Deloitte-NL

Factsheet Risk & Security

Deloitte-NL & Deloitte Dutch Caribbean are ISO27001 certified. Cyber & physical security is anchored in this norm.

Deloitte-**NL** uses its own data centre in Amsterdam that uses a mirrored active-active design. All essential customer data is stored in this data centre. In addition, a third storage is utilised in Rotterdam. We also use MS and Amazon Cloud services.

Deloitte -NL is ISO27001 certified. Together with all other Deloitte member firms in the world, we use the same ISO27001 standard.

Deloitte-NL

Factsheet Risk & Security

Deloitte Cyber Security Strategy Identify measures

Policies and Standards
Asset & Configuration Management
Information Classification & Labelling
Compliance reporting
Threat Analitics

Policies and Standards

All Deloitte member firms are ISO27001 certified for the full scope. Certificates and statement of applicability can be send when requested.

Asset & Configuration Management

We use tooling to inventory all assets. Managing asset tools are being implemented.

Information Classification & Labelling

Data client data is classified confidential, also we use separate classifications for highly confidential internal and external data.

Discovery Scanning

All servers are scanned for compliance. Compliance is in line with the international CVC code. Deloitte uses a 24u implementation strategy for CVC 8 and 9 codes.

Pentesting

External environments are tested annual and are bi-monthly tested with our own HaaS (Hacking as a Service). The same service we offer to our clients. Applications are tested annually.

Vigilant Shield

Applications are inspected for vulnerabilities and analyzed for security flaws. All major released are run through the Vigilant Shield process.

Deloitte-NL

Factsheet Risk & Security

Threat intelligence service

Predict and prevent increasingly sophisticated attacks before they become a real threat by expanding sources, analysis, and applications to secure defenses, introduce cyber analytics tools and techniques and integrate with Brand Protection monitoring team activities (e.g. social media monitoring). Deloitte uses sophisticate tooling and manual research to perform threat intelligence on a Global scale.

GDPR

Deloitte is compliant to the European data privacy legislation GDPR. Also suppliers from outside Europe are held to this. Important for our suppliers is that privacy data is stored on European soil.

Vendor risk assessment

Vendors are assessed on annual basis to protect against unjustified risk.

Regionalized security

Global security strategy is the norm and regional where required. Local security is only used as last resort.

Cyber risk management, metrics and reporting

We use standardized programs for security metrics, benchmarks and reporting, security audit/compliance and security risk and real-time state of cyber security dashboard across Deloitte and its member firms.

Cloud risk management

Allows to safely use existing and emerging cloud technologies by the use of cloud security architectures, standards, and use models and CASB technologies.

Deloitte-NL

Factsheet Risk & Security

Deloitte Cyber Security Strategy Protective measures

Identity Management
Access Control
Authentication
Authorization

Identity Management

- Microsoft identity manager is used to manage the user accounts. Administrator accounts are handled separately and are stored in the Thycotic Privileged Access Management solution when not used.

Access Control

- At the moment MS-DA tunneling is used. We plan to implement Global VPN services via our F5 systems.
- Laptop and server endpoint protection.
  - Standard Removable Media Protection capability to force encryption and/or stop data transfer to portable media.
  - User training materials to member firms to educate staff on portable media protection measures.
  - Blocking user access to malicious websites.
  - Used tools like OpenDNS, Bluecoat proxy, monitoring agents (for blocking/restricting user access to malicious websites).
- Conditional access
  - Allows for access to cloud services based on conditions like managed devices and locations, depending on the risk the authentication controls can be elevated.
- Cloud access security broker service
  - Allows to safely use existing and emerging cloud technologies by cloud security architectures, standards.
- Network segregation & zoning
  - Network segmentation is used to reduce change of server and storage compromise by implementing layered access to the true data source.
- Privileged Access Management Service
  - Implemented to protect systems and network from suspicious activity of unauthorized users by managing and monitoring administrative/super-user accounts.

Deloitte-NL

Factsheet Risk & Security

- System hardening
  - OS, applications and endpoints are hardened to limit exposure to abuse.
- VIP cyber security
  - Defense against cyber risks targeting our executives by monitoring cyber risks facing our senior executives.
- Global firewall implementation
  - Perimeter, Intranet and GWAN firewalls on a Global level with member firm wide common implementation.
- Encryption and key management
  - Compliance with a global encryption and key management standard, registration of certificates and private key.

Authentication

Two factor authentication is applied on high risk systems now and all other eligible systems and services in process.

Authorisation

- System & Application certification.
  - A standard set of best practices, default configurations and review process of any new system or major change on an existing system. The certification is to ensure the system/service is build secure by design and regularly reviewed to ensure this is still the case.
- Endpoint content filtering
  - Used to reduce the risk of brand damage and loss of confidential information by blocking user access to malicious websites.
- Patch management
  - Centralized global patch management provides global compliance with the latest updates.
- Physical environment protection
  - Gates, access identification and authorization. CCTV and building security are implemented on all locations. Pass back and tailgating protocols are implemented.
- Enterprise Rights Management
  - Increased protection of electronic information by use of Azure IP for Enterprise Rights Management.

Deloitte-NL

Factsheet Risk & Security

- Confidentiality culture awareness
  - protection of our data by providing enhanced training and tools.
- Mobile device management
  - Use of InTune MDM to enroll and manage mobile devices. Supported conditional access for Internet facing services. Also BYOD devices are enrolled using MDM to enforce security policies.

Deloitte-NL

Factsheet Risk & Security

Detecting measures

Security Monitoring

Intrusion Detection

Behavioural Analytics

Vulnerability management

Weekly scanning of our systems to discover non compliances on basis of used cases coordination on Global and local level.

Enhanced threat protection

Expanded intrusion prevention services (IPS), monitor internal networks using the use of other monitoring tools.

Intrusion detection service

Operation intrusion detection on NL domains, other domains to be processed.

Insider threat

The environment is tested yearly by a red team (hacking service) to discover new threats and test existing ones. The results are used to further harden security.

ATP (advanced threat protection)

ATP is used to do behavioral analytics. This tooling is more powerful than a simple virus scanner because it also detects zero day malware.

Deloitte-NL

Factsheet Risk & Security

Respond & Recovery measures

Incident response

Security operation

Business Impact

Disaster recovery

Global and Netherlands/Dutch Caribbean Incident response

Detect and counter external and internal suspicious activities with tight integration of Intrusion Detection Service, Threat Intelligence, and Security Operations Center services and tools

Security operation centre service

Global log collection and Security Incident and Event Monitoring. 24x7 investigation response to identified security alerts

Business impact

Extensive business continuity program with annual testing and bi-annual testing for severe crisis situations from a board operated national response team.

Disaster recovery

The data centre is tested annual for disaster recovery. E.g. power outage. Extra measures are taken for essential (client) data at an off-site backup location.

Deloitte-NL

Factsheet Risk & Security

Contacts

NL Deloitte 5.1.2e @deloitte.nl