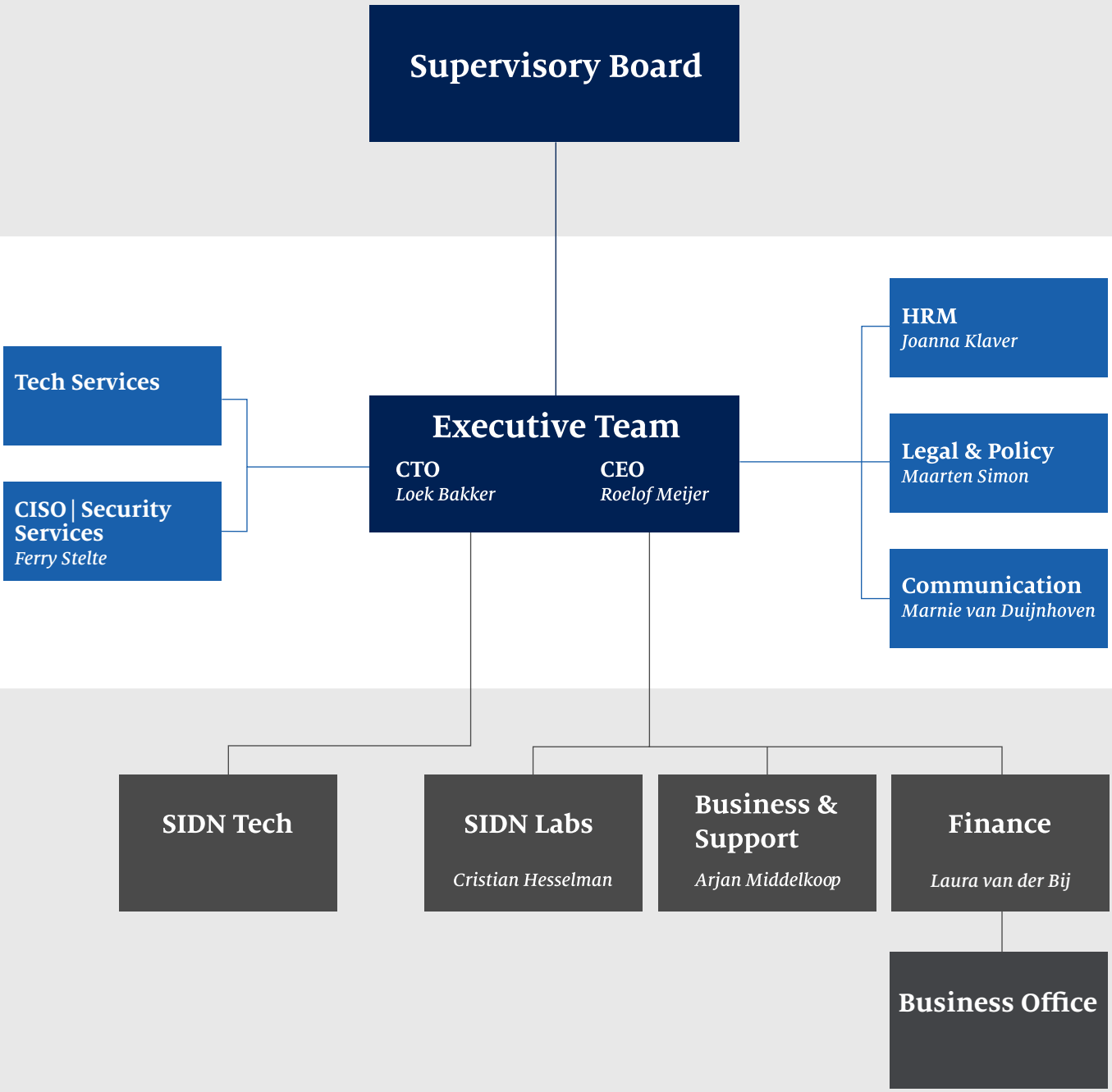
As manager of the .nl top-level domain, SIDN operates at the heart of the internet, in the Netherlands and for the Netherlands. It's a source of great pride for us that .nl is one of the world's largest and most secure country-code domains. However, we are active in many other fields as well. We share our knowledge, develop cybersecurity services and support initiatives that help to make the internet better and stronger. Our mission is therefore to promote problem-free, opportunity-rich digital living for everyone.

Legal structure



A legal separation exists between the delegation of the .nl domain (i.e. the right to run the domain), and the domain's operation (its day-to-day running and related activities). The delegation is held by the original foundation, SIDN, while .nl's operation has been transferred to a private limited company formed in 2023, called SIDN B.V. The original foundation is the sole (indirect) shareholder in SIDN BV. The separation was created in order to spread the business risks that our operations involve as widely as possible. We see that as the best way to safeguard the continuity of the .nl domain.

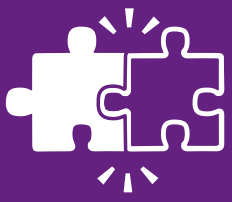
Organizational chart



Our themes and priorities

A globally prominent .nl domain

Putting internet users centre stage



Turning problems into opportunities

Contributing to a future-proof internet

Collaboration

Our value to the internet community

2 Our strategy for a secure internet

Our central role in the Domain Name System (DNS) implies great responsibility towards all Dutch internet users. Ever since we started running the .nl domain, security and reliability have been our top priorities. Our strategy is the means by which we translate our goal of problem-free, opportunity-rich digital living for everyone into practical action. It has 5 central themes, each linked to priorities, activities and strategic choices aligned with our role and responsibilities for the Netherlands and the wider world. Further details are provided below.

A globally prominent .nl domain

In the Netherlands, .nl is by far the most popular domain. It also plays a leading role on the global stage. The quality, security and reliability of our core systems (the DNS and DRS) and .nl services are therefore top priorities, and the starting point for defining our agenda. We uphold the security of .nl by actively fighting internet abuse, constantly innovating and using data-driven working methods. We also work with the best people and the latest proven (cloud) technology. Together, we work to ensure that .nl domain names are easily and widely accessible for everyone.

› For details, see section 3 and section 6.

Putting internet users centre stage

SIDN is a private organisation with a public role. We work for the internet user in partnership with registrars, service providers, public bodies and other members of the internet community. We work with the internet community to produce and share research findings, open-source software, data and open standards, and to promote the adoption of such standards. And in the field of user autonomy, we advance the principles of privacy and security by design, open-sourcing and decentralisation.

› For details, see section 3, section 4 and section 5.

Turning problems into opportunities

We are constantly striving to increase the security of internet users and to promote optimal, responsible internet use. That includes working to resolve problems in the field of internet infrastructure and cybersecurity. We seek to generate a responsible surplus, so that we can help the Netherlands and the wider world to innovate, and so that we can invest in problem-free, opportunity-rich digital living. We also bring research and practice together to realise new solutions for Dutch consumers and organisations, for the internet community, and for our own use.

› For details, see section 3 and section 4.

Contributing to a future-proof internet

We work tirelessly to help improve the security and resilience of the existing internet infrastructure and the infrastructure of the future. Our work in that field involves applying our own research results, supporting projects and developing new services. And, by doing so, we contribute to a fair, inclusive and sustainable digital society.

› For details, see section 4.

Collaboration

At SIDN, we work as a single team. Because we can achieve more together than alone, we pursue expertise and technology partnerships with actors in the Netherlands, other European countries and beyond. We work with partners whose values align with our own and who share our commitment to problem-free, opportunity-rich digital living.

› For details, see section 5 and section 6.

Strategy Consultation Group

We have a Strategy Consultation Group, enabling us to maintain a continuous strategic dialogue with people representative of our stakeholder groups. The Strategy Consultation Group includes people from government ministries, universities, internet industry players (including registrars), community groups and lobby groups. At our meetings with the consultation group, we seek input for and feedback on our strategy, which are then used to inform subsequent strategic decision-making. We attach particular importance to obtaining insight into – and promoting the clarification and discussion of – the interests of our various stakeholder groups.

As in previous years, we organised 2 Strategy Consultation Group meetings last year. The meeting in June was devoted mainly to the lessons learnt from the debate surrounding our proposed migration to the AWS public cloud. Other topics covered were our plan of working with Canadian partner CIRA to make the new registration platform available to other ccTLDs once it has been successfully rolled out for .nl. The November meeting focused primarily on the prevention of abuse in the .nl zone. The risks associated with phishing and fake webshops, and the efforts being made to stamp them out, were among the matters discussed. We know from Strategy Consultation Group feedback on the meetings and the group's composition that there is a desire to explore relevant issues in greater depth. From 2025, we will therefore make more time available for the meetings.

Photo: ANP / Sandra Uittenbogaart

Our top priority is a secure and stable .nl

3 A globally prominent .nl domain

One of the many fields in which we are a global leader is tackling internet abuse within the .nl zone. We work in partnership with organisations such as the police in order to maximise our impact. Using our RegCheck system, we're able to identify suspect domain name registrations very early. And we help organisations protect their brands with our SIDN BrandGuard service. We also work to reinforce .nl by the promoting the active use of .nl domain names – through our incentive scheme for registrars, for example. In 2024, we extended and broadened our collaboration with the Registrars' Association (RA).

Tackling internet abuse

As operator of the .nl domain, we constantly work to make the zone even more secure. Fighting abusive and criminal activities within the domain is one of our core activities. There is an ongoing need for such work, because cybercriminals are continually coming up with new ploys. We therefore investigate malpractices involving domain names, and we work with .nl registrars, universities and other actors, such as the NCSC.

We also use a system called RegCheck, which can automatically identify suspect domain name registrations at an early stage. Developed by SIDN Labs, RegCheck assigns risk scores to new registrations. The ability to identify malicious registrations as soon as possible and intervene promptly is very important because scams often claim most of their victims in the first 24 hours. If a registration is flagged up as suspicious, we ask the registrant for proof of identity, after which they have 3 days to respond. The approach helps us to nip many abuses in the bud.

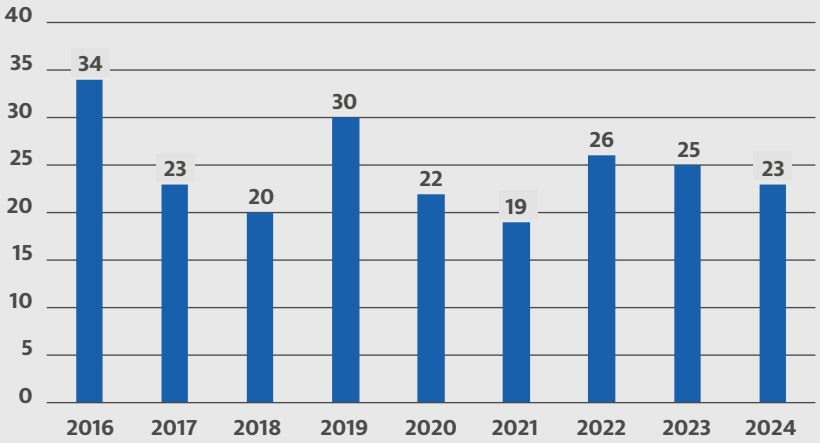
As well as working to detect suspect registrations, we seek to stop .nl domain names being abused for internet-based criminal activities, such as phishing, malware and fake webshops. Whenever we discover that a .nl domain name is associated with phishing or malware, we send a detailed report to the registrant, the registrar and the hosting service provider. That gives them the opportunity to resolve the issue and prevent further attacks. In 2024, our reports led to registrars taking down more than 60 per cent of phishing sites and malware distribution sites within 24 hours. In about 400 cases, we intervened ourselves by making the domain name and thus the associated website unreachable. And in November, we disabled roughly 125 domain names registered by a malicious actor. Action like that is taken only after detailed investigation of the individual case.

In the fight against fake webshops, we work closely with the Netherlands Consumer Authority (ACM), the police and other partners. At the end of November 2024, we announced that we were linking up with the Police National Internet Fraud Desk (LMIO) to improve the way internet fraud is tackled. Whenever detailed investigation leads the LMIO to identify a site as a fake webshop, they inform us straight away. We then immediately disable the malicious site without further investigation of our own, and we tell the registrant what we've done. The policy minimises the time window that fraudsters have to operate and gives consumers better protection. The importance of the initiative is underscored by police data, which shows that the number of webshop fraud reports rose from 16,000 in 2023 to 20,000 in 2024. As well as intervening when abuse is suspected, we sometimes have to act in response to court proceedings. That can be the case if, for example, a registration infringes someone's copyright or their right to a trading name. In circumstances like that, we may need to cancel a .nl domain name's registration. We aim to be open and transparent about our intervention activities, because they can have major consequences for the parties involved. We therefore publish quarterly Transparency Reports on our website.

› Read our Transparency Report on sidn.nl

In collaboration with the Platform for Internet Standards, we promote the use of modern, open internet standards: internationally agreed quality and security requirements that data exchanges between ICT systems must meet. The implementation of such standards helps to make the internet secure, stable and accessible. We therefore promote their use through our Registrar Scorecard (RSC) scheme, and we are a partner in Internet.nl, a joint initiative by various internet industry players and the Dutch government. Our collective efforts are helping to drive up the use of secure modern internet standards. In addition, we

Fig. 1 | Average up-time of phishing sites and websites with malware, in hours



support internet users with security-related publications, we share our knowledge through the SIDN Academy, SIDN TechTalk, webinars and practical guides, and on our website we publish answers to frequently asked questions about the standards.

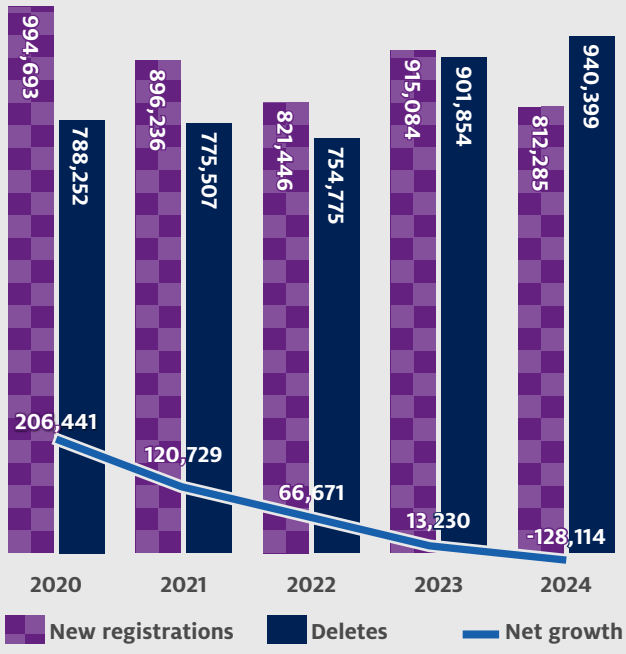
> Read more about modern internet standards on sidn.nl

We use the RSC to promote the use of modern, open internet standards.

Development of the .nl domain and domain name market

In January 2024, the .nl domain grew slightly, after which the Dutch domain name market stabilised. From February to September, there was a modest contraction of 1.7 per cent, and the zone contracted again in December. By the end of 2024, there were almost 6.2 million .nl domain names, down from 6,297,384 at the start of the year. In absolute terms, the .nl domain therefore remained one of the 5 biggest country-code domains in the world (source: Verisign, 2024).
Drivers of .nl's contraction in 2024 included an increase in cancellations at the end of the first year of a domain name's registration, which many registrars offer at a discount rate. In addition, new registrations fell by 10 per cent, probably due to a decline of 8 per cent in the number of business start-ups and a 15 per cent rise in the number of business closures (source: Chamber of Commerce, 2024). However, the size of the .nl domain is influenced by non-domestic factors as well.

Fig. 2 | Development of the .nl domain



International developments affect .nl along with other ccTLDs and gTLDs. Potentially relevant factors identified by CENTR included the cancellation of domain names registered for short-term purposes and the rise in ccTLDs' renewal fees (source: CENTR, 2024). Stagnation and contraction were evident throughout the domain name market. The domains that experienced contraction included .eu and most generic top-level domains (gTLDs), such as .online and .top.

However, demand for .com domain names continued rising on the Dutch market all year. Growth was strongest in the months prior to the .com's 7 per cent price rise in September, but the domain continued growing in the Netherlands at a more modest rate after that. In the first 3 quarters, .com grew by 7.5 per cent in the Netherlands, despite contracting at the global level by 2.2 per cent year-on-year.

A further factor that we have been monitoring is the effect of artificial intelligence (AI) on the domain name market. We commissioned market research bureau GfK to look at how AI is influencing the use of .nl domain names. It's increasingly common, for example, for people to ask AI systems such as ChatGPT and other AI chatbots for information that they would previously have looked for on websites. We therefore wanted to know what the implications might be for the size of the .nl domain. What GfK found was that it's mainly older ChatGPT users who are visiting fewer websites.

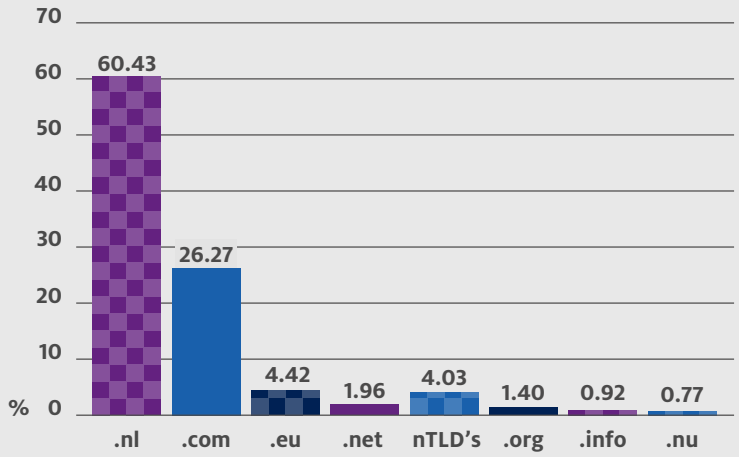
Market share

The .nl extension has a prominent position on the Dutch market. Particularly amongst people with their own businesses, .nl is the preferred option. Nevertheless, .nl's market share fell slightly from 62 per cent in 2023 to 61 per cent in 2024. Meanwhile, .com's share of the Dutch market went up from 23 per cent to 25 per cent at the close of 2024.

Covenant with Ministry of Economic Affairs

Since 2008, we have had a covenant with the Ministry of Economic Affairs (EZ). In the covenant, we and EZ agree to work together to assure the continuity and stability of the .nl domain. We also undertake to maintain .nl's ties with the Netherlands and to keep SIDN based in the country. In connection

Fig. 3 | Market share in 2024

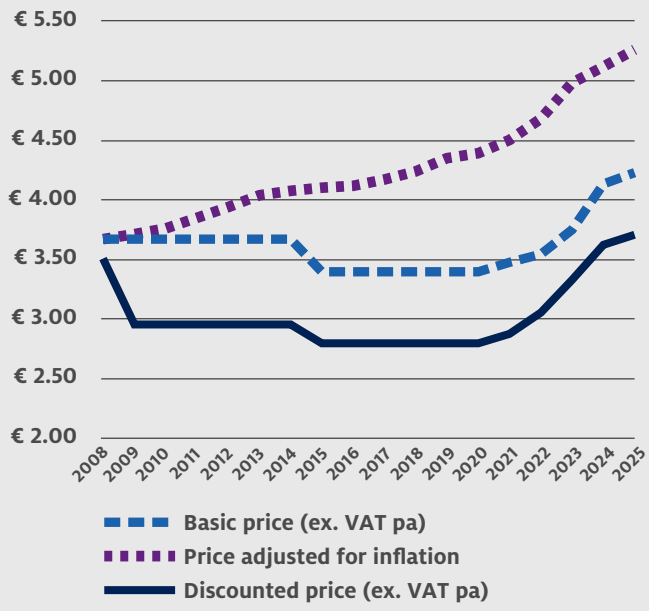


with the covenant, we held regular discussions with the ministry in 2024. The proposed (partial) migration of our registration system to the public cloud and the research carried out in connection with the move were the main topics addressed.

Supervision by the Dutch Authority for Digital Infrastructure

In 2018, the Network and Information Systems Security Act (Wbni) took effect in the Netherlands. The Act is intended to boost the digital resilience of the Netherlands, mitigate the impact of cyber-incidents and prevent disruption to society. Under the Wbni, SIDN was designated an 'operator of essential services' (OES): an organisation that provides services that are vitally important to Dutch society. As an OES, we are subject to supervision by the Dutch Authority for Digital Infrastructure (RDI),

Fig. 4 | .nl price change over time (euros)



and we have a duty to manage the security risks to our network and information systems and safeguard against incidents. We are also required to report any incidents that have major implications for service stability. No such incidents occurred in 2024. We nevertheless informed the RDI about the data breach caused by maintenance to sidn.nl and about our plans to (partially) migrate our registration system to the public cloud.

Cooperation with the RA

The Registrars' Association (RA) engages in dialogue with SIDN on behalf of .nl registrars. The RA gives us advice, both when we ask and on its own initiative, on governance matters, technology, marketing and legal issues. With regard to the proposed migration of our registration system to the public cloud, we accept that we were slow to engage with the RA and didn't initially involve them closely enough.

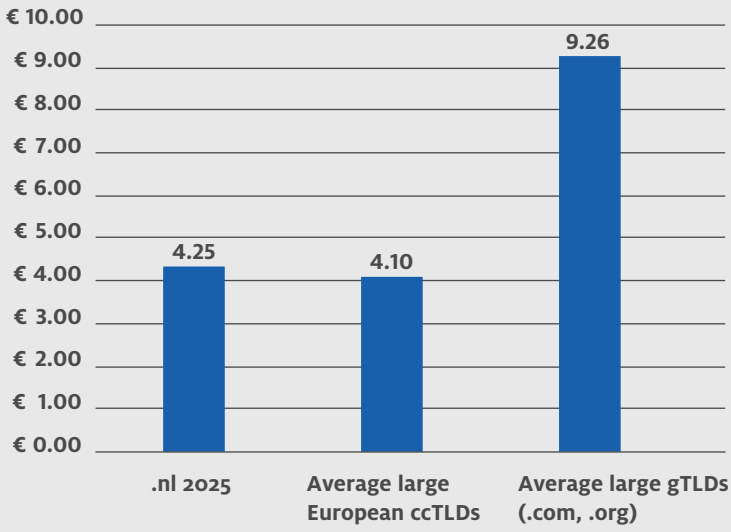
Since 2024, we have therefore been consulting the RA more and at an earlier stage about important decisions and activities. That's been the case with further planning of our public cloud use and the exit strategies, for example. We've also worked closely with the RA's Marketing & Communications Committee and Technical Committee, and we've set up a working group to get registrars' input on migration to the new registration system and communication on the migration process. We've also discussed working together more closely on tackling abuse in the .nl zone. At the end of 2024, we extended our cooperation agreement with the RA for 2025.

We intensified our collaboration with the RA.

Price adjustment

At the start of 2024, we increased our registry fees by 10 per cent. We made the adjustment to assure the long-term health and stability of the .nl domain. Our costs are rising considerably, due to high inflation, the need for ICT investment and a tight labour market. At the same time, we are seeing little or no autonomous growth in our income from .nl domain names. We also need to build up a reserve to cover the cost of essential investment in our ICT environment and modernisation of the Domain Registration System. That will enable us to avoid major fluctuations in the amount we adjust our pri-

Fig. 5 | Price levels of .nl and peers (excl. discounts and registrar fees, euros)



ces later. In 2024, the basic annual cost of a .nl domain name was €4.15 (excluding discounts and incentives). The registrar's account fee was €83 a month.

Developments in the registrar community

In 2024, the total number of .nl registrars increased from 1,079 to 1,114. However, the new accounts are not generating growth in the .nl zone, because they have been created mainly to enable registrars to look up additional data for commercial purposes. There was little movement at the top of the channel: at the end of 2024, the 25 biggest registrars were responsible for 83 per cent of all .nl domain names. That is very slightly up on the end of 2023 (82 per cent). It was noticeable that more registrars are actively seeking to prolong registrations, for example by promoting renewal at the end of the first year and making renewal easier. That trend was apparent both in the Netherlands and elsewhere.

Registrar satisfaction remains high

In 2024, registrars gave our services an average rating of 7.8 out of 10: slightly down on the 8.1 they gave in 2023. The main and most often cited reasons were the need for our systems to be updated, and the rate of progress. Those are exactly the issues that we focused on in 2024 and will focus on in 2025. 2024 was dominated by preparations for migration

We supported 7 registrar campaigns aimed at strengthening .nl's position.

to the new registration system, but registrars will not benefit from that work until early 2026. The 10 per cent price increase that we were obliged to make also affected satisfaction. Registrars were nevertheless positive about our services and personal contact with our staff, with the Support Department getting an average mark of well over 8.

Co-funded marketing

In partnership with our registrars, we work to reinforce .nl's position in the Netherlands and promote its use. One way we do that is by helping registrars to raise .nl's profile and encourage the renewal of .nl registrations. Throughout the year, registrars can apply to us for marketing support. We also reach out to registrars proactively to offer assistance, particularly in the form of funding, data and expertise.

In 2024, we supported a total of 7 registrar marketing campaigns, which yielded about 20,000 extra .nl registrations. Using our data platform SIDN Insights and other vehicles, we also supported initiatives and campaigns by registrars and resellers aimed at making the .nl zone stronger. Another way we help is by making 5 marketing toolkits available to registrars. The kits include ready-to-use promotional material.

SIDN Academy

We operate an online platform called the SIDN Academy, where .nl registrars can brush up on topics relevant to a secure and stable .nl domain. We published microlearning modules about the e-mail security standards StartTLS and DANE and

Fig. 6 | Development in customer satisfaction

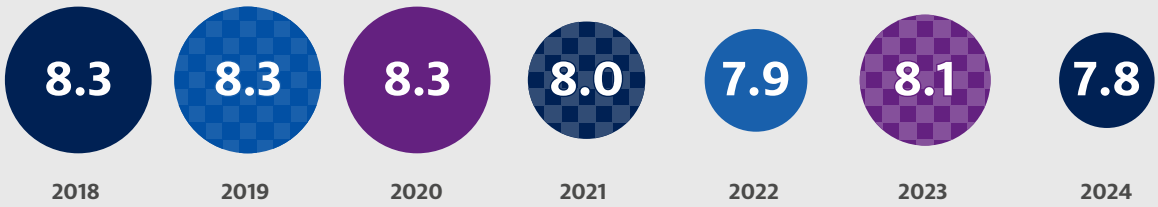


Fig. 7 | Development in the number of DNSSEC-enabled domain names (x 1,000)

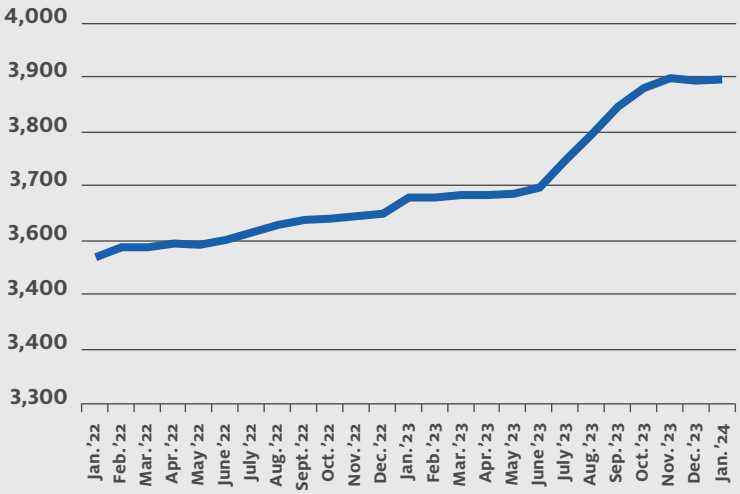


Fig. 8 | IPv6-enabled domain names (€m)

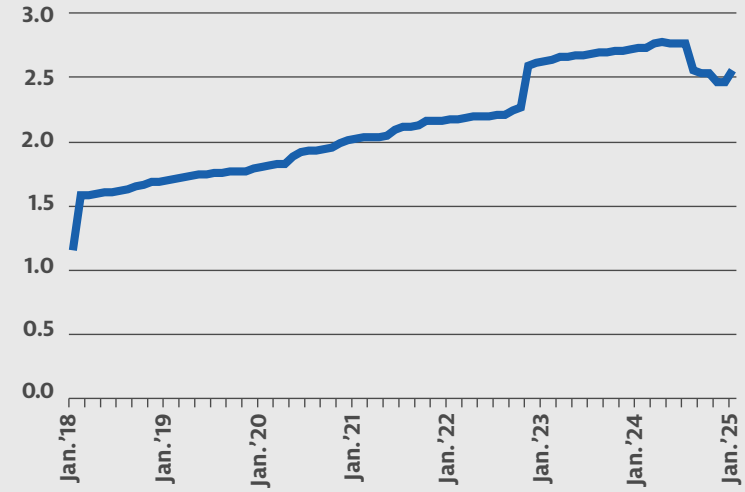
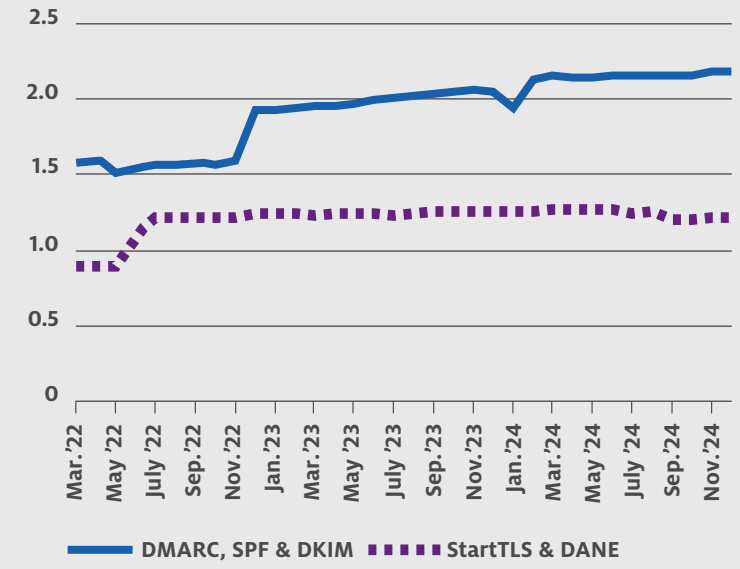


Fig. 9 | Use of e-mail security standards (€m)



about the Notice-and-Take-Down Procedure. All the Academy's e-learning modules are now available in English as well.

Facilitating the sale of existing domain names

Since 2023, we have been facilitating the sale of existing domain names through a pilot running on sidn.nl. If a visitor uses our .nl Suggestion Tool to check the status of a domain name, and the name is 'Active' and 'For sale', a pop-up appears providing details. An evaluation of the pilot in early 2024 found that registrars were generally positive, so the function has been retained on our website. Registrars can also integrate the function into their own domain name suggestion tools if they wish.

Registrar Scorecard

The Registrar Scorecard (RSC) is our incentive programme for nl registrars. Through the programme, we offer financial incentives in order to promote the active use of domain names and the adoption of modern, open internet standards. So that data exchange in the .nl zone is more secure.

We didn't introduce any new incentives to the RSC in 2024, but continued using the RSC to promote the adoption of IPv6, DNSSEC and the e-mail standards StartTLS, DANE, DMARC, DKIM and SPF. For a registrar to qualify for any RSC incentive, a percentage of the .nl domain names in their portfolio must be DNSSEC-enabled. In 2024, we increased that threshold from 10 per cent to 20 per cent.

The IPv6 incentive was reduced from 8 cents to 6 cents per qualifying domain name per half year because IPv6 is increasingly the norm. The total value of financial incentives paid out was €900,000 in 2024, and the adoption levels of all standards remained stable. As well as receiving payments, registrars participating in the RSC are provided with performance data. Each registrar has a personalised dashboard where stats on abuse prevention and registration data quality are made available, and they can see how they compare with their peers.

SIDN Panel

In 2024, our SIDN Panel had 550 or so members, including .nl registrants, internet users and entrepreneurs. By inviting panel members to complete questionnaires, we're able to improve our understanding of market developments and continue refining our services. The questionnaires address subjects such as cybercrime, website findability on Google and content management system preferences. The feedback we receive is used in our communications and provides insight into trends affecting .nl. The average response rate in 2024 was about 20 per cent, or roughly 100 respondents.

Feedback from the SIDN Panel provides insight into trends affecting .nl.

Complaints and Appeals Board

The registration and assignment of .nl domain names nearly always goes without a hitch. In the rare cases where a .nl registrant or registrar is unhappy with a decision made by SIDN, they can appeal to the Complaints and Appeals Board for .nl Domain Names (C&AB). The C&AB also considers complaints about domain name registrations that are believed to be inconsistent with public order or decency – in other words, morally unacceptable to society. In 2024, the C&AB ruled on 1 appeal against a registrant change made by SIDN. No new complaints or appeals were received. The C&AB's rulings are published on cvkb.nl.

Dispute Resolution System for .nl Domain Names
Sometimes, a disagreement arises regarding a domain name's similarity to a brand name, trading name, personal name or organisation name. Our Dispute Resolution Regulations for .nl Domain Names lay down the rules for handling such disputes. The system offers registrants and other internet users a relatively low-cost alternative to taking a dispute to court. A new version of the Dispute Resolution Regulations took effect on 1 September 2024. In 2024, 51 dispute cases were started. Our mediators handled 20 of those cases. In 9 of them, successful mediation led to the dispute being settled early.

Notice and Take Down Code

The Notice and Takedown (NTD) Code provides the internet industry with guidance on how to proceed when told about unlawful or criminal internet content, such as child sexual exploitation material, discriminatory content, plagiarised content or phishing material. There is no legal obligation to follow the Code, but it serves as a framework for responding appropriately to requests to take down internet content. Along with many other internet industry actors, we support the NTD Code.
When problematic content is detected on a .nl website, we are among the actors with a part to play. However, the person seeking to get the content taken down has to take a number of steps before we can intervene. We received 58 notice-and-take-down requests in 2024, which led to us disabling 14 domain names. In the other cases, either someone else intervened or we decided that the content was not clearly criminal or unlawful.

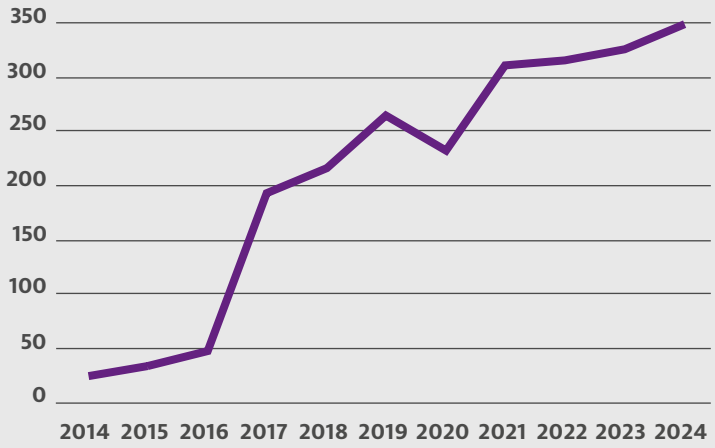
European NIS2 Directive

The second Network and Information Security Directive (NIS2) is an EU law designed to address digital threats to network and information systems. The ultimate aim being to increase member states' digital and economic resilience. NIS2 includes requirements on domain name registrations and the accuracy of the associated data, such as registration data. For example, all registries and registrars for domains in the EU will have to publish information about how they verify their Whois data. NIS2 also designates all DNS service providers as operators of essential services. As such, like SIDN, they must meet strict security requirements and new cybersecurity requirements, and they have a duty to report certain matters to the competent authority.

In 2024, we continued preparing for introduction of the new rules. In partnership with the RA, we developed a protocol for checking registration data, which was submitted to the Ministry of Economic Affairs for comment. We're aiming to make further progress with the registration data process in 2025. We also set up an online trust centre last year, offering real-time information about our security status and ISO 27001:2022 certification status, for example. Registrars need such information to comply with NIS2.

The deadline for implementation of NIS2 was 17 October 2024. We and the registrars completed our preparations before that date. However, implementing legislation was delayed in most EU member states, mainly because NIS2 leaves a lot of scope for interpretation, inevitably leading to debate. The Dutch government did publish a draft of its proposed Cyber Security Act for online consultation, which clarifies how the Dutch authorities interpret NIS2. The draft says that the policies and procedures for verifying registration data should as far as possible follow existing international standards and procedures, such as the data validation process for gTLDs.
The Cyber Security Act will certainly not come into effect in the Netherlands until at least the third quarter of 2025. Nevertheless, NIS2 is already directly relevant to hosting service providers and registrars, because many operate in multiple member states. A lot of them are therefore taking steps such as rolling out uniform e-mail address verification and registrant ID verification procedures for all European customers, in the interest of workable NIS2 compliance.

Fig. 10 | Number of brands protected by SIDN BrandGuard



Registry services for .amsterdam, .aw and .politie

As well as operating the .nl domain, we act as registry service provider for 2 gTLDs, namely .amsterdam and .politie, and for Aruba's country-code domain .aw. We also provide DNS services for the Curaçao's .cw domain and Denmark's .dk. In 2026, ICANN is expected to open a new gTLD application window. Corporations and governments will then be able to apply to ICANN to set up extensions matching their own names, as Amsterdam and Friesland have already done with .amsterdam and .frl.
SIDN therefore commissioned Markteffect to find out what Dutch internet users think of domain name extensions for cities, regions and corporations. The survey revealed that there is a market for new domain name extensions, especially for the Netherlands' larger cities and regions. In this field, we're working with Dotlocal to support Dutch entities that want to start new geographical top-level domains (geoTLDs). Our focus is the technical infrastructure for such domains, while Dotlocal are handling the marketing and organisational aspects.

SIDN BrandGuard

Brand abuse can put internet users at risk and undermine brand owners' reputations. We therefore offer a monitoring service called SIDN BrandGuard, which helps public bodies, online retailers and other organisations to protect their brands. And, by doing so, keep their customers and visitors safe while also boosting their own security. A personalised dashboard immediately alerts the SIDN BrandGuard subscriber whenever a domain name is registered that matches or resembles their brand name, enabling them to respond promptly. Where possible, the service flags up registrations not only under .nl, but also under other top-level domains (TLDs). BrandGuard also has a logo detection module, whose users receive information about the use or abuse of their logos on .nl websites. Where appropriate, subscribers can request specialist assistance from our legal consultants ICTRecht, and can undertake action themselves.

SIDN BrandGuard now protects more than 200 brands belonging to public bodies, hospitals, banks, insurance companies and telecoms companies. In 2024, we made a number of minor changes to the service's user interface. IP whitelist-based access control was replaced by 2-factor authentication, meaning that subscribers can log in securely from any location. We also invested in improving our logo detection algorithm, enabling faster and more accurate logo recognition.

SIDN BrandGuard protects 350-plus brands.

Data breach caused by maintenance activities

In September, as a result of maintenance to sidn.nl, the registration data on 1,918 domain names was temporarily visible to Whois users.
The information mistakenly disclosed was the name, address, e-mail address and phone number of the registrant, and the administrative and technical contact details. That information should be visible only to the domain name's registrar and to us.
We therefore contacted the registered contacts for all 1,918 domain names and immediately reported the incident to the Data Protection Authority and the Dutch Authority for Digital Infrastructure (RDI). We also investigated the impact, so that we could take steps to prevent any recurrence. As far as we are aware, the incident had no negative consequences for the people whose data was compromised.

.nl Control 2.0

Our .nl Control service offers .nl registrants greater control over their domain names. For example, the registrant must give the registrar explicit consent for transactions such as cancellation of a protected domain name. We had planned to launch version 2.0 of .nl Control in 2024. However, those plans were ultimately dropped, because we'll be able to offer .nl registrars the new functions via Hello Registry from 2026.

Outlook

Collaborating to fight online fraud

In 2025, we plan to make it easier to act quickly against phishing mail. We'll define a set of criteria, which mail must meet to be blocked. With a view to tackling online fraud, we're also aiming to form new partnerships with organisations such as The Netherlands Gambling Authority and the regulatory bodies for the medical sector and oil trade. Cybercriminals targeting the oil trade use the same tactics as fake webshops, creating .nl websites where oil is offered at attractive prices, and invoicing for non-existent storage capacity.

Registry fee uplift

Having made a relatively large adjustment in 2024, we are increasing our registry fees only by the rate of inflation in 2025. At the start of the year, we increased our fees by 2.5 per cent. The basic cost to a registrar of registering a .nl domain name for a year is now €4.25, while a registrar's account costs €85 a month.

Ending privacy and proxy services

Since 1 October 2023, it's been against the rules to register a .nl domain name with someone who isn't the domain's actual controller – e.g. a privacy or proxy registration service provider – named as the registrant. We therefore monitor new registrations, and we're working with privacy and proxy service providers active in the .nl domain to get existing registrations amended. Our aim is to eliminate all privacy and proxy registrations from the .nl zone by 1 October 2025.

Incentive for security.txt

From 2025, we're adding a financial incentive for the adoption of security.txt to the RSC. The scheme involves giving registrars rebates on .nl domain names whose websites have valid security.txt files. At the end of 2024, only 2.8 per cent of .nl websites had such files.

NIS2 implementation

We'll continue talking to the RA about how we can help registrars comply with NIS2 – particularly its registrant data verification requirements – and the Cyber Security Act, which will implement the directive in Dutch law. We're keeping a close eye on developments in this field.

Registry services via Hello Registry

We envisage using Hello Registry as a platform for a network of like-minded top-level registries that are dedicated to innovation, share certain core values and want to build a collaborative community. At ICANN 81 in Istanbul, where we and CIRA unveiled the name of the new registry platform, and in the weeks that followed, Hello Registry attracted considerable interest from other registries. Once we have migrated .nl in 2026, we therefore plan to invite other ccTLDs to get onboard. So that our fellow ccTLD registries have access to a sound and stable solution, and so that the internet is more secure. Together with CIRA, we're approaching interested parties and attending events where we can reach out to other ccTLD registries.

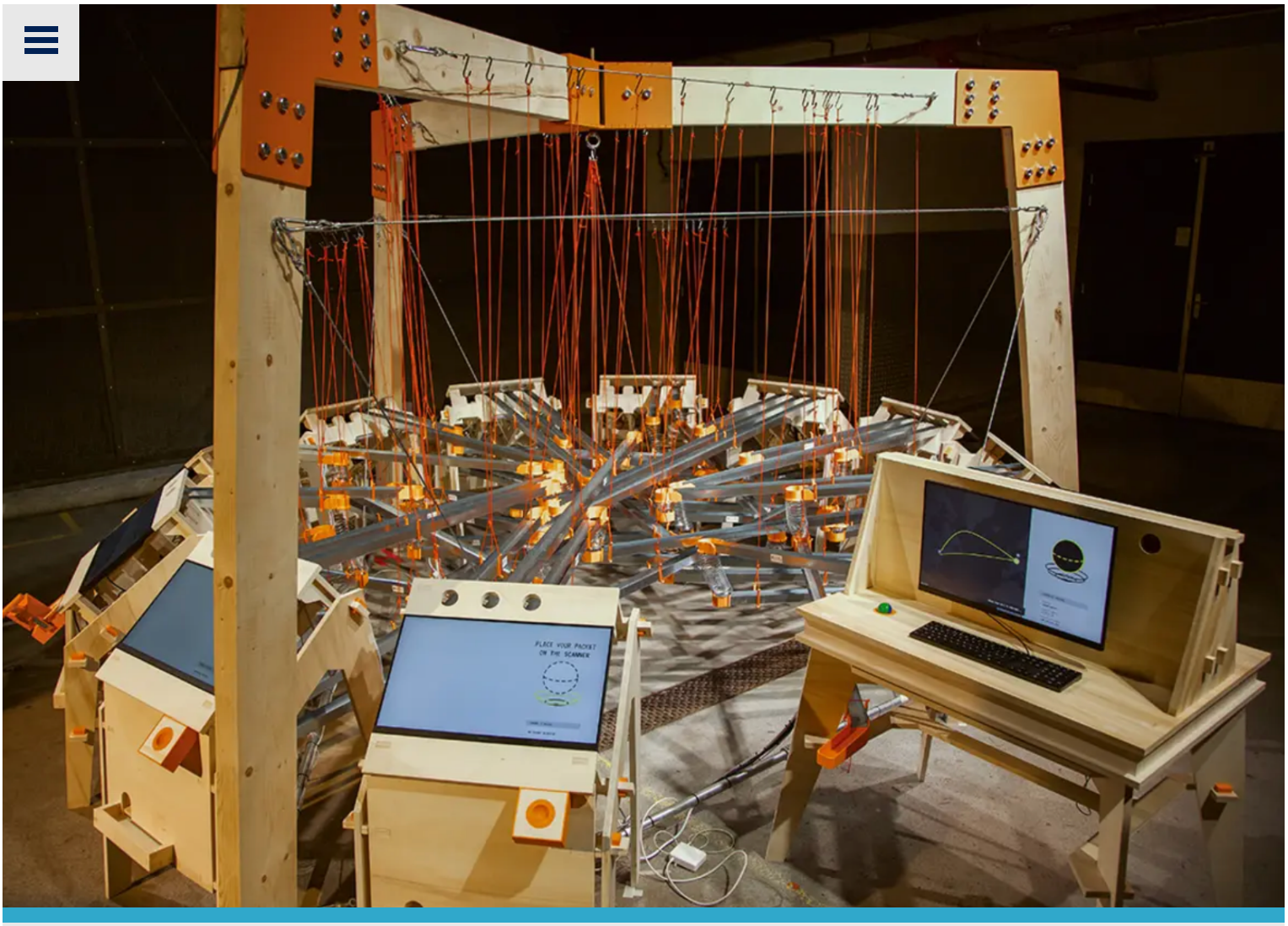
"Although a scam like that requires a lot of up-front investment, the potential rewards easily make it worthwhile for the crooks."

Gijs van der Linden
Team Leader Police National Internet Fraud Desk

Every hour counts

"The number of trading fraud reports we get about webshops is rising all the time. The figure has gone from 16,000 in 2023 to 20,000 and counting in 2024. And it's estimated that only 1 in 5 victims actually report what's happened. Some scams are very professionally organised, maybe involving very precise copies of popular legitimate webshops. Although a scam like that requires a lot of up-front investment, the potential rewards easily make it worthwhile for the crooks. Every hour that a malicious webshop remains live, it claims more victims. So SIDN has agreed with the Police National Internet Fraud Desk (LMIO) that SIDN can immediately disable any webshop identified by LMIO as fraudulent, without further investigation."

> **Read more about the partnership**



Our public role working for the Dutch and global internet communities

4 A secure, stable and future-proof internet

A secure internet is a prerequisite for people to have confidence online. Especially as our dependence on the internet continues to increase. We therefore work to build and maintain a secure, stable and future-proof internet for the Netherlands, Europe and the wider world. We focus particularly on the .nl domain and its contribution to Dutch society. Against that background, SIDN Labs carries out applied technical research with the aim of further enhancing the security of the internet infrastructure. And, through SIDN Fund, we invest in projects that contribute to an inclusive, secure and uniting internet. Furthermore, SIDN Labs and SIDN Fund collaborate with external partners and work together on projects such as Visualising the Internet Infrastructure.

SIDN Labs

In the modern world, the internet plays a vital role. Modern digital societies are therefore highly dependent on a secure internet infrastructure. The infrastructure is an indispensable layer that transports data across the internet from A to B, typically via multiple networks. Our research team, SIDN Labs, works to continue increasing the security of that infrastructure for the Netherlands, Europe and the wider world through applied technical research. SIDN Labs' research agenda spans 3 primary themes: domain name security, infrastructure security and emerging internet technologies. The team collaborates with universities, infrastructure operators and other research centres on both short-term and long-term projects. Particular attention is paid to operational challenges of concern to SIDN and .nl. The team's research findings are made available to the public and are widely applicable, so that other stakeholders can make their own contributions to internet resilience.

SIDN Labs brings research and practice together and acts as a bridge between the research world and the operational world. In 2024, we taught courses on Advanced Networking and Security Services for the Internet of Things at the University of Twente (UT), and we delivered guest lectures at Leiden University and UT. We also collaborated closely with the UT within the Twente University Centre for Cybersecurity Research (TUCCR) consortium, providing cybersecurity input that TUCCR used for research and in the development of new solutions. In addition, we supervised 5 MSc students and 3 PhD students. As in previous years, we seconded 4 of our team members, each for 1 day a week, to various universities for joint research and teaching: Delft University of Technology (1 team member), the University of Amsterdam (1) and the UT (2). We were also actively involved with Internet.nl, and our researchers sat on SIDN Fund's Advisory Panel, 2 IETF working groups, and ICANN's Root Server System Advisory Committee (RSSAC). Furthermore, SIDN Labs' Director is a member of the Dutch government's Cyber Security Council. In that role and acting as a representative of the academic community, he helps to guide efforts to enhance the security of the Dutch and European internet infrastructures.

Some of the projects undertaken by SIDN Labs in 2024

Post-quantum cryptography in the DNS

PATAD (Post-quantum Algorithm Testing and Analysis for the DNS) is a project we are running to empirically map the impact of post-quantum cryptography (PQC) on DNSSEC. In 2024, we made the PATAD testbed software available to other DNS researchers and operators in open-source form. Using our software, such actors can experiment with using the PQC algorithms MAYO, Falcon and SQCSign in the DNS. For example, the software makes it possible to systematically model realistic DNS topologies, and to evaluate how DNSSEC works with PQC. The 3 algorithms are included in the PQC algorithm evaluation and standardisation programme run by the National Institute of Standards and Technology (NIST). We also performed various experiments in our testbed, including a comparison of the signing of several DNS zone files using MAYO and Falcon with using the traditional algorithms RSA and ECDSA.

DDoS Clearing House

The Clearing House system generates DDoS fingerprints, which essential service providers, including governments, banks and internet access providers can use to automatically share information about DDoS attacks. Because the better informed they are, the better prepared they are.

Since April 2024, the National Internet Providers Management Organization (NBIP) has been running the DDoS Clearing House under the flag of the Dutch National Anti-DDoS Coalition (NL-ADC). Over the last few years, our SIDN Labs team has led the underlying research and the development of the Clearing House in partnership with SURF and the University of Twente. With the same partners, we wrote an article about the DDoS Clearing House, which was published by the peer-reviewed journal IEEE Communications Magazine.

Our article about the DDoS Clearing House was published in the peer-reviewed journal IEEE Communications Magazine.

Autocast
Autocast is short for automated anycast. Anycast serves as an observation platform for a DNS operations team such as SIDN's. The platform makes automated recommendations about interventions such as enabling or disabling .nl anycast nodes or sites on the basis of much more detailed data than that used by traditional monitoring systems, including country, region and round-trip time. Autocast draws on passive and active internet measurements, such as those generated by our ENTRADA open-source data platform and our Verfploeter software.

Using ENTRADA data, we improved our understanding of the round-trip times of .nl queries: the number of milliseconds it takes for a DNS query to reach a DNS server and for the response to get back to the query's author. We also worked with SIDN's DNS team to perform active daily internet measurements from the production name servers for .nl. The results helped us to assess .nl's status within the DNS and to further optimise the location of .nl's name servers.

RESTful Provisioning Protocol
The Extensible Provisioning Protocol (EPP) is a protocol for managing domain name objects within a registry, for purposes such as updating domain names. EPP is standardised by the IETF and based on Extensible Markup Language (XML). As a 'stateful' protocol, EPP uses the 'session' concept, where the EPP server logs information about the client. That complicates the task of developing a scalable system capable of rapidly processing a large number of EPP messages. EPP is now about 15 years old, and SIDN has been using it for .nl since 2010.

The RESTful Provisioning Protocol (RPP) is a standard for a new domain name registration API, whose development we initiated. As well as being easier for registrars to use than EPP, RPP will help domain registries by increasing scalability and improving performance and security. Furthermore, RPP is a stateless protocol, making it more compatible with modern software-engineering technologies, such as containerisation and Kubernetes. We are now progressing the development of RPP after restarting a project from 2012.

At IETF 121 in Dublin, we organised a meeting for delegates interested in RPP, such as engineers from other European registries. Sufficient consensus was found for the creation of a new IETF working group. With our community partners, we therefore got the ball rolling by drafting a charter, setting out the basic principles for the group.

DNS root servers
In partnership with NLnet Labs, we undertook research for the root server operators Verisign and ISC. The work involved independently checking ICANN measurements indicating that the availability of the root server system often fell below the required level. Our research showed that most problems were attributable to ICANN's measurement platform and the network path between the platform and the root servers. We also discovered and fixed a bug in the measurement software, which made the root servers' response times appear poorer than they actually were. The root server operators were pleased with the project outcome.
This was our third study of the security and stability of the DNS root, and it emphasised that we are now regarded as experts in this field.

RegCheck
Our machine learning system RegCheck assigns risk scores to new domain name registrations, so that our support team and teams at other registries are able to identify potentially malicious domain names at the time of registration. During the year, we switched to a new classification algorithm based on decision trees. We also made the RegCheck dashboard more user-friendly and linked RegCheck to Microsoft Dynamics 365, enabling the support team to initiate registrant investigations sooner when a registration is flagged by RegCheck.

We additionally modernised and automated RegCheck rollout and training, to make the system more flexibly deployable on any modern computing platform. Finally, we shared the RegCheck software with a few other registries, so they can incorporate it into their systems for their own use.

Study of phishing in the .nl, .be and .ie domains
In September 2024, we teamed up with DNS Belgium (the registry for .be), IE Domain Registry (for Ireland's .ie) and the universities of Twente, Delft, Leuven and Grenoble to produce a peer-reviewed article about our research into the evolution of phishing attacks. We analysed a total of 28,754 incident reports relating to the .nl, .be and .ie domains issued by security service provider Netcraft during the period 2013 to 2023. We also compared the 3 domains' registration and mitigation policies.
Our findings were presented at various operator community forums, including RIPE, DNS-OARC and CENTR, and at ACM Computer and Communications Security – a renowned academic conference, for which our paper was accepted.

We analysed more than 28,000 phishing reports issued by security service provider Netcraft.

BGP-security
The BGP (Border Gateway Protocol) is used to route data from origin to destination across the 75,000-plus networks that together make up the internet. The security of the BGP is vital to the entire internet, including core systems such as the DNS. Unfortunately, however, the existing technologies used to increase BGP security don't resolve all the problems with the protocol. In 2024, we therefore added BGP security to our research portfolio.
We developed a research agenda for BGP security and built up our collaboration with the University of Twente in this field. For example, we teamed up with the university to demonstrate that the internet has a longstanding problem with 'serial hijackers': networks that persistently seek to divert traffic intended for other networks to themselves. We also investigated which routing implementations support BGPsec, and how we could set up a local BGPsec testbed for experimental use.

Resilience of critical and essential services in the Netherlands
We investigated the resilience of the DNS infrastructures of all 6.2 million .nl domain names and of 700 critical and essential service providers in various sectors. The work involved testing the relevant domains' public DNS servers to see whether 3 proven measures for boosting availability were in use. The measures we looked at were distribution of the DNS servers across multiple networks, use of anycast, and use of multiple IP prefixes (groups of IP addresses).
Our results were presented at the ECP Annual Festival, which is traditionally attended by many policymakers. We also made our test software available as open-source code, so that organisations such as hospitals can check their own DNS resilience.

Internet sanctions against Russian media
We studied DNS data to assess the effectiveness of EU sanctions against Russian media outlets. The work was done in collaboration with teams from the University of Twente, the University of Illinois at Chicago, the University of Amsterdam and the non-profit organisation Open Observatory of Network Interference. Our findings were summarised in a peer-reviewed paper, which one of our partners presented at a conference called Free and Open Communications on the Internet.

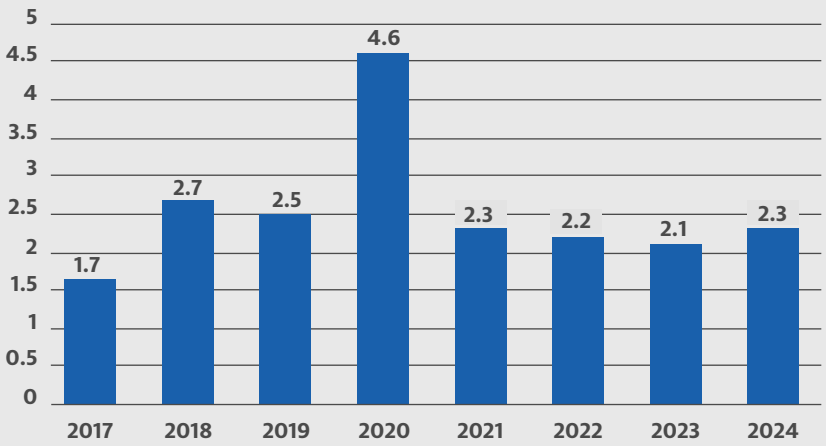
Our study illustrated how internet measurements can support policy evaluation, in this case the evaluation of European Union policy. It also highlighted the importance of combining expertise in various fields, in this case internet measurement expertise and expertise in European and media studies.

Our internet measurements support policy development and evaluation.

SIDN Fund

The internet has great benefits for present day society, and for the society of tomorrow. SIDN Fund therefore works to promote a strong internet for everyone by supporting innovative projects that contribute to an open, free and reliable internet. The focus is on 3 fields: a strong internet, strong internet users and the societal side of the internet.

Fig. 11 | Annual contribution to SIDN Fund (€m)



In 2024, it was 10 years since SIDN Fund's formation. In that time, the Fund has supported more than 400 projects in fields including disinformation, online resilience and electronic accessibility. Nearly €15 million has been granted to promising projects and about €800,000 to academic research. The Fund has also formed important partnerships with municipal authorities, the Ministry of the Interior (BZK) and other funding bodies with similar aims.

In March 2024, SIDN Fund made a call for proposals for larger projects and smaller pioneering projects linked to the theme of Internet Sustainability. Through the call, the Fund aimed to support initiatives to make the internet more sustainable or to reduce its environmental impact. With the Fund's support, 4 projects linked to the theme were started, including 2 pioneering

projects. Through a second call on the theme of Participation in Digital Society, the Fund made grants to 6 projects aimed at building up the skills of people who find it hard to participate in digital society. In addition, pioneering project organisers were again able to make applications for grants of up to €10,000 at any time, rather than within a particular window. As in previous years, the Fund also scouted projects with significance for society and the potential to make an impact in one of the 3 focus fields.

Three-yearly evaluation

SIDN Fund's activities are evaluated once every three years, and 2024 was one such year. The Advisory Panel and stakeholders were particularly positive about the Fund's approach, which was seen as delivering projects and coalitions with real benefits, such as combining support from SIDN Fund with grants from other sources. As a result, the Fund was able to maximise the scope and impact of supported projects. Aspects of the Fund's work flagged up as opportunities for improvement included building awareness of the pioneering project funding mechanism, improving the efficiency of collaborative programmes, upgrading the scouting process, investing in relations with registrars, and reinforcing strategic communication.

The Advisory Panel and stakeholders also highlighted the need for a strong financial base. The Fund was accordingly advised to seek inward funding from additional sources, and to investigate the possibility of partnering with other bodies on multi-year programmes.

Collaboration between SIDN Fund and SIDN Labs

August saw the start of Visualising the Internet Infrastructure: a joint SIDN Fund-SIDN Labs programme aimed at raising awareness of the importance of the digital infrastructure amongst stakeholders such as politicians and journalists. For the programme, 3 designers are creating interactive visualisations of the digital infrastructure: a simulation game called Packet Panic and online visualisations entitled Are We Digitally Autonomous Yet?, The Border Gateway Protocol Travel Guide and How the Net Works. The programme is inspired by the large-scale internet measurements that research teams at SIDN Labs, the UT, TU Delft and elsewhere constantly perform.

Responsible Internet Thesis Award

Freedom Internet, Mijndomein, SIDN Fund and the Dutch Royal Academy of Science promote internet responsibility by organising the Responsible Internet Thesis Award. The annual award is given to (former) master's students who have done research into a responsible internet where security, privacy and access are centre stage. In 2024, the first prize of €3,000 went to a researcher who had investigated the regulation of influencers who share advertising content on social media. The €1,000 second prize was given for a study into the unauthorised sharing of personal data by online pharmacies in Europe.

Some of the projects supported by SIDN Fund in 2024

Grid-aware websites

Every time an internet user loads a website, the site's servers and the user's device use electricity, leading to 'invisible' carbon emissions. The Green Web Foundation is therefore building an open-source toolkit that developers can use to make their websites grid-aware. A 'grid-aware' website is one that can react intelligently to the carbon emissions and energy consumption of the electricity grid. Using software that enables 2 applications to communicate with each other (APIs), information is gathered about the visitor's electricity grid, which is then used to make eco-friendly adjustments to the site's design. SIDN Fund financed the entire project through its Sustainability call in 2024.

DigiPad

DigiPad helps young people in care, youth detention and special education to develop vital digital skills in a safe and accessible learning environment. The project was supported

through the Participation in Digital Society call in 2024. DigiPad is an online programme that enables young people to become more resilient and participate more independently in digital society. It was developed in partnership with the Lelystad Youth Detention Centre. SIDN Fund paid for the programme's refinement and wider rollout.

The Green Web Foundation's open-source toolkit makes websites grid-aware.

Carefree Connection campaign
Every day in the Netherlands, large numbers of people use public Wi-Fi networks, which often aren't secure and expose their users to risk. The cities of Amsterdam, Eindhoven, The Hague and Rotterdam therefore teamed up with Publicroam to run the Carefree Connection campaign. The initiative was jointly supported and financed by the cities and SIDN Fund. Local amenities such as museums, sports venues and cultural centres were therefore able to try out Publicroam's secure and privacy-friendly Wi-Fi roaming services for free.

Open-source AI auditing
Along with the Ministry of the Interior and Kingdom Relations, SIDN Fund supported the Open-source AI Auditing project, which builds on tools previously developed by the Algorithm Audit foundation. The tools help with the identification of normative issues with the use of algorithmic systems, such as what is ethical. The project involves the development of 2 technical open-source tools for detecting and migrating advantageous features of algorithmic systems. The project team are also developing a qualitative methodology known as algoprudence, where questions about responsible use are dealt with on the basis of consultation.

Unlocking digital resilience
In October 2024, a consortium of Dutch foundations and companies, the police and the government organised a national campaign called Unlock Digital Resilience. The National Digital Resilience Course, which formed a major part of the campaign, was developed with support from SIDN Fund. As well as helping internet users to recognise unsafe situations online, the course builds awareness of online fraud, cybersecurity, fake news, online polarisation and other such issues.

The National Digital Resilience Course helps internet users to recognise unsafe situations online.

Digital autonomy
Dutch society is increasingly dependent on non-European technology. Our data is saved on cloud platforms, over which we have little control. A project called Are We Digitally Autonomous Yet? therefore set out to discover which Dutch organisations are dependent on which suppliers and what technology. As well as providing an extensive overview of dependency and demonstrating its impact on individuals, the findings highlight opportunities for increasing our digital autonomy.

Offlimits Hash Check Service
Offlimits fights online sexual exploitation and works to make the online world more secure. One way that the expertise centre does that is by providing the Hash Check Service (HCS). Originally a European Commission initiative, the service enables users to scan data to see whether it includes images previously identified as depicting the sexual exploitation of minors. The service makes use of the hash lists published by organisations such as the Dutch police and the National Centre for Missing and Exploited Children. A project was set up to increase the reach of the HCS, raise the quality of the hashes and secure long-term governance and funding for the service. The more companies sign up to use the service, the more images that are proactively taken down. The project was underwritten by SIDN Fund and the Ministry of Security and Justice.

Outlook

SIDN Labs

Post-quantum cryptography in the DNS
In partnership with SURF and the UT, we're using our PATAD testbed to establish which new and as yet unstandardised PQC algorithms may be suitable for DNSSEC. Our findings will be fed back to NIST and the internet community. We also plan to extend the PATAD testbed. The analyses and measurement results will be published in 1 or more technical reports and peer-reviewed articles co-authored with SURF and the UT.

Autocast
One of our aims is to make Autocast more widely available to DNS operators. In 2025 , we'll open-source the Autocast dashboards and the supporting data model as an ENTRADA extension. We'll also continue Autocast's development, transforming it from an observation dashboard to an anycast control centre. The resulting system will be made available not only to our own DNS team, but also to other DNS operators, so they can use their anycast platforms to distribute traffic across multiple locations more effectively.

RESTful Provisioning Protocol
In 2025, we'll work with the community to take forward development of the RPP charter, and we'll contribute to formulation of the standard.

RegCheck
We're planning to improve the risk scores generated by RegCheck by utilising DNS query data, such as resolver IP address and query type. We'll also investigate the scope for using information from the Domain Name Ecosystem Mapper – our web crawler known as DMAP for short – to speed up the identification of phishing sites and other malicious websites. We remain in discussion with registries and registrars with a potential interest in the RegCheck-software.

SIDN Labs' research infrastructure is being relocated to Nikhef and SURF.

Phishing follow-up study
In 2025, we'll build on our earlier phishing research. A follow-up study will be organised with our established partners – the registries for .be and .ie – plus the registries for .eu and .br.

Research infrastructure

In 2025, SIDN Labs' research infrastructure will be relocated to Nikhef research institute in Amsterdam. The move has various advantages, including an autonomous system of our own, which we can use to independently install and experiment with BGPsec software. The DNS query data we use for our research will be stored at SURF, the operator of the Netherlands' research and educational network. We'll make the data accessible on our servers at Nikhef via a high-speed link with SURF. In line with those developments, a new item will be added to our research agenda for 2025: research infrastructure operations, which will cover the management and continuous improvement of our research network.

SIDN Fund

In partnership with Topsector ICT, SIDN Fund is organising a call for proposals linked to the theme of the responsible use of AI in practice. The year's second call will be Getting a Grip on Polarisation 2, organised together with the Limelight Foundation and the Gieskes Strijbis Fonds. In addition, organisers will again be able to submit applications at any time for grants of up to €10,000 in respect of pioneering projects linked to any of the 3 focus fields. The Fund will also proactively scout promising projects aligned with its objectives. SIDN Fund particularly welcomes proposals for projects concerned with sustainability, accessibility and security. Finally, the Fund will continue its sponsorship of the Responsible Internet Thesis Award and its partnership with SIDN Labs. One field of collaboration will be the programme Visualising the Internet Infrastructure.

"Many .nl domain name operators take steps to increase availability, but there's still room for improvement."



Moritz Müller, Thijs van den Hout, Caspar Schutijser
Research Engineers at SIDN Labs

Can the Netherlands' digital infrastructure withstand a knock?

"As the NAFIN outage in 2024 showed, digital infrastructure outages can cause widespread disruption to modern societies. So, here at SIDN Labs, we investigated the Netherlands' digital resilience. We assessed resilience by testing the public DNS infrastructures of more than 700 organisations on the internet, and of all 6.2 million .nl domain names, to find out how many were using certain measures to protect against outages and attacks. Many organisations in the Netherlands do appear to be paying attention to the resilience of their DNS servers. However, it's apparent that more could be done for many domain names, such as those used in the hospital sector. We're publishing the test tool that we developed, so that others can use it to perform their own surveys."

> Read more about the study

"Experiment with grid-aware websites to make the internet greener."

Hannah Smith
Operational Director at The Green Web Foundation

Project SIDN Fund: Grid-Aware Websites

"Every time you load a website, your device and the site's servers use electricity, leading to 'invisible' CO_2 emissions. And finding a solution isn't easy, because electricity networks are very complex. So The Green Web Foundation is building an open-source toolkit that developers can use to create websites that are grid-aware, meaning that they respond to the network providing the electricity. We want the internet to be fossil-fuel-free by 2030. SIDN Fund's support means that developers can now experiment with grid-aware websites, which hasn't been possible before."

› **Read more about the project**

National and international partnerships based on shared values

5 Working together for the internet user

Partnerships are invaluable for a globally unified, secure and open internet. They are also needed to accelerate technological innovations and to maximise impact breadth. After all, the internet is the world's biggest joint undertaking, whose further development is everybody's collective and individual responsibility. We therefore share our expertise and research results on topics such as abuse prevention and cybersecurity with others in the internet community and the academic world. We also play an active role in international technical and internet governance forums, including the IGF, ICANN and IETF. And we support initiatives to tackle abuse on the internet and to increase its value.

Contributions to organisations and conferences

We place great emphasis on collaborating with partners in the Netherlands, the European Union and beyond. For example, we play an active role in various international forums, as illustrated by the examples below.

ICANN
The Internet Corporation for Assigned Names and Numbers (ICANN) performs a number of important internet-related tasks. It distributes IP addresses, for example, and decides the policies governing the issue of gTLDs, such as .com, .net and .shop. One particularly significant function for SIDN is management of the 'root' and the root server system, which is done by ICANN's affiliate IANA. We play an active role in several working groups, particularly the ccNSO (country code Name Support Organization), the body for country-code registries within ICANN.

In 2024, we linked up with the Dutch government's economics ministry to organise a pre-ICANN session for stakeholders in the Netherlands. ICANN again held 3 meetings during the year. ICANN 79 took place in San Juan, Puerto Rico, in March, and was followed by ICANN 80 in Kigali, Rwanda, in June and ICANN 81 in Istanbul, Türkiye, in November. The meetings were dominated by planning for the new gTLD application window in 2026, and by efforts to clamp down on abuse. At ICANN 81 in Istanbul, we introduced Hello Registry to all the delegates from registries, registrars and other interested organisations. SIDN Labs made a presentation describing the team's research into post-quantum cryptography in the DNS.

RIPE NCC
RIPE's Network Coordination Centre (NCC) is responsible for tasks such as issuing IP addresses to internet service providers and other bodies in Europe, the Middle East and parts of Central Asia. RIPE held 2 physical meetings in 2024, which we attended. RIPE 88 was in Krakau, Poland, in May, while RIPE 89 ran from late October to early November in Prague, Czechia. One member of the SIDN Labs team co-chairs RIPE's DNS Working Group. In 2024, another team mem-ber co-authored the RIPE report DNS Resolver Recommendations (RIPE-823), based on our work with DNS4ALL.

IETF
The Internet Engineering Task Force (IETF) works on evolution of the internet protocols and internet architecture, and on optimising the internet's performance. Various network operators, designers, vendors and researchers participate in this international community, membership of which is open to all. The IETF held 3 physical meetings in 2024. IETF 119 was in Brisbane, Australia, in March, IETF 120 in Vancouver, Canada, in July, and IETF 121 in Dublin, Ireland, in November. At the meetings, SIDN Labs made presentations on topics including the RESTful Provisioning Protocol. SIDN Labs also contributed to a draft research agenda for a post-quantum DNSSEC.

DNS-OARC
The DNS Operations, Analysis and Research Center (DNS-OARC) is a platform for key operators, analysts and researchers to share information and knowledge and coordinate responses to attacks and other problems. In 2024, the platform held 2 international meetings for stakeholders. OARC 42 was held in Charlotte, USA, in February, and OARC 43 in Prague, Czechia, in October.

CENTR
CENTR is an association of European ccTLD registries. CENTR and its members are jointly responsible for 80 per cent of all registered country-code domain names in the world. We are active members of the organisation. In 2024, our CEO, who was already a CENTR board member, was appointed to the chair of CENTR's Board of Directors.

A member of our ICT team also co-chairs the Technical Working Group and an SIDN Labs team member co-chairs the R&D Working Group. In 2024, CENTR held various workshops in Europe on marketing, security, administration, legislation, and research and development. SIDN staff made presentations at the CENTR Jamboree and CENTR GA 72, as well as to the CENTR Tech and R&D working groups. CENTR holds an annual Registrar Day, to which we invite .nl registrars. One member of our team also co-chairs the Tech Working Group.

CENTR members represent 80 per cent of the world's registered country-code domains.

ECP Annual Festival 2024

From its neutral, independent position, ECP | Platform for the Information Society contributes to a trustworthy, opportunity-rich and resilient digital society. It works in partnership with both public and private organisations. ECP's 2024 Annual Festival was held in The Hague in November. Its theme was 'We've gone digital?!', and we were present as one of the partners. SIDN Fund's CEO was one of the speakers, talking about the Fund's first 10 years and other topics. In connection with the question of how society can get a grip on polarisation, we teamed up with SIDN Fund to organise an event entitled Cybersecurity 2024 - Standing up to Digital Threats Together. Representatives from 2 projects supported by SIDN Fund made presentations about their work, and 2 members of the SIDN Labs team presented the results of their research into the Netherlands' digital resilience. Packet Run – an installation developed from a collaboration between SIDN Fund and SIDN Labs, which demonstrates the inner workings of the internet – was also exhibited on the networking floor.

EuroDIG

European Dialogue on Internet Governance (EuroDIG) is an open platform where stakeholders exchange ideas about the internet and its governance. EuroDIG promotes discussion and collaboration within the internet community linked to the theme of public internet policy. We are active members of the platform, and in 2024 we sponsored the annual EuroDIG conference in Strasbourg, France.

Internet Governance Forum

The United Nations' Internet Governance Forum (IGF) brings together stakeholder groups from all over the world to discuss internet governance and digital policy. Various important themes were addressed in 2024, including cybersecurity, emerging technologies, data management and trust, AI and internet fragmentation. We attended the annual IGF meeting as part of the Dutch delegation. The event took place in Riyad, Saudi Arabia. In October, the annual preparatory meeting was hosted by NL IGF, which is a partnership involving the Dutch government's economics ministry, ECP and SIDN.

ONE Conference

The ONE Conference is an annual event organised by the National Cyber Security Centre, the Dutch government's economics ministry, and the Municipality of The Hague. Held at the World Forum in The Hague, the ONE Conference is Europe's most important cybersecurity event, where knowledge, best practices and research results are shared. The 2024 ONE Conference addressed topics including malware detection, law enforcement, cybersecurity research and public-private partnerships. SIDN Labs contributed an article to the ONE Magazine about post-quantum cryptography in the DNS.

A Picture of the Internet: Past, Present & Future
'A Picture of the Internet: Past, Present & Future' was an event organised by the Internet Society of the Netherlands (ISOC NL), the Platform for Internet Standards (PLIS) and NL IGF. It was held to mark 25 years of ISOC NL, 10 years of Internet.nl and almost 20 years of the IGF. The theme of the event was the development of the internet. SIDN Labs' Director chaired a panel discussion regarding PLIS and Internet.nl, while SIDN's CEO was part of a group of speakers who looked back at the IGF and other developments. A colleague from SIDN Fund made a presentation and shared examples of projects that help to make the internet more secure and more inclusive.

Chamber of Commerce Start-ups Day
In 2024, the Chamber of Commerce once again invited us to take part in its Start-ups Day. The event was held on 16 November at Ahoy, Rotterdam. We teamed up with the Benelux Office for Intellectual Property to run 5 workshops on coming up with the right business name, brand name and domain name. With the help of 2 .nl registrars, Metaregistrar and Team Blue, we answered questions from people just starting out in business. We gave them advice on topics such as hosting, online security, modern internet standards and business e-mail.

SIDN Inspire
On 16 May 2024, we held the fourth edition of SIDN Inspire at LIEMÈS, Utrecht. The theme of the event was 'Forward Together'. A cybercrime specialist and digital detective talked about the importance of collaboration between the police, the business community and victims, and about developments in cybercrime and AI. Topics covered included the domain name industry, the new ICANN contract for gTLDs in 2026, the NIS2 directive, the Lees Simpel app and the use of AI for writing letters. SIDN Labs also discussed post-quantum cryptography and made a presentation on progress with the PATAD DNS testbed.

The theme of SIDN Inspire 2024 was 'Forward Together'.

SIDN TechTalks
Every year, we organise 2 SIDN TechTalks for technical professionals and students. At our offices in Arnhem, we share knowledge and discuss developments relating to issues such as abuse, security and data. Team members also present the results of relevant research and projects. Our 2024 TechTalks were held in April and November. Subjects discussed included the development of an anycast measurement tool, and TimeNL, SIDN Labs' NTP service.

Involvement with outside organisations

Acting as both a knowledge partner and a sponsor, we support organisations and projects that promote use of the internet or address its unwanted side-effects.

Collaboration within Europe
We were part of a 12-strong consortium that set up the European Top-Level Domain Information Sharing and Analysis Centre (TLD ISAC). Since its formation in 2023, TLD ISAC's membership has increased to stand at 17 by the end of 2024.

Our CEO sits on the TLD ISAC steering committee, and CENTR is supporting the initiative. TLD ISAC pools cybercrime-related insights, knowledge and experience. By sharing such information with each other, consortium members can protect their services and the critical infrastructure more effectively and enhance the security of Europe's top-level domains. In October 2024, representatives from the EU ISACs met in Athens to exchange expertise and information about their activities, successes and challenges. At the TLD ISAC annual congress in Brussels in November, a member of the SIDN Labs team made a presentation on Vulnerability Management.

Internet Security Platform
SIDN is a member of the Internet Security Platform (known by its Dutch initials, PIV). The PIV is a partnership of commercial and public organisations that want to make a structural contribution to improving internet security for all users. Important issues addressed by the PIV include privacy, phishing, and how to stop online child sexual exploitation and the sharing of associated images. The PIV serves as a neutral forum for strategic discussions, leading to concrete agreements and initiatives.

Notice-and-Take-Down Working Group
SIDN is a member of the Notice-and-Takedown Working Group, which operates under the auspices of the Internet Security Platform. The Working Group's main aims are management of the national Notice and Take Down Code and the sharing of knowledge and experience relating to the working of the Code. The Code is a stakeholder framework for dealing with reports of unlawful or criminal internet content.

Offlimits
Offlimits is a spinoff of the Online Child Abuse Expertise Bureau. The organisation supports people who have encountered inappropriate behaviour or abuse on the internet, especially the sexual exploitation and abuse of children and adults. The organisation also works to make the online world safer and to strengthen the position of internet users. SIDN sponsors Offlimits.

Public-Private Partnership for Online Content Moderation
Hosting service providers, registrars, social media platform operators and SIDN hold regular meetings with relevant public bodies to discuss ways to optimise the removal or blocking of illegal content. An initiative by the Dutch government's justice ministry, the meetings are part of the European Digital Service Act regime. A low-threshold reporting system for internet users is also being developed.

Alert Online
SIDN is a partner in Alert Online: an initiative by the Dutch government's economics ministry to boost awareness of online security issues, and to encourage cybersecure behaviour by government bodies and the Dutch public. During Cybersecurity Month in October, Alert Online encourages cybersecure behaviour and online security awareness. As part of the Alert Online campaign, we commissioned Markteffect to find out what people in the Netherlands see as the main obstacles to safe and convenient digital living. Phishing mail and other types of attempted fraud were mentioned by 50 per cent of the 1,000-plus respondents, while 47 per cent said they were worried about untrustworthy or suspicious websites.

Bits of Freedom
Bits of Freedom campaigns for internet user freedom and for an open and fair information society. The foundation influences policy and legislation by means of legal action, campaigning and lobbying in the Netherlands and Brussels. As a sponsor, we help to ensure that Bits of Freedom is able to work independently for privacy and freedom of communication.

TUCCR
The Twente University Centre for Cybersecurity Research (TUCCR) is an association of knowledge partners, experts, professionals, businesses, researchers and students working in the field of cybersecurity. The Centre works to reinforce the security and digital autonomy of our society. As one of the partners, we contribute to applied cybersecurity research, and we support other academic research undertaken within TUCCR. Our CEO sits on TUCCR's Management Board, while an SIDN Labs team member co-chairs the Centre's Network Security group. We also co-fund a PhD student who is researching the phenomenon of routing hijacks.

DINL
Digital Infrastructure Netherlands (DINL) is a vehicle through which various organisations work together to campaign for a strong digital infrastructure as the foundation of the Dutch digital economy and society. DINL helps governments, businesses and private citizens to make their way in the online economy, and shows how they can reinforce the Netherlands' position as an international digital leader. We were one of DINL's co-founders and partners. In 2024, we rejoined the foundation, and our CEO accepted a seat on DINL's board. Collaborating with other DINL members enables us to advance our shared views on a strong digital infrastructure more effectively within the political debate.

We are one of the founders and partners of the Digital Infrastructure Netherlands.

ECP | Platform for the Information Society
Within the ECP, member companies, governments, community organisations and knowledge centres collaborate to shape our digital society. As an ECP Partner, in 2024 we were involved in the Dutch Internet Governance Forum (NL IGF), the Internet Security Platform, the veiliginternetten.nl website, and the ECP Annual Festival. We were also involved with the ScamCheck tool, the Platform for Internet Standards and the further development of Internet.nl.

National Coalition for Sustainable Digitisation
In 2024, we joined the National Coalition for Sustainable Digitisation. The coalition is a public-private initiative dedicated to removing barriers to sustainable digitisation in order to reduce the environmental impact of – and arising from – the adoption of electronic technologies.

NLnet Labs
NLnet Labs is a non-profit organisation that develops free, open-source software for the DNS and BGP routing. The NLnet Labs team also undertakes research, develops standards and supports the internet community. We sponsor the important work done by NLnet Labs, and our CTO is a member of the organisation's Supervisory Board. NLnet Labs also partners SIDN Labs on various research projects, such as the contract research undertaken for the root server operators Verisign and ISC in 2024.

European Summer School on Internet Governance
As we have done for some years, we sponsored the European Summer School on Internet Governance (EuroSSIG): a non-profit organisation that provides an annual introductory programme for students, academics, businesses and government bodies. EuroSSIG helps them to understand global internet governance debates and broadens their knowledge of pertinent issues. In July 2024, the eighteenth edition of the summer school was held in Meißen, Germany.

Dutch Cloud Community

The Dutch Cloud Community is the trade association of the cloud and internet service industry in the Netherlands. The organisation protects the interests of its 100-plus members and gives them access to technical publications, knowledge sessions, market intelligence and legal advice. We are one of the Community's sponsors. In 2024, we had regular discussions with the Community's managing board on topics such as the media reaction to the proposed migration of our registration system.

Dutch Anti-DDoS Coalition

The Dutch Anti-DDoS Coalition is a public-private partnership of government bodies, internet providers, non-profit organisations, banks, internet exchanges and academic institutes. We are one of the Coalition's partners. The Coalition's 20 member organisations work together to minimise the societal impact of DDoS attacks by sharing knowledge, studying attacks that do occur and organising drills. In 2024, we were involved in the Coalition's Clearing House, Legal and Intel & Attribution working groups. We also participated in the annual national anti-DDoS exercise.

2STiC

SIDN Labs is one of the founders of 2STiC (Security, Stability, and Transparency in inter-network Communication). Within this community, we work with the other members to investigate extensions and upgrades to the internet infrastructure, including infrastructures such as SCION, which employ alternative architectures to increase the security of internet communications.

Liaison with the National Cyber Security Centre

The National Cyber Security Centre (NCSC) is part of the Ministry of Justice and Security, which works with partners to promote internet security in the Netherlands. As an NCSC liaison organisation, we contribute to its work by sharing our knowledge and connecting the NCSC with other partners.

"Once an image has been identified as illegal, it's given a unique digital fingerprint known as a 'hash'."

Yvette Velzeboer
Project Coordinator of Offlimits' Hash Check Service

SIDN supports the work of Offlimits

We're longstanding co-funders of the Reporting Hotline for Internet Child Pornography, operated by Offlimits. Through SIDN Fund, we've also supported various other Offlimits initiatives, including the Hash Check Service. Yvette Velzeboer, Project Coordinator of Offlimits' Hash Check Service: "Once an image has been identified as illegal, it's given a unique digital fingerprint known as a 'hash'. The hash is then added to a database and used for vetting subsequent uploads. If anyone tries to upload the same image again, it's immediately blocked. Affiliated actors, such as hosting service providers, can voluntarily check any image uploaded to their servers to see whether its hash is in the Hash Check Service database."

> Read more about the Hash Check Service

Innovating in pursuit of our societal mission

6 Developments at SIDN

In 2024, much of our attention was focused on our technical base. We restructured our ICT Department, for example, and renamed it SIDN Tech. Other dominant features of the year were the proposed migration to the public cloud and development of the new registration system in collaboration with CIRA. The technical changes and the public interest in our migration plans prompted discussion within our teams, as reflected in the feedback from our staff survey. We also enhanced the electronic accessibility of sidn.nl in line with the Web Content Accessibility Guidelines (WCAG).

ICT transition and IT sourcing strategy

On 1 January 2024, we adopted a new IT sourcing strategy and restructured our ICT Department, now known as SIDN Tech. The restructured department consists of 3 teams, each with its own focus: ICT & Security Operations, Software Engineering and Cloud Engineering. The teams have 5 primary tasks:

1. Maintaining the security of the .nl zone
2. Assuring the continuity of our services
3. Continuing the standardisation and streamlining of our processes and systems
4. Developing a new domain registration system
5. Migrating our registration application to the public cloud

The dominant feature of 2024 was the process that followed the announcement of the proposed partial migration of our registration system infrastructure to the public cloud platform operated by Amazon Web Services (AWS) in Europe. We assisted a quick scan of the Dutch and European cloud services markets commissioned by the government's economics ministry (EZ). We also arranged a Data Protection Impact Assessment (DPIA), and the General Intelligence and Security Service (AIVD) performed a risk analysis. Pending the outcome of the investigations in January 2025, we undertook to refrain from any irreversible action.

We are committed to retaining the management of .nl permanently in house, including development and management of our registration system, our primary DNS and our DNS anycast system. The .nl domain will always be operated for and from within the Netherlands. We are absolutely dedicated to ensuring that .nl is available at all times and that our data is secure. Our core resolving service and the associated DNS infrastructure will not be migrated to any public cloud platform operated by a hyperscale service provider. By using open standards and open-source technology, we will make our registration system as platform-independent as possible. Moreover, the database for the zone file will be hosted by a Dutch service provider. That database serves as the primary, authoritative and trusted source for the generation, signing and publication of the zone file via a Dutch service provider without using AWS. Our architecture and exit strategies are based on that principle, so that, if a suitable Dutch or other European cloud service provider is identified in the future, migration is relatively straightforward.

› Read about our proposed migration to the public cloud

Other activities that occupied us in 2024 included reinforcing the DNS infrastructure, by further increasing the capacity of our anycast platform for example. Punktum dk, registry for Denmark's .dk domain, also started making use of our platform. Technical improvements to the DNS infrastructure are vital for the security, availability and resilience of the .nl domain.

New registration system

In the first half of 2024, we obtained full access to the source code of the Fury Registry Platform of our partner CIRA. Using the existing platform as a basis, we worked with our colleagues at CIRA on the development of a new registration system called Hello Registry, which will be designed to utilise cloud technology. Our aim is to have .amsterdam, .politie, .aw and .nl running on the platform by late 2025 or early 2026. We are working closely with CIRA in other fields as well.

With CIRA, we're developing the Hello Registry platform, which will utilise generic cloud technology.

SIDN's data platform

Our data platform enhances the availability of data, both to registrars and to users within our own organisation. Registrars access the platform via the SIDN Insights portal. In 2024, we completed work on the platform's foundations and configured the reporting functions for our Support Department and others. We also prepared for interfacing with Hello Registry, so that the platform is ultimately able to process data from the new system as well. On the user side, we enabled access to additional data sources useful to .nl registrars.

Improving SIDN's electronic accessibility

We believe it's important that everyone, including people with functional disabilities, can access our products and services. We therefore organised an internal presentation and workshop for staff and developers to increase awareness of electronic accessibility, in relation to our websites and our other communication channels. We also worked with our service provider to make improvements to sidn.nl with the aim of complying with the WCAG.

The WCAG is a European law intended to ensure that all Europeans have access to online products and services by June 2025. The improvements included adding an accessibility statement to the website and giving visitors to sidn.nl a choice of 3 colour options.

We improved the electronic accessibility of sidn.nl for visitors with disabilities.

New constitution

In summer 2024, changes were made to SIDN's constitution, and to the articles of association of its subsidiary companies. Certain amendments were needed to bring the documents into line with the Management and Supervision of Legal Entities Act, whose provisions are intended to ensure the quality of the supervision and governance of entities such as ours. Following the changes, all SIDN's subsidiary companies have identical articles of association. The amendments to the constitution's foundation also included a number of substantive changes. However, our objectives and the rights of .nl registrars remain unaltered.

> Read more about the new constitution and articles of association on sidn.nl

Cyber-exercises and security activities

A proactive approach to cybersecurity is increasingly important. Especially in view of the constantly evolving and challenging nature of the digital landscape. SIDN was one of organisations behind formation of the European Top-Level Domain Information Sharing and Analysis Centre (TLD-ISAC) in 2023. The centre acts as a forum for collaboration amongst TLD registries with the aim of increasing cyber-resilience.

We also take part in the annual nationwide DDoS exercises held by the National Anti-DDoS Coalition. The Coalition's purpose is to investigate and counter DDoS attacks from various angles. Participation in the exercises helps us improve our threat preparedness. For our own personnel, we organised campaigns throughout the year to raise awareness of cyberthreats.

ISO 27001 certification

Certification under ISO 27001 is the gold standard for information security. In 2024, the annual external audit confirmed that we remain compliant with the standard. We also invested considerable energy into preparing for transition to the 2022 version of the ISO standard. The switch was originally planned for 2025, but was actually realised in 2024.

Transfer of Yivi to Privacy by Design

Yivi is a privacy-friendly platform that individuals and organisations can use to securely log in online, exchange data and sign or approve electronic documents. Our investment in Yivi over the last 5 years has resulted in a more professional, high-availability platform and a redesigned app that meets users' needs. The principles underpinning Yivi – privacy by design, open-source software and decentralised architecture – have also gained wider acceptance. Those principes are now more firmly established in the proposed Digital Government Act (Wdo) the have been adopted by the European Commission for use in the development of new European identity wallets.

In April 2024, a gradual transfer process concluded with Yivi's formal return to the control and ownership of the Privacy by Design Foundation. We remained temporarily responsible for the platform's technical management on behalf of Privacy by Design, while preparations were made for transfer to the Caesar Group at the start of 2025.

Workforce and sickness absence

During the year, we continued with the reorganisation of SIDN Tech. A number of staff members were given new roles, some of which were completely new to SIDN, such as the role of Cloud Engineer. We also welcomed a new Chief Financial Officer (CFO) and a new Public Affairs Manager. Improvements were made to our processes for preparing and inducting new recruits, and we reinforced our contacts with universities and colleges. Such contacts are important to our ability to fill entry-level vacancies and internship places. During the year, a total of 16 colleagues joined the workforce, while 20 left the organisation. We ended 2024 with 99 employees (90 FTEs). The sickness absence rate was 6.14 per cent, up from 4.9 per cent the year before. The rise was attributable to the level of prolonged sickness absence for non-work-related reasons.

Staff welfare

In 2024, we supported the welfare of SIDN staff in a variety of ways. For example, 59 per cent of our people had preventive medical check-ups with our occupational health service. The check-ups provide

insight into workers' physical and mental health and any associated absence risks. The results also serve as a basis for lifestyle advice. Other ways we promote staff wellbeing include making fruit available in the office and taking part in boot camps on the premises and physical activities during the SIDN weekend.

Staff survey

In 2024, we carried out a staff survey. We found that our people are positive about the atmosphere and cooperation within their own teams, but feel that collaboration and communication between teams could be better. The results also showed that job changes within SIDN Tech and the outside world's response to our proposed cloud migration had caused uncertainty and disquiet within the workforce. In addition, there was a general sense that the management was not listening to the staff as much as in the past. Various steps were taken in response, such as holding feedback sessions so that better use could be made of the expertise and views of staff members prior to management decision-making.

Professional development

We provide a comprehensive compensation and benefits package that includes a development budget. In 2024, more than 75 per cent of the budget for education and training courses was utilised. Courses on subjects such as data engineering, cloud engineering and cloud technology are made available via our learning management system. A total of 15 cloud technology qualifications were secured by staff members. In connection with our partnership with CIRA, we encourage our people to take English-language courses.

Personal sponsorship budgets

Every member of staff is allocated an annual personal sponsorship budget for donation to a good cause of their choice. In 2024, many of our people chose to donate to GIRO555, an appeal on behalf of victims of the fighting in Gaza and the Middle East. We matched their donations to bring the total given to €22,000. Other good causes supported by staff included the Royal Society for the Protection of Dogs, the Dutch Cystic Fibrosis Foundation, the Special Children Team and the Komma Foundation.

Privacy Board

As the operator of the .nl domain, we process personal data in order to continue increasing the security and stability of the .nl zone. We therefore have an internal Privacy Board, which reviews all data processing activities to make sure that they are responsible and performed with due diligence. The Privacy Board asks the owner of every new study, project or system to draw up a privacy policy, which is then submitted to the Board for review. All privacy policies and the associated Privacy Board assessments are published on our website. In 2024, the Privacy Board reviewed the privacy policy for RegCheck, the system that our Support Department uses.

› Read more about the Privacy Board on sidn.nl

Staff Council

Staff Council activities in 2024 included helping to organise the staff survey and to formulate the job profile for a prevention officer tasked with promoting the health and safety of our people. The Council's advice was sought regarding the formation and position of a new Security Team. In January and September, the Council met SIDN's Supervisory Board.

Outlook

ICT transition

The quick scan, DPIA and AIVD risk analysis were all completed in the latter part of 2024. On the basis of the results, at the start of this year the government decided to allow SIDN to proceed with migration of a smaller portion of the .nl registration system to the AWS public cloud, subject to strict conditions. In light of advice from the AIVD, we agreed with the economics ministry that various steps would be taken, primarily to ensure that .nl's availability does not depend on AWS. Key components of our services, such as the DNS zone file generator and signer and the hidden primary name server will be hosted by a Dutch service provider. Further implementation of the measures and preparation for the partial migration of our technical infrastructure will take place in close consultation with the economics ministry, the Dutch service provider in question, the RA and registrars.

We'll work with our registrars to set up a test environment for Hello Registry.

Future of the domain registration system

In partnership with CIRA, we will continue development of the shared registry platform. We intend to begin by migrating .amsterdam,

.politie and .aw from late 2025. The process will then be reviewed and optimised as necessary so that we can migrate .nl smoothly to Hello Registry in 2026 while assuring its uninterrupted availability. In 2025, we'll also work with our registrars to set up a test environment, so they can try out the new registration system before it goes live.

Technical management of Yivi

Yivi's technical management will be fully transferred to Caesar Group in 2025 for further development on behalf of Privacy by Design. We expect the process to be completed in April.

Staff satisfaction and employability

From 2025, we'll carry out a thorough staff satisfaction survey annually, and we'll do a quick scan once a quarter. The new approach is intended to aid the identification of opportunities for improvement and provide a better picture of what our people are concerned about, so that their views can be taken into account. The results will be used to further improve collaboration.

Learning management system

Implementation of the SIDN Tech training plan will be completed in 2025. The exercise will provide a better picture of the knowledge and training required in connection with migration to and use of cloud technologies.

Electronic accessibility of our websites

In 2025, we will ensure that the PDFs and forms on our websites are accessible for all visitors. The electronic accessibility of the SIDN Fund and C&AB websites will also be improved in line with the WCAG.

"We want everyone to have access to our products and services, including people with disabilities."

Nicole Wedler
Online Communications Consultant at SIDN

Improving SIDN's electronic accessibility

"SIDN's mission is problem-free, opportunity-rich digital living for EVERYONE. Naturally, therefore, we want our website to be accessible to everyone, including people with disabilities. So that our products and services are open to all.
And we've been making great strides recently towards our goal of ensuring that sidn.nl meets the highest global accessibility standards. With the help of the Accessibility Foundation, we've carefully analysed the electronic accessibility of sidn.nl. We're now working with our partner Us Media to improve the site in line with the findings.
Got feedback on the changes we've made, or ideas for further improvements? Drop us a line! After all, the best testers are real-life users. Mail your input to communicatie@sidn.nl."

> **Read more about how we're making sidn.nl more accessible**

Our Sustainable Development Goals

Affordable and clean energy

Good health and wel-being

Industry, innovation and infrastructure

Climate action

Quality eduation

Partnerships for the goals

Our impact on a sustainable digital society

7 Sustainability report

At SIDN, we aim to play our part in building a sustainable digital society. That implies working with customers, partners and suppliers to promote an opportunity-rich, secure and healthy living and working environment for everyone at SIDN and in the wider community. In our efforts to fulfil our sustainability ambitions, we are guided by the United Nations' Sustainable Development Goals (SDGs). We have selected the 6 SDGs that are most relevant to us, and in relation to which we can achieve the greatest impact.

SDG 3: Good health and well-being

SDG 3 is "Ensure healthy lives and promote well-being for all at all ages". Our impact in relation to this goal is described above in Section 6, together with our work on sickness absence and the promotion of preventive medical checks.

SDG 4: Quality education

SDG 4 is "Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all". Our impact in relation to this goal is described above in Section 6. For example, we promote professional development by giving each member of staff a training budget.

SDG 7: Affordable and clean energy

SDG 7 is "Ensure access to affordable, reliable, sustainable and modern energy for all". In support of SDG 7, we are committed to reducing energy consumption per FTE. In 2024, about 15 per cent of the electricity used at our offices was provided by our own solar panels. Our office building and our data centres also run entirely on renewable energy. In addition, we investigated the scope for generating energy for our offices by installing a wind turbine. Unfortunately, the cost of a wind turbine was found to be out of proportion to the amount of energy it would provide. We will nevertheless continue to monitor developments in this field. In another initiative, we joined discussions with the association of the proprietors of businesses on our business park about the possibility of collective energy generation and the long-term options.

Our office building and our data centres run entirely on renewable energy.

SDG 9: Industry, innovation and infrastructure

SDG 9 is "Build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation". In pursuit of this goal, we aim to reuse or recycle equipment and other materials wherever possible. At least 95 per cent of our equipment is recycled or reused, and we use office fittings made from recycled materials. Wherever new hardware is bought, we give preference to the most sustainable and circular options. A procurement specialist assesses equipment and materials procurement transactions above a threshold of €10,000.

A particular focus for 2024 was the catering for our offices, because it accounts for about 12 per cent of our total annual carbon emissions. We liaised with the contractor regarding possible ways of making the catering more sustainable, such as buying more local produce and offering products with a smaller carbon footprint. The various initiatives led to a drop of roughly 12.5 per cent in our catering-related carbon emissions in 2024.

We realised a drop of roughly 12.5 per cent in our catering-related carbon emissions.

SDG 13: Climate action

SDG 13 is "Take urgent action to combat climate change and its impacts". In line with SDG 13, we're working to reduce our carbon emissions per .nl domain name. One of our biggest challenges is home-work travel, which accounts for 41 per cent of our carbon emissions. We therefore operate a lease cycle scheme and provide business rail cards to encourage people to commute to the office by bike or by public transport more often. For journeys of less than 750 kilometres, we also have a policy of travel by train or electric lease vehicle rather than by air. Since 2024, only electric vehicles have been available to staff members who qualify for a company lease vehicle.

Furthermore, all the energy we use comes from renewable sources (see SDG 7), and on quiet days we close 1 or 2 floors of our office block, so that the lighting and climate control systems are not operating. In 2024, we introduced a waste separation policy to our offices. We also encourage water conservation, for example with stickers in the toilets. We now have an electronic screen in our foyer, providing information about water consumption and residual waste production at SIDN. Although our water consumption was already quite low, we managed to reduce it by a further 10 per cent in 2024. Our waste separation performance also improved.

SDG 17: Partnerships for the goals

SDG 17 is "Strengthen the means of implementation and revitalise the Global Partnership for Sustainable Development". In this field, our focus is on partnerships with a direct relationship to sustainability. Since 2024, for example, we've belonged to the National Coalition for Sustainable Digitisation. We're also in CENTR's Sustainability Mailing Group, whose members exchange knowledge about sustainability issues and work to build support for sustainability within the wider CENTR community. Finally, we partner MVO-Netherlands, the sustainable business network.

In 2024, we also prepared for the EU's Corporate Sustainability Reporting Directive (CSRD), which is expected to indirectly apply to organisations like SIDN from 2026. One of the CSRD requirements is reporting our environmental, social and governance (ESG) impacts.

Since 2024, we've belonged to the National Coalition for Sustainable Digitisation.

Outlook

Reframed pursuit of sustainability ambitions

We will continue to pursue our sustainability ambitions in 2025, but within the ESG framework. We will make our ESG impacts measurable by relating them to the SDGs. In 2025, we'll also tighten up our Key Performance Indicators (KPIs), targets and reporting methodology, to ensure that they remain both challenging and realistic.

Another objective for 2025 is to limit our carbon emissions to no more than 25 grams per domain name. That translates to a 75 per cent reduction relative to our reference year, 2019.

Marjet van Zuijlen
Chair of SIDN's Supervisory Board

8 Report of the Supervisory Board

The Supervisory Board (SB) oversees the organisation's strategy, policy and general operational position. For example, the SB monitors the strategy and the risks associated with our business activities, the design and effectiveness of our risk management and control systems, and the realisation of our objectives. The SB also acts as a discussion partner for the Executive Board, and as the Executive Board members' employer.

Meetings

In 2024, the SB held 4 ordinary meetings and 2 extra online meetings. The extra meetings were devoted to the detailed arrangements for implementation of the cooperation agreement made between SIDN and CIRA in October 2023.

Other items approved or adopted included the following:

- Annual Reports and Annual Financial Statements of SIDN and all its subsidiaries for 2023
- Annual reports of the SB, the Selection, Appointments and Remuneration Committee, the Audit Committee and the Security and Stability Committee, and the Executive Board's Annual Declaration, in the context of corporate governance
- SIDN's annual plan and budget for 2025

In connection with adoption of the Annual Financial Statement for 2023, the SB considered the risks associated with the business and the findings of the Executive Board's assessment of the design and performance of the internal risk management and control systems.

Before the April meeting, the SB spoke to the Chair and Director of the Board of the Registrars' Association (RA). Before the September meeting, the SB held discussions with SIDN's Staff Council. Later in the autumn, the SB performed its regular self-evaluation. The main topics identified by a survey were considered by the SB prior to the December meeting.

Members of the SB took part in the Strategy Consultation Group meetings organised by SIDN, as well as in other internal and external activities organised by SIDN.

Topics discussed

The partnership with CIRA was a fixed item on the SB's agenda. Topics considered by the SB in 2024 included how the collaboration with CIRA was to be detailed in a series of supplementary agreements. The SB authorised the Executive Board to go ahead and formalise the agreements. In the discussions, specific attention was given to:

- Governance of the partnership
- Safeguards concerning a possible future exit
- The focus on SIDN's implementation of the jointly developed registration system
- The decision to, the purpose of and the parameters for making registry services available to third parties in the future, in partnership with CIRA

In addition, the SB regularly considered the developments surrounding the public and political debate concerning SIDN's proposed partial migration of the registration system to the AWS cloud. The SB was given regular updates regarding those developments by the Executive Board. The SB was also involved with the developments, both in the meetings and through an ad-hoc committee.

Another topic discussed by the SB was the decline in the number of registered .nl domain names and the financial and other consequences of that decline for SIDN. In addition, the SB discussed improving the attention given to liaison with stakeholders, and SIDN BrandGuard was evaluated.

On the organisational front, the SB discussed the findings of the SIDN staff survey with the Executive Board. The SB also defined a new policy on Executive Board members' expenses.

At its scheduled meetings, the SB received regular feedback from the Audit Committee and the Security and Stability Committee, and discussed any relevant matters arising.

Committees

The Selection, Appointments and Remuneration Committee held several meetings in 2024. The annual performance evaluations of the Executive Board members were discussed. In addition, together with the Executive Board members, relevant SB members and (at some stages) the HRM Manager, the Committee interviewed candidates for the position of CFO. That vacancy was filled with effect from September 2024.

The Audit Committee met 4 times. All the meetings were attended by SIDN's CEO, interim CFO and, following her appointment in September, the new CFO. At the meetings, the Committee discussed matters including the Annual Financial Statement and Annual Report for 2023, the audit report and the analysis of the annual data with the Executive Board and the external auditor. In November, the Audit Plan for 2024 was also discussed with the external auditor. Other topics addressed included the budget for 2025 and the price indexation to take effect on 1 January 2025. The Audit Committee also discussed the 2025 procuration arrangements, the proposed new policy on Executive Board members' expenses, and the proposal that a new treasury policy should be developed in 2025. Finally, at each of its meetings, the Audit Committee discussed the interim financial data and its implications for the forecasts for the current financial year and beyond.

The Security and Stability Committee held 4 meetings in 2024. Following Olaf Kolkman's appointment with effect from 19 June, the Committee had 4 members. SIDN's CTO and CISO attended the meetings. Matters considered by the Committee included:

- The internal auditor's audit plan and findings
- The strategic risks that SIDN faces, the associated actions and progress
- Regular reporting to the Committee by SIDN
- Security developments
- ICT transition
- ISO 27001 recertification
- Developments surrounding the proposed partial migration of the registration system to the AWS cloud

In 2024, the SB had 2 ad-hoc committees. The committee set up in 2023 in connection with development of the partnership with CIRA completed its work in 2024. Made up of Gerben van Leeuwen and Dennis Raithel, the committee's role was to oversee (on the SB's behalf) the process of formalising detailed arrangements between SIDN and CIRA in a series of implementation agreements. In that role, the committee acted as a discussion partner for the Executive Board. It also prepared the necessary resolutions giving authorisation for conclusion of the agreements.

The second ad-hoc committee's members were Marjet van Zuijlen and Mark Frequin. Its role was to act as a discussion partner for the Executive Board. The committee also supported the executives in connection with the public debate and the involvement of politicians, ministries and the AIVD in SIDN's proposed partial migration of the registration system to AWS.

Membership

On 31 December 2024, the Supervisory Board had 8 members.

- Marjet van Zuijlen, Chair, also Chair of the Selection, Nomination and Appointments Committee
- Mark Frequin, Vice-Chair, also member of the Selection, Nomination and Appointments Committee
- Wim Hafkamp, also member of the Security and Stability Committee
- Olaf Kolkman, also member of the Security and Stability Committee
- Sandra Konings, also member of the Security and Stability Committee
- Gerben van Leeuwen, also Chair of the Security and Stability Committee
- Jeannine Peek, also member of the Audit Committee
- Dennis Raithel, also Chair of the Audit Committee

The following changes to the membership of the SB took place in 2024:

- Mark Frequin was reappointed for 2 years with effect from 1 April 2024, due to compelling circumstances*.
- Olaf Kolkman joined the Security and Stability Committee with effect from 19 June 2024.
- Jeannine Peek was reappointed for 1 year with effect from 1 July 2024, due to compelling circumstances*.
- Dennis Raithel was reappointed for 3 years with effect from 5 November 2024.

SB members must be independent, as provided for in SIDN's Constitution and the SB's Standing Orders. However, the current rules allow for the participation of one non-independent member. None of the members was deemed non-independent in 2024. Nor were any potential conflicts of interest reported by SB members.

Retirement and reappointment rota for Supervisory Board members

In accordance with Article 29 of the Constitution, SIDN has a retirement and reappointment rota for SB members. As of 1 April 2025, the rota is as follows:

	1st appointment	Latest permitted term end date	Committee membership(s)
Jeannine Peek*	1 July 2015	1 July 2025	Audit Committee
Wim Hafkamp	1 January 2023	1 January 2026	Security and Stability Committee
Mark Frequin*	1 April 2015	1 January 2026	Selection, Appointments and Remuneration Committee
Gerben van Leeuwen**	16 April 2021	1 July 2029	Security and Stability Committee
Dennis Raithel	5 November 2021	1 January 2030	Audit Committee
Marjet van Zuijlen	1 September 2022	1 January 2031	Selection, Appointments and Remuneration Committee
Sandra Konings	1 January 2023	1 January 2032	Security and Stability Committee
Olaf Kolkman	1 January 2024	1 January 2033	Security and Stability Committee

* *In March 2024, the SB decided to extend the terms of office of Mark Frequin and Jeannine Peek by, respectively, 1 year and 2 years beyond the normal limit, in order to prevent the Supervisory Board losing an excessive amount of its knowledge and experience.*

** *Gerben van Leeuwen's appointment was proposed by the RA. In accordance with Article 24, clause 3, paragraph c, of SIDN's Constitution, the RA will be consulted before the SB resolves on reappointment. In accordance with Article 24, clause 3, paragraphs a and b, of SIDN's Constitution, at the end of Gerben van Leeuwen's final term of office, the RA will be invited to propose a candidate to replace him, or will be consulted regarding a replacement proposed by the SB.*

9 Annual Financial Statement

Notes to the Annual Financial Statement

We aim to maximise the added value we provide while generating a responsible and justifiable positive result. Our financial policies are not therefore directed towards the maximisation of profit, but towards the maximisation of our contribution to society. The surplus from 2024 will be added to the foundation's equity capital. The equity capital includes a continuity reserve, as agreed with the Dutch government, the purpose of which is to support the object of the foundation. Part of the equity capital is also required for the migration of .nl to the Hello Registry platform in 2026 (see the section headed 'Outlook' for details).

Comparison with budget

The pre-tax result for the accounting year was a surplus of €2.3 million: considerably better than the budgeted pre-tax surplus of €22,000. The difference is accounted for mainly by personnel costs in the accounting year being €1.0 million below the budget figure, and other operating expenses being €0.9 million below the budget figure. The personnel costs were lower because fewer full-time posts were filled than anticipated in the original budget. That in turn was a consequence of a decision to use third-party services for certain functions, particularly functions for which SIDN does not have a long-term need. External staff hire costs were correspondingly higher than budgeted. Other operating expenses fell as a result of reduced expenditure on (online) marketing. Furthermore, the budget for 2024 assumed faster transition to the cloud. Growth in the foundation's deposit interest received in 2024 resulted in financial income €0.1 million higher than budgeted.

Comparison with 2023

The pre-tax result for the accounting year was €2.4 million higher than in 2023.
The improvement is attributable largely to the higher turnover and increased operational efficiency, but higher interest income also contributed. Whereas banks were still charging interest on deposited funds in 2022, they returned to paying interest in 2023, and the rates of interest rose further in 2024. The result before taxation was improved not only by the €2.6 million increase in net turnover (including €0.7 million non-recurring grant income) and the relatively small €0.3 million rise in operating costs, but also by €0.1 million from financial income and expenditure.

Within the operating costs, personnel costs fell by €0.9 million, while overhead costs rose by €0.5 million. For certain specialist roles, we used external personnel out of choice. That provides us with the flexibility needed to respond to incidents, developments and fluctuations in our systems management capacity requirements, as well as facilitating downscaling in appropriate circumstances. That in turn enables us to safeguard the continuity of our services and ensure that the availability of our core systems always remains very high and in accordance with our agreed service levels. The overhead costs were higher than in 2023, due mainly to the cost of external consultancy services required in connection with the cloud migration pathway, and to the outsourcing of certain services.

Taxes

As a consequence of the changes to our legal structure, corporation tax for the period to 28 February 2023 was calculated separately for each entity. On 1 March 2023, a unified fiscal entity came into being, and the corporation tax due in respect of the remainder of the year was therefore calculated on the basis of the consolidated result for SIDN Groep BV. On 1 January 2023, the Foundation for Internet Domain Registration in the Netherlands ceased to be liable for the corporation tax. The corporation tax liability takes account of modest tax-deductible expenditure. In 2022, we extended the settlement agreement with the Tax Service to cover the period 2021 to 2025. The corporation tax payable in respect of 2024 is €908,000.

Expenditure on activities and services

We believe it is important to be transparent about what we spend money on. We therefore make an annual assessment of the proportion of our expenditure attributable to activities and services under each of a number of headings. The figures for 2024 are presented below.

1. A valuable and value-based .nl domain

This heading covers mainly expenditure on activities linked to management and development of the .nl domain. The other forms of expenditure included are:

- .nl activities and research and development undertaken by SIDN Labs in support of our core task
- Discounts: direct debit and volume discounts
- Registrar Scorecard incentives
- Funding of projects for registrars and grant to the Registrars' Association (RA)

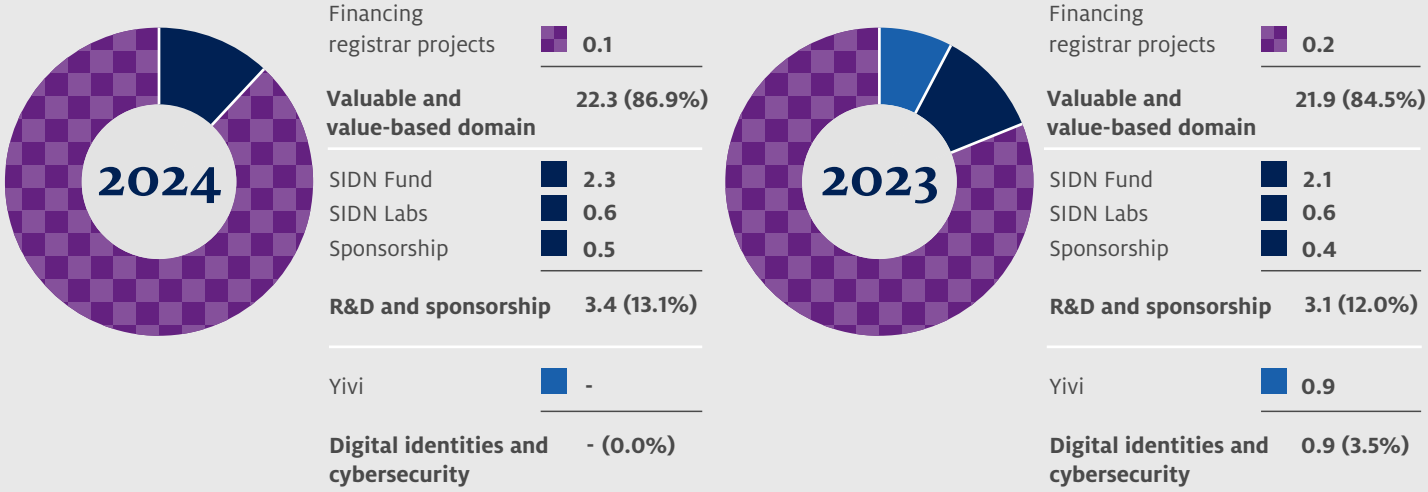
2. Research, development and investment in the internet community

The positive return on the operation of .nl is used for the benefit of the Dutch and international internet communities. This heading covers expenditure in that context, namely our funding of SIDN Fund, certain SIDN Labs activities, and other investment in the internet community. In 2024, investment in the internet community included support for NLnet Labs, ECP, Offlimits/Reporting Hotline for Internet Child Pornography and Bits of Freedom.

3. Digital identities

This heading covers expenditure on Yivi. With effect from April 2024, Yivi was transferred to the Privacy by Design Foundation.

Fig. 12 | Expenditure on activities and services, detailed breakdown (€m)



Financial policy

The fee charged to register a .nl domain name for 12 months was €4.15 in 2024, 10 per cent higher than in 2023 (€3.76). We found it necessary to increase registry fees for several years to come because of inflation and the need for investment in our ICT systems. The higher registry fees meant that our turnover rose by €1.9 million to a little over €25.6 million, despite a decline in the number of registered domain names in 2024. For the first time since SIDN's formation, the .nl zone c ontracted in size in 2024. Therefore, without the registry fee uplift, our turnover would have declined while our costs continued to increase.

The higher turnover and improved operational efficiency yielded a much improved operating result. The result is substantially higher than budgeted. However, it is appropriate, given the size of the contingency buffer required for 2025 and 2026, partly as a consequence of the non-recurring expenses we anticipate incurring in connection with the migration to Hello Registry.

On 1 January 2025, the fee charged to register a .nl domain name for 12 months rose to €4.25, a 2.5 per cent increase relative to 2024.

Outlook

Continuing inflation is expected to drive up our costs further in 2025. We also need to invest in the modernisation of our domain registration system. For the first time since SIDN was formed, the number of domain names fell in 2024, and we expect a further decline in 2025.
The migration to Hello Registry and AWS (which will take place mainly in 2025/2026) will mean that the residual book value held by our existing infrastructure and DRS-related assets at the time of decommissioning must be entirely written off in 2026. Depreciation charges will therefore rise considerably when we begin using Hello Registry. The combination of non-recurring expenses and structural cost increases mean that the outlook for 2026 is very different. In the interests of financial health and stability, we therefore needed to increase our registry fees by 2.5 per cent in 2025. The budgeted result for 2025, before taxation and interest, is a surplus of €357,000. The surplus is intended to cover unexpected expenditure relating to the migration to Hello Registry/AWS in 2025/2026.
Hence, by means of sound financial management, we expect our equity capital to remain stable.

Risk management

The Vanta risk management information system helps us to monitor risks and risk control measures. The monitored risks vary from IT risks, financial risks and fraud risks to statutory and regulatory compliance. Risks are periodically discussed with the Executive Board, the management and the SB, and the risk profile updated accordingly.
In the context of our risk management, we distinguish between soft and hard controls. Both types of control are vital to realisation of the organisation's objectives and management of the risks faced.

Hard controls

Hard controls are formal, structured measures implemented with a view to minimising risks and ensuring compliance with applicable legislation and regulations. They include automated controls within our IT systems, the enforcement of role demarcation in relation to payment traffic, salary payments and invoice authorisation and settlement, and detailed procedures that staff are required to follow. Such controls provide a substantive framework for the measurable control of risks and contribute to transparency and accountability within the organisation. The presence and effectiveness of our hard control measures are reviewed by means of internal and external audits.

Soft controls

Soft controls are less formal and intended to influence the culture of and behaviour within the organisation. They involve monitoring how staff and management handle risks, the advancement of certain ethics within the organisation and the promotion of an open communication climate. Our soft controls include leadership, training and the reinforcement of risk awareness within teams. They are very important for the development of a culture in which staff have a sense of responsibility for risk management and integrity. We expect all our personnel and anyone that acts on our behalf to have integrity. Integrity is vital in the context of our organisation's professional performance. The expected behavioural standards are also set out in our Code of Conduct. In addition, we have an internal Whistle-blowers' Charter, under which misconduct or irregularities can be reported to an external confidant.
The combination of hard and soft controls provides a solid framework for risk management and ensures that risk management is not merely an administrative process, but a responsibility shared throughout the organisation.
The presence of that framework enables us to identify and mitigate both internal and external risks, while also reinforcing our organisational culture.

Governance

Our Supervisory Board (SB) oversees SIDN's strategy, policy and general operational position. The SB pays explicit attention to risk management, which is scrutinised by the SB's Audit Committee and Security and Stability Committee.
The Security and Stability Committee supports the Board's supervision of the integrity, confidentiality and stability of our services, and of the system for monitoring compliance with applicable legislation, regulations and codes of conduct.
The Security and Stability Committee additionally oversees significant business risks relating to security and stability, paying particular attention to the findings of the annual internal and external audits, including the ISO 27001:2022 audit and the audit by the Dutch Authority for Digital Infrastructure (previously known as the Radiocommunications Agency), and to implementation of the ICT Roadmap and Security Roadmap.
On the SB's behalf, the Audit Committee supervises the integrity of the organisation's financial reporting, compliance with legislation and regulations and with applicable codes of conduct, and SIDN's financing arrangements.

Organisation

The management team is responsible for risk policy and risk tolerance, and for the direction of control measures. Where information security risks are concerned, we are supported by the Chief Information Security Officer. The work organisation is responsible for primary risk management and the associated reporting.
Since 2022, we have had an internal auditor and therefore a strong internal management system. The internal auditor tests the effectiveness of the management system and processes. When selecting audit subjects, the internal auditor refers to an estimate of the risk that a process is subject to insufficient control, resulting in under-utilisation of opportunities.
With a view to providing the management with additional assurance, a number of operational audits were performed in the year under review. Particular emphasis was placed on assessing the management system, internal control of information security processes, and demonstrable compliance with privacy legislation. In late 2024, DEKRA performed the annual audit for our certification under the ISO information security standard (ISO 27001). We passed the audit and thus successfully migrated to the 2022 version of ISO 27001.

Dealing with risks

Our risk policy involves the definition of parameters, standards and values with a view to maximising the effectiveness of our efforts to realise our objectives. We consider it important to operate transparently and with integrity.

Risks and risk tolerance

The most significant risks associated with our operations are identified below. Our risk tolerance in each area is defined on the basis of careful analysis. The defined risk tolerance then determines whether and to what extent a given risk should be taken. The risk tolerance definitions provide parameters for

Fig. 13 | SIDN's risk tolerance

Category	Risk	Low	Moderate	High
Strategic	Dependency on .nl		•	
Operational	Service availability interruptions	•		
	Breaches of the confidentiality or integrity of important data	•		
Financial	Solvency	•		
	Liquidity risk	•		
	Market risk		•	
	Currency risk		•	
	Interest rate risk		•	
	Credit risk		•	
	Bad debt risk		•	
	Damage claims and penalties	•		
Legislation and regulations	Risk of non-compliance with legislation or regulations	•		
Reputation	Reputation risk		•	
Equity capital requirement	Risk of equity capital falling below the defined minimum		•	

decision-making, control measures and course adjustments where additional intervention is needed to keep risks to the desired level.
The main risks and uncertainties in each area are described in the following paragraphs. The developments and control activities associated with each risk area are also summarised.

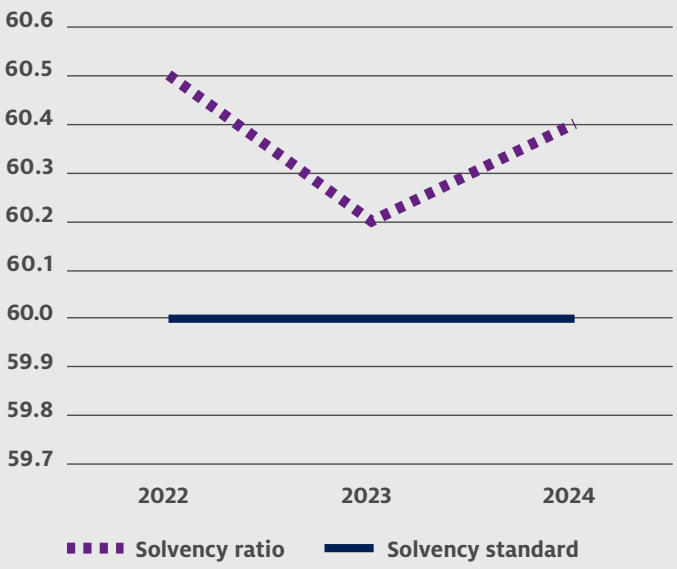
Strategic risks
The main risks associated with SIDN's strategy stem from the strong dependence on (earnings from) the .nl domain. Our .nl domain registration services are sold through registrars. We therefore work closely with the registrar community, as represented by the Registrars' Association (RA), on the promotion of .nl domain names and on continuous improvement of the security and quality of .nl.
The coronavirus pandemic proved to be a strong driver of growth in domain name registrations. However, growth subsequently plateaued, and the number of registered domain names even began to decline in 2024. In the next few years, we expect further contraction of the .nl zone. Given our limited capacity to influence the end market, our strategic risk tolerance is moderate.
We are seeking to increase our impact and extend the range of services we offer. In the field of Electronic Identities and Cybersecurity, we accordingly plan to continue investing in SIDN BrandGuard.

Operating risks
The main risks associated with our operating activities are interruptions to the availability of our services and breaches of the confidentiality or integrity of important data. Such problems could arise from technical and/or human error, or from deliberate (targeted or indiscriminate) human action.
A prolonged, large-scale problem in one of those fields has the potential to threaten the continuity of the organisation in 2 ways. First, by seriously damaging our reputation, giving rise to doubts in political circles and the community at large as to SIDN's legitimacy as the registry for the .nl domain. Second, by leaving us vulnerable to large compensation claims from clients. Since 2011, we have been ISO 27001-certified. In the context of our Information Security Management System (ISMS), we perform business impact analyses. That involves following an annual cycle in accordance with a defined information security policy. We also identify risks, implement control measures and assess residual risks. The findings, reports and internal and external audits are regularly discussed, e.g. in our Tactical Security Meetings, after which any necessary improvements are implemented. The outcomes are monitored by means of biannual management reviews. In that context, consideration is given to the results of the audits and performance assessments, as well as to the status of audit action points and any security incidents that may have occurred.
We assess the significance of each key process for service continuity by means of business impact analyses in the context of the ISMS. Our DNS services – the basis of the functionality of registered domain names – are the most critical, closely followed by our registration services, which enable users to register new domain names and to update and cancel existing registrations. Also rated as critical are the public Whois/Is, the Registrar Whois/Is, the power supply, our office ICT systems, our website www.sidn.nl, and our communication and telecommunication systems. With a view to assuring availability, integrity and confidentiality, we have put a wide variety of risk management measures in place, designed to minimise the likelihood of serious problems, and to enable swift corrective action and minimise impact if problems do arise. Our operating risk tolerance is low in relation to interruptions to the availability of our services and to breaches of the confidentiality or integrity of important data.

Financial risks

Solvency
Solvency is equity capital expressed as a percentage of the balance sheet total. Our solvency at the end of 2024 was 60.4 per cent (2023: 60.2 per cent), slightly higher than the norm value of 60 per cent. For several years prior to 2024, our equity capital had been declining as a consequence of budgeted deficits. In 2024, however, we generated a surplus. As a result, our contingency buffer remained adequate at roughly €3 million. We therefore expect our equity capital to remain stable, within the norm value range.

Fig. 14 | Solvency



Liquidity risk (including concentration risk)
Liquidity risk is the risk of having insufficient liquid assets to meet our obligations. The balance of our liquid assets at the end of 2024 was €28.5 million, down €0.9 million on the close of 2023 (€29.4 million). Our liquid asset balance is amply sufficient to cover our short and long-term finance needs. Concentration risk is addressed by having our liquid assets spread across 3 Dutch banks.

Market risk
Market risk is the risk of our government bonds and/or other securities decreasing in value. We intend to hold our Dutch and German government bonds until maturity. If circumstances should necessitate disposal of the bonds prior to maturity, we would face the risk of the bonds having lost some of their purchase value. Our holdings of other securities are at risk of declining in value. However, we have not detected any signs (trigger events) indicative of such an eventuality.

Currency risk
Currency risk derives firstly from the risk that our other securities are devalued by movement in the value of the Norwegian krone. Secondly, there is the exchange rate risk associated with transactions in currencies other than the euro. Our .nl services are priced in euros and therefore entail no currency risk. Because we make little use of suppliers that charge us in currencies other than the euro, our purchasing entails very little currency risk either.

Interest rate risk
Interest rate risk is the risk that our government bonds and/or receivable loans are devalued by movement in market interest rates. Because we intend to hold our government bonds until maturity, the associated interest rate risk is negligible.

Credit risk
Credit risk is the risk that a party with whom we have a contract defaults on their contractual obligations, as associated with other securities, accounts receivable and other receivables. Our bad debt risk is modest, because about 75 per cent of registrars pay by direct debit. Our General Terms and Conditions make provision for action to be taken if a registrar does not fulfil its financial obligations.

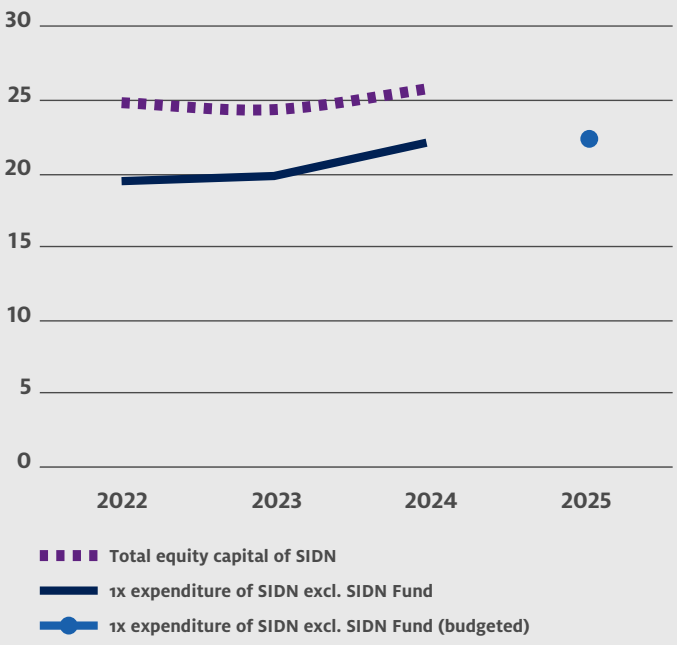
Damage claims and penalties
This is the risk arising from service interruptions and data confidentiality or integrity breaches. Our General Terms and Conditions limit or exclude our liability for such problems. Our risk tolerance in this field is moderate to low.

Legislative and regulatory risks
Changes to national or international legislation and regulations have the potential to affect our organisation and operating processes. We take stock of potentially significant proposed or impending legislative and regulatory changes – e.g. changes in employment law, tax law or information security law – at an early stage. The impact of any such change is assessed and translated into organisational adaptations, which are then implemented. The HR Manager and Legal and Policy Manager advise on risks relating to legislation and regulations. We have a Data Protection Officer and a Privacy Board, pursuant to the General Data Protection Regulation.
Our legislative and regulatory risk tolerance is low.

Reputation risk
With a view to managing reputation risks, we work closely with our stakeholders, including the .nl registrars, the RA and the Ministry of Economic Affairs and Climate Policy. Where the registrars are concerned, we pursue an active stakeholder-management policy through the RA. We attach great importance to the quality of our services and to the maintenance and elevation of service quality. In that context, we undertake an annual Registrar Satisfaction Survey. We also actively monitor our media coverage.

Contingency buffer
In order to assure the continuity of our organisation, it is important that we have an adequate financial buffer to protect against the possibility of losing a large portion of our income. The contingency buffer additionally serves to protect against the financial implications of the materialisation of an identified risk. Moreover, in the event of discontinuation, we would require sufficient funds to ensure the orderly winding up and/or transfer of our .nl activities.
Our minimum equity capital requirement is a sum equal to our annual expenditure. Our equity capital is currently above the defined minimum. Our Finance Department monitors the sufficiency of our equity capital in relation to the defined minimum and periodically reports its findings.
In view of the contingency buffer, the ratios, the budget for the coming year and the current situation within SIDN, we believe that it is appropriate that the Annual Financial Statement should be formulated according to the continuity principle.

Fig. 15 | Equity capital relative to contingency buffer (€m)



Fraud and irregularities
Our organisation manages communal capital. Our stakeholders may therefore expect us to make efficient, effective and legitimate use of our resources, and to account for that use. Fraud undermines that principle and is therefore unacceptable. The prevention of misconduct and fraud is vitally important for the assurance of an honest, secure and responsible working

environment. As well as harming SIDN's reputation, security and financial stability, misconduct and fraud undermine the trust of our staff, the government, customers and other stakeholders.

Our organisation has therefore taken various measures to prevent fraud and irregularities. Information regarding those measures is provided in the section on risk management, where our soft and hard controls are described, and elsewhere. The measures include operating a Code of Conduct, performing regular internal audits and having an internal Whistle-blowers' Charter, under which staff can report irregularities anonymously. In 2025, we will additionally introduce an external Whistle-blowers' Charter, and our fraud risk analysis will be integrated into Vanta, our risk management system.

The Executive Board and the Supervisory Board bear primary responsibility for the prevention and prompt detection of fraud. In 2024 and until the time of the compilation of this Annual Report and Annual Financial Statement, we had not detected any instances of fraud or any irregularities within our organisation.

Consolidated Annual Financial Statement 2024

Consolidated balance sheet as at 31 December 2024

Assets	31 December 2024 (in €)	31 December 2023 (in €)
Intangible fixed assets		
Intangible fixed assets under development	3,363,989	1,008,273
Software	447,052	183,058
	3,811,041	1,191,331
Tangible fixed assets		
Commercial property	4,384,912	4,613,717
Machinery and equipment	523,034	840,023
Other fixed business assets	372,424	516,439
	5,280,370	5,970,179
Financial fixed assets		
Participations in other group entities	3	-
Other participating interests	1,300,000	1,300,000
Receivables from other group companies	158,148	-
Other securities	1,386,229	622,436
	2,844,380	1,922,436
Current assets		
Receivables		
Trade receivables	728,524	736,259
Tax and social security contributions	-	18
Accrued income and prepaid expenses	1,561,880	1,306,420
	2,290,404	2,042,697
Liquid assets	28,479,022	29,362,816
Total	**42,705,217**	**40,489,459**

Liabillities

	31 December 2024 (in €)	31 December 2023 (in €)
Group equity	25,825,090	24,424,224
	25,825,090	24,424,224
Short-term liabilities		
Accounts payable	512,017	572,552
Tax and social security contributions	1,911,452	1,357,292
Accrued liabilities	14,456,658	14,135,391
	16,880,127	16,065,235
Total	**42,705,217**	**40,489,459**

Consolidated profit and loss account for 2024

	2024 (in €)	2023 (in €)
Net turnover	25,609,819	23,004,433
Total operating revenue	**25,609,819**	**23,004,433**
Cost of sales	63,439	111,558
Personnel costs	12,063,380	12,922,996
Depreciation and revaluations	1,630,451	928,342
Other operating expenses		
Accommodation costs	470,572	416,484
Operating costs	2,392,723	2,216,159
Selling costs	1,355,329	1,600,840
Office costs	741,508	705,184
Overhead costs	4,874,811	4,360,082
Total operating expenses	**23,592,213**	**23,261,645**
Operating result	**2,017,606**	**-257,212**
Interest receivable and similar income	326,122	166,891
Interest payable and similar charges	-34,597	-
Financial income and expenditure	**291,525**	**166,891**
Result before taxation	**2,309,131**	**-90,321**
Taxes	-908,266	-282,214
Result after taxation	**1,400,865**	**-372,535**

Consolidated cash flow statement for 2024

	2024 (in €)	2023 (in €)
Operating result	2,017,606	-257,212
Adjustment for depreciation	1,630,451	928,342
Movement in trade receivables	7,735	-549,377
Movement in other receivables	-255,442	617,792
Movement in trade payables	-60,535	137,992
Movement in other short-term liabilities (excl. liabilities to credit institutions)	875,427	415,833
Cash flow from operating activities	**4,215,242**	**1,293,370**
Interest received	326,122	166,891
Interest paid	-34,597	-
Profit tax paid	-908,266	-282,214
Cash flow from operating activities	**3,598,501**	**1,178,047**
Investments in intangible fixed assets	-3,836,562	-255,578
Divestments of intangible fixed assets	377,456	-
Investments in tangible fixed assets	-105,304	-540,702
Divestments of tangible fixed assets	4,057	5,535
Acquisition of non-consolidated companies	-3	-
Movement in other financial fixed assets	-1,007,939	-35,431
Income from securities	86,000	273,777
Cash flow from investment activities	**-4,482,295**	**-552,399**
Movement in liquid funds	**-883,794**	**625,648**

10 Directors and officers

Executive Board
Roelof Meijer (CEO)
Loek Bakker (CTO)

Special Advisors
Piet Beertema
Boudewijn Nederkoorn
Ted Lindgreen
Eddy Schuyer

Executive Board
Laura van der Bij (CFO)
Cristian Hesselman (Director of SIDN Labs)
Arjan Middelkoop (Commercial Director)

Staff Council
Jeroen Roosen (Chair)
Carolien Bruggeman
Chris Faber
Romana Siebers (Secretary)
Angelika Takes
Thymen Wabeke (Vice-Chair)

Complaints and Appeals Board
Doeke Kingma (Chair)
Elmar Besselink
Klaas Bisschop
Huib Gardeniers (Secretary)
Sylvia Huydecoper
Elisabeth Thole

Supervisory Board
Marjet van Zuijlen (Chair)
Mark Frequin (Vice-Chair)
Wim Hafkamp
Olaf Kolkman
Sandra Konings
Gerben van Leeuwen
Jeannine Peek
Dennis Raithel

11 Glossary

Abuse
Use of the internet for an inappropriate purpose. Common forms of abuse include sending spam, phishing and creating botnets.

Anycast
Global anycast is a proven and effective technology for spreading network load across multiple instances of seemingly the same server. The way it works is as simple as it is effective: a number of servers share a single IP address, making routers 'think' that they are all the same server. IP packets are forwarded to the 'nearest' point. Local anycast differs from global anycast insofar as a number of local nodes are created. A node is a computer or another device connected to a given network, which can only be approached locally. As a result, worldwide DDoS traffic cannot ever reach a local node. The only DDoS traffic that can reach the node is locally generated traffic, which is much easier to control. Local anycast is therefore an effective response to the risk of major DDoS attacks.

Artificial intelligence (AI)
Artificial intelligence, or AI for short, involves the use of computers to perform tasks that normally require human intelligence.

Autonomy
Autonomy means being able to decide for yourself how to behave, without being restricted, compelled or influenced by anyone else.

AWS
AWS stands for Amazon Web Services, a part of Amazon.com that provides web and cloud computing services.

Border Gateway Protocol (BGP)
The internet's main routing protocol, used for routing traffic between systems on the internet.

ccTLD
In full: country-code top-level domain. A top-level domain linked to a country, e.g. .nl (the Netherlands), .de (Germany) and .fr (France).

CENTR
An association for the registries that run ccTLDs, including SIDN. It is a forum for discussion about policies that affect ccTLDs and a conduit for communication between the ccTLDs and other parties involved in the internet's (further) development, such as ICANN. See also centr.org.

CIRA
The registry for Canada's .ca domain.

Complaints and Appeals Board (C&AB)
An independent body to which .nl registrars and registrants can appeal against certain types of decision made by SIDN. The C&AB also considers complaints asserting that a domain name's registration is inconsistent with public order or decency. See also cvkb.nl.

Cloud-native
Designed and built to fully utilise the distributed computing potential afforded by a cloud-based delivery model. Cloud-native applications benefit from the scale, elasticity, resilience and flexibility provided by the cloud.

DANE
DNS-based Authentication of Named Entities (DANE) is a protocol for the secure publication of public keys and certificates.

DDoS
A distributed denial-of-service attack is a concerted effort to make a computer, network or service unavailable to its intended user(s). DDoS attacks can be carried out in several different ways.

DKIM
DomainKeys Identified Mail (DKIM) prevents e-mail tampering. If the content of a mail message has been altered in transit, DKIM flags it up.

DMARC
Domain-based Message Authentication, reporting and Conformance (DMARC) is a system for telling mail servers what to do with suspect incoming messages. Servers might be advised to delete all such messages, for example, or to forward them to a particular address. DMARC also provides mail domain operators with information about scam mail supposedly sent from their domain.

DNS
Abbreviation of Domain Name System or Domain Name Server. The global DNS is the system and protocol used on the internet to translate domain names into IP addresses and vice versa.

DNSSEC
Domain Name System Security Extensions (DNSSEC) is a suite of extensions to the DNS protocol. It involves the use of cryptographic techniques to prevent cybercriminals diverting internet traffic to fraudulent websites without the users realising. The basic DNS protocol does not provide optimum protection against such threats.

Domain name
A name within the Domain Name System (DNS), the internet's naming system. A domain name such as sidn.nl is made up of several parts: the top-level domain, '.nl', and the second-level domain, 'sidn'.

Registrant
The person or organisation in whose name a domain name is registered. Only the registrant is entitled to receive SIDN's services.

Domain Registration System (DRS)
The system that we make available to .nl registrars for registering .nl domain names and managing existing registrations.

Data Protection Impact Assessment (DPIA)
A Data Protection Impact Assessment is a means of determining and analysing the privacy risks associated with a planned data processing activity, before any data is actually exchanged.

ECP
ECP, the Platform for the Information Society, is a vehicle for the business community, the government and social organisations to work together to support the use of ICT in Dutch society. See also ecp.nl.

ENTRADA
An open-source big data platform developed by SIDN Labs for the analysis of large volumes of DNS data. The database that ENTRADA uses contains more than 100 million DNS queries.

Dispute Resolution System for .nl Domain Names
Anyone who registers a .nl domain name is responsible for making sure that the registration doesn't infringe anyone else's rights. If a registration appears to infringe someone's rights, a dispute can arise. That can happen if, for example, the domain name makes use of someone else's brand name, trading name, personal name or organisation name. SIDN's Dispute Resolution System has been set up as a quick and affordable alternative to using the law courts to settle a dispute.

gTLD
Generic top-level domain: one of the main types of internet domain. Well-known gTLDs include .com, .org and .edu. The introduction of numerous new gTLDs, including .amsterdam, began in 2014.

Hosting service provider
A hosting service provider is a business that provides web hosting services, involving the provision of storage space, processing capacity and network traffic handling capacity on a web server. As well as providing website and e-mail hosting on a dedicated or shared server, nearly all hosting service providers also provide domain name registration services.

ICANN
The Internet Corporation for Assigned Names and Numbers is a non-profit organisation that performs a number of important tasks, such as assigning and specifying top-level domains, assigning domain names and allocating IP addresses. ICANN does not manage any domain names itself. That job is delegated to registries such as SIDN (.nl) and VeriSign (.com and .net). See also icann.org.

IETF
The Internet Engineering Task Force is an international community of network designers, operators, suppliers and researchers, which develops internet standards. See also ietf.org.

(Internet) extension
Another term for a top-level domain: the last part of an internet address, after the dot, e.g. '.nl' in 'sidn.nl'.

Internet governance
The development and application of shared principles, standards, rules, decision-making procedures and programmes that shape the way the internet is used.

Internet Governance Forum (IGF)
The Internet Governance Forum (IGF) is an annual gathering of governments, market players and non-governmental organisations, under the auspices of the United Nations. At the IGF, public policy issues are discussed with the aim of ensuring that the internet remains manageable, robust, secure and stable. The IGF does not define policy. See also intgovforum.org.

Internet Protocol (IP) address
A unique combination of numbers and/or letters. Every computer or server on the internet has an IP address, at which it can be found. If you visit www.whatismyip.com you can check the IP address of the device you are currently using.

IPv6
Every computer or server on the internet has an IP address, at which it can be found. Addresses are created in accordance with the Internet Protocol. IPv6 is the latest version of the protocol, which supports an almost infinite number of IP addresses. It has been developed to succeed IPv4 (version 4), because IPv4 addresses are running out.

ISP
An internet service provider (ISP) is a business that provides internet access services to other businesses or private individuals. Many ISPs also provide other services, such as e-mail, web hosting and spam filtering.

Malware
Any kind of malicious software, including computer viruses and worms.

Name server
A computer on the internet, which 'translates' a domain name into an IP address (a unique numeric internet address). The name server is part of the DNS.

Fake webshop
An internet site that looks like a normal webshop, but has actually been set up by fraudsters to trick people out of money and/or to steal data.

NL IGF
A joint initiative by the Ministry of Economic Affairs, SIDN and ECP. Its purposes are, first, to embed the conclusions of the international Internet Governance Forum (IGF) in national policy and, second, to ensure that the Netherlands has a voice and that Dutch issues are aired within the international IGF.

Notice-and-Take-Down Procedure
A voluntary internet industry code of conduct on dealing with reports of unlawful or illegal website content, such as child sexual exploitation material, plagiarised content, discriminatory content or content linked to the sale of illegal goods. The code describes the procedure for complaining about the content of a website.
A complaint should be addressed first to the provider of the offending content. If the provider cannot be contacted or refuses to take the content down, the matter may be taken up with the next party in the chain. The chain is as follows:
- Content provider
- Website provider (registrant)
- Website hoster
- Internet access provider
- SIDN (registry)

If all the other parties in the chain have been asked to take down the offending content but have not done so, SIDN can, in the last resort, disable the associated domain name.

NTP
The Network Time Protocol (NTP) is a protocol that interconnected computers use to synchronise their internal clocks with other computers.

Open-sourcing
A development philosophy based on making source material freely available to all. Open-source software is software whose source code is freely available, so that anyone may copy it, modify it or distribute it without having to pay for the privilege.

Phishing
A form of internet crime. It involves sending e-mails and setting up websites that look as though they come from or belong to well-known and trusted organisations, when in fact they are fakes. The forged messages and sites encourage people to part with information, such as log-in details and credit card details, which the criminals then use for their own purposes.

Polarisation
A process whereby people see the world increasingly in terms of 'us' and 'them'. Differences between different groups within society are amplified, leading to increasing social discord.

Post-quantum cryptography (PQC)
The development and use of cryptographic algorithms (usually with public keys) that are believed to be secure against cracking by a quantum computer; also known as quantum-proof, quantum-safe or quantum-resistant cryptography.

RegCheck
A system that assigns interpretable risk scores to new domain name registrations.

Registrar
An intermediary who acts for a registrant or prospective registrant in interaction with a registry. (The registry for .nl is SIDN.) Most registrars are hosting service providers, internet service providers or access providers.

Registrar Scorecard
An incentive programme for .nl registrars. Participating registrars can qualify for financial incentives by enabling modern internet standards such as IPv6 and DNSSEC for the .nl domain names in their portfolios.

Registry
In full: domain name registry. The register of all the internet domain names under a given top-level domain, or the organisation that manages that register.

Registry service provider
An organisation (typically a registry) that provides registry services for top-level domains delegated to other organisations. For example, we provide registry services for the .amsterdam and .politie domains.

Resolving
Responding to DNS queries.

Resolver
When you enter a web address (URL) into your browser's address bar, it is translated into the IP address of the relevant domain. The translation process is known as resolving, and the machine or software that does it as a resolver.

RIPE NCC
The Réseaux IP Européens Network Coordination Centre is the Regional Internet Registry (RIR) with responsibility for issuing IP addresses in Europe and the Middle East. RIPE NCC is one of the world's five RIRs, the other four being APNIC (for Asia and Australia), AfriNIC (for Africa), LACNIC (Latin America) and ARIN (for North America). See also ripe.net.

SCION
A new internet architecture designed to support route control, error isolation and the exchange of explicitly confidential information for end-to-end communication.

Sustainable Development Goals (SDGs)
The United Nations' 17 goals for making the world a better place by 2030. They serve as a global compass for tackling challenges such as poverty, education and the climate crisis. The goals were adopted by all 193 UN member countries in 2015, and apply to all countries and all people.

Security.txt
An internet protocol that standardises the use of a simple text file containing a website operator's contact details. The file is placed on the site's web server so that people such as ethical hackers and benevolent cyber-investigators can draw the operator's attention to issues they have detected. Adoption and use of the protocol ensures that issue reports go straight to the appropriate person or department.

Server
A powerful computer with a fast connection, which is set up to provide information. A web server is directly connected to the internet.

Service provider
A provider of internet-enabled services, such as internet TV or internet telephony. Some service providers also supply equipment for domestic networks.

Signing
DNSSEC works with digital signatures, known as 'private keys'. For effective security, DNS data needs to be signed with a digital signature and the signature needs to be checked ('validated') by the data user.

Spam
Unsolicited e-mail.

SPF
Sender Policy Framework (SPF) is a technology for preventing mail 'spoofing' (sending mail pretending to be from someone else). With SPF, the authenticity of mail senders is checked.

StartTLS
A protocol for establishing secure connections between sending and receiving mail servers.

TLD
Abbreviation of top-level domain. The domain whose name forms the last part of an internet address, after the dot. For example, 'nl' in the domain name 'sidn.nl'.

Top-level domain
The domain whose name forms the last part of an internet address, after the dot, e.g. '.nl' in 'sidn.nl'.

Typosquatting
A form of internet abuse that takes advantage of the fact that people sometimes make slips when typing web and e-mail addresses. A user who mistypes an address lands on the typosquatter's site. Typosquatting is often associated with malicious activities such as phishing.

Validation
DNSSEC works with digital signatures, known as 'private keys'. For effective security, DNS data needs to be signed

with a digital signature and the signature needs to be checked ('validated') by the data user.

Registrars' Association (RA)
Association that speaks for the .nl registrars in their relations with SIDN and regularly discusses the main features of registry policy with SIDN.

Whitelisting
Whitelisting means putting things on a 'trust list'. For example, you can whitelist IP addresses whose traffic can be trusted for forwarding.

Whois
A protocol for retrieving the details of a domain name, e.g. the name and address of the registrant and registrar, from a database. SIDN manages the Whois data for all .nl domain names. See sidn.nl/whois.

WIPO Arbitration and Mediation Center
An independent, international non-profit organisation that arbitrates in domain name disputes and other cases. See also wipo.int.

Yivi
Yivi provides a privacy-friendly way to log in with service providers. First, the user 'populates' the Yivi app with validated data, or 'attributes'. Then, when the user accesses a service, the app passes on only the information about the user that the service provider actually needs. So data sharing is kept to the minimum, and the user stays in control of what they share with whom. Yivi was previously known as IRMA. The name was changed in 2022.

Zone file
A text file listing all the domain names in a zone, plus the associated web server IP addresses.

Publisher
SIDN
Meander 501
6825 MD Arnhem The Netherlands
P.O.Box 5022
6802 EA Arnhem The Netherlands
+31 (0)26 352 55 00
communicatie@sidn.nl
www.sidn.nl
www.sidnlabs.nl

Concept and design
Lumen Ontwerpersnetwerk

Text
Kilay Brands

Translations
G & J Barker Translations

Copyright
©SIDN
Text and figures from this report may be reproduced, but we ask that you credit us as the source. Please also let us know of your intentions in advance by mailing communicatie@sidn.nl.

Colophon