Information Security Management System

Implementation of ISO 27001 in IMSM of State Data Agency (Statistics Lithuania)

STATISTICS LITHUANIA
STATE DATA AGENCY

Vadimas Ivanovas
Head of State Data Governance Information System division
State Data Agency (Statistics Lithuania)

Overall IT security context in State Data Agency

STATISTICS LITHUANIA
STATE DATA AGENCY

Security context in the State Data Governance Information System

- Collect and store personal and companies data for statistical purposes.
- Our State Data Governance Information System ingests and exports data from a large number of datasets from other organizations information systems.
- Our data processing solutions help organizations, such as municipalities or hospitals, to make data-driven decisions.
- The data from our Information System is published on the web.
- Many datasets are transformed to open data – into National Open Data portal.
- Our Information System also features sandbox projects where other governmental organizations can make their own analysis using the integrated data and tools available within the system.

STATISTICS LITHUANIA
STATE DATA AGENCY

Continuous development of State Data Lake

- In the last three years, an established and functioning state data lake ecosystem has been created, with integration with over **115** state information **systems**/resources.
- Approximately **300 more systems**/resources will be integrated in the coming years.
- State Data Agency also develops internal applications for operational data and external public dashboards.
- Currently, our information system has nearly **2500** internal and external user accounts, with number of roles, and responsibilities

The scope of Information Security Management System (ISMS) in State Data Agency

- There is a constant need of robust ISMS risks related to:
  - large number of heterogenous systems
  - sensitive personal and health data
  - relatively large number of projects
  - relatively large number of users
  - complexity of data processing
  - other risks, related to IT technologies (web security, viruses, soc engineering, physical security, etc.)

It‘s necessary to protect confidentiality, integrity, and availability of information in the State Data Governance Informations system.

STATISTICS LITHUANIA
STATE DATA AGENCY

Maintenance of ISMS

STATISTICS LITHUANIA
STATE DATA AGENCY

Leadership

Top management shall demonstrate leadership and commitment with respect to the information security management system.....

Information security policy of the State Data Governance Information System (#1-6)

1. Conduct activities, taking into account the key principles of information security – confidentiality, integrity, and availability, to protect the information provided by respondents and other interested parties;
2. Manage data, create and develop data management processes, adhering to personal data protection requirements;
3. Ensure the secure collection, processing, and dissemination of statistical data and the statistical information;
4. Ensure the continuity of the State Data Governance Information System's operations, vulnerability management, and protect its data from unauthorized disclosure or distribution without permission;
5. Aim for the implementation of the set security assurance goals of the State Data Governance Information System;
6. Develop the information security skills of the State Data Agency's employees;

Information security policy of the State Data Governance Information System (#7-11)

7. Participate in cybersecurity exercises and training at various levels;

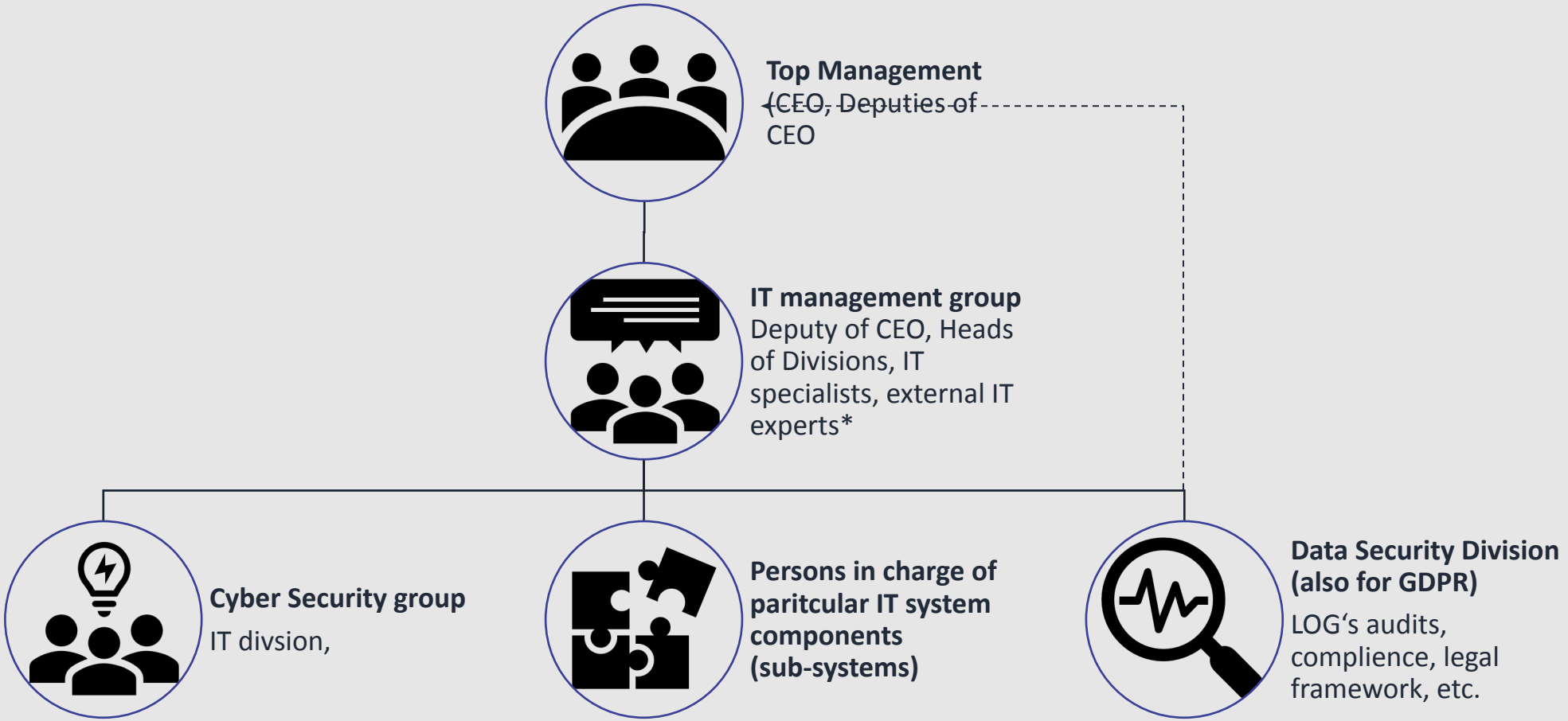
8. Continuously update technical measures used to ensure information security, allocate other resources necessary for the proper functioning of the information security management system;

9. Ensure a continuous security management cycle of the State Data Governance Information System, conducting an annual security audit of the State Data Governance Information System;

10. Continuously improve the information security management system and its effectiveness, ensuring compliance with the LST EN ISO/IEC 27001:2017 standard and other requirements set for the State Data Agency;

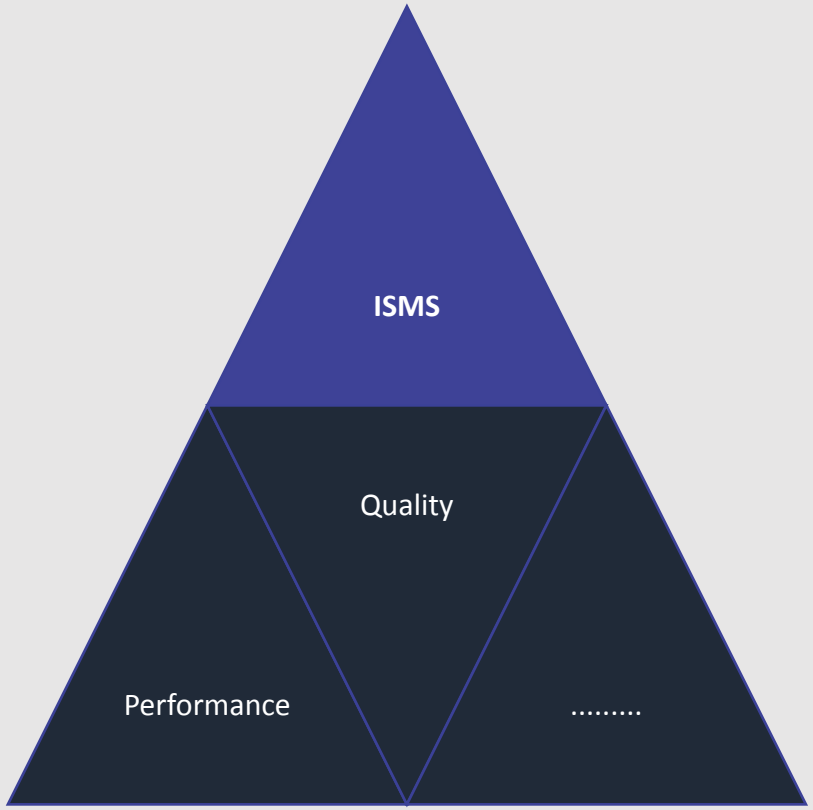
11. Strengthen international and inter-institutional cooperation in the field of information protection, actively participate in the activities of the European Statistical System and other international organizations on this issue.

Hierarchy and structure of realization of ISMS



KPIs of ISMS within the Overall KPI system

1. Uninterrupted availability of public electronic services ensured, %;
2. Continuous availability of internal electronic services, %;
3. The number of cases of long-term failures of public electronic services;
4. The number of unfixed vulnerabilities during the reporting period;
5. Information security incident resolution time compared to average resolution time;
6. The number of information confidentiality violations
7. Change in the results of the assessment of legal compliance
8. Impact of cyber incidents on the Information system performance



Measurement plan of performance, quality and information security indicators

STATISTICS LITHUANIA
STATE DATA AGENCY

Support

Resources, Competence, Awareness, Communication, Documented information

Documentation

There are more than 17 documents some of them are:

1. Summary of Cybersecurity Assurance Measures for Employees
2. State Data Agency's Information Security Policy
3. Change Management Procedures for Applied Software of ISMS
4. SDG IS Information Classification Procedures
5. Information Security Incident Communication Plan
6. ISMS Guide
7. Internal Audit Procedure Description for ISMS
8. Cyber Incident Management Plan for SDG IS
9. Risk Assessment Rules
10. Procedures for Reviewing the Appropriateness of Rights Granted to SDG IS Users Against Their Functions
11. SDG IS Data Security Provisions
12. SDG IS Rules for Secure Electronic Information Management
13. SDG IS End-User Obligations for Data and Information Protected by Ownership Rights
14. SDG IS User Administration Rules
15. SDG IS Business Continuity Management Plan
16. Rules for the administration of users of the SDG IS

Competence and awareness

- Documentation itself – every new employee must read key documents:
  - SDG IS Business Continuity Management Plan
  - SDG IS Rules for Secure Electronic Information Management
  - SDG IS End-User Obligations for Data and Information Protected by Ownership Rights
  - SDG IS Data Security Provisions
- Monthly information bulletins/one-pagers (about Cyber threats and GDPR)
- Mandatory additional learning courses (including tests) on the internal learning platform.
- Participation in National cybersecurity trainings organized by the National Cybersecurity Center (at least 2-3 times per Year).

STATISTICS LITHUANIA
STATE DATA AGENCY

Communication

- Dedicated VirusBox email for informing about suspicious emails.
- The push emails to the entire organization regarding recognized threats and suspicious emails, along with provided instructions.
- Monthly information bulletins/one-pagers about Cyber threats and GDPR.

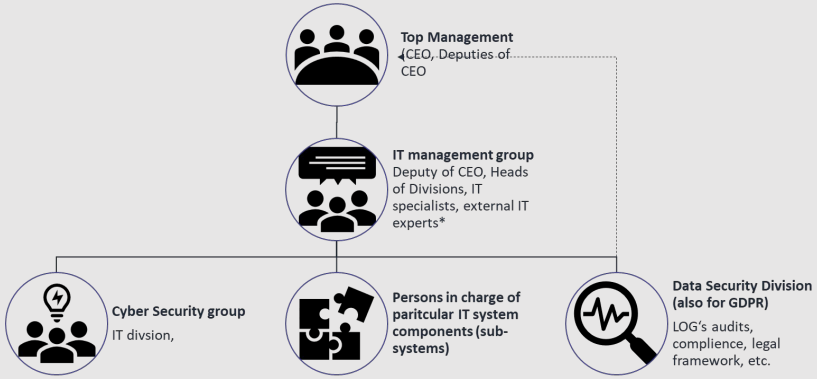
Resources

Personel:

- Data Security Division (4):
  - Data security officer;
  - GDPR lawyer;
  - LOG‘s analyst;
- IT department (7):
  - DB administrators;
  - Helpdesk team;
- SDG IS division (3):
  - LOG‘s analyst
  - DB adminstrators

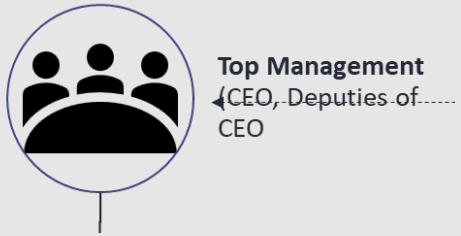
IT infrastructure and software:

- WiFi management;
- VPN;
- Incidents registration and helpdesk;
- Remote personel PC and mobile devices management;
- LOG analysis;
- .....

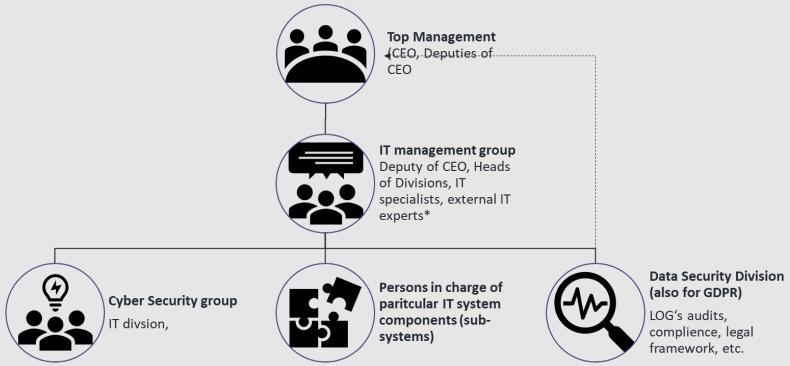


Main Roles and Responsibilities

Top Management



Approves a budget and main change of ISMS



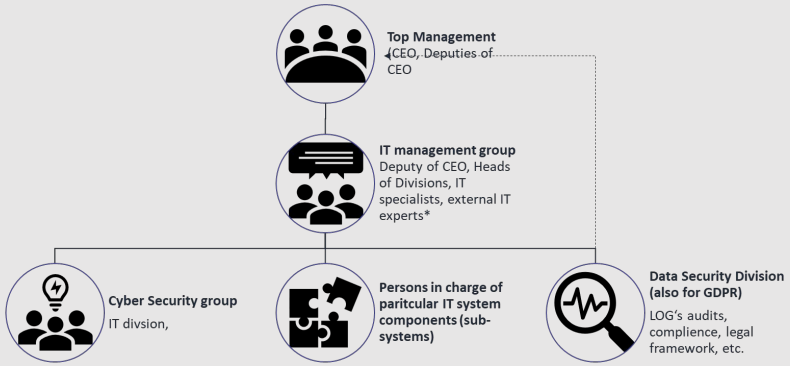
IT management group

IT management group
Deputy of CEO, Heads of Divisions, IT specialists, external IT experts*

Supervises the maintenance of ISMS processes;

Plans, coordinates, approves the implementation of necessary improvements in ISMS processes;

Prepares and controls a budget for investments in ISMS;

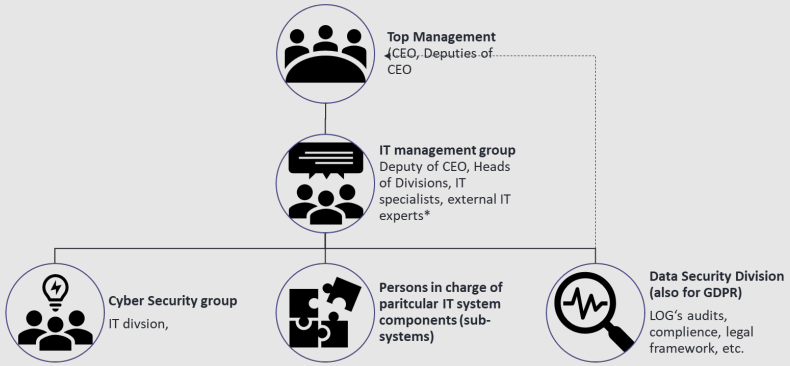


Cyber Security group

Coordinates information security measures in SDG IS:

- controls processes;
- coordinates the resolution of IT security incidents;

Prepares a plan for the improvement of cyber security measures and submits it to the IT management group for approval



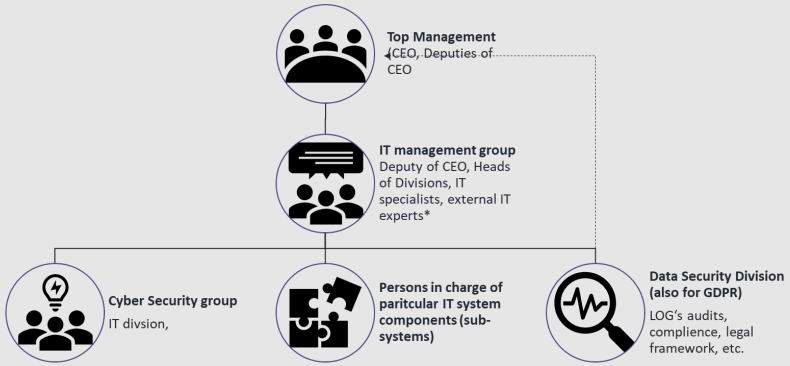
Data Security Division

Controls compliance with GDPR and other legal acts applicable to information systems;

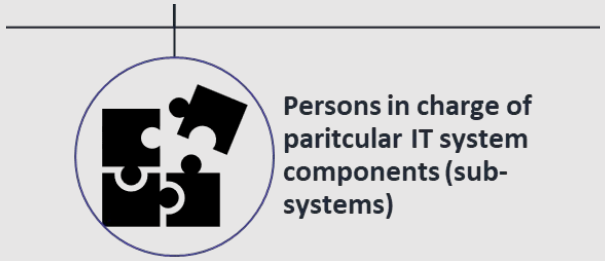
Involved in determining user access rights model;

Maintains and keeps up to date the main ISMS documentation;

Performs users actions log analysis;



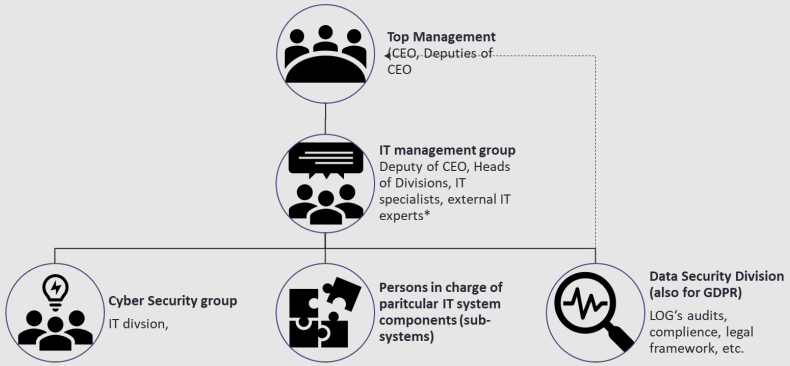
Supervisors of subsystems of SDG IS



Controls the adherence to processes in the subsystems for which they are responsible;

Improves proceses in the supervised subsystem;

Prepares a plan for the improvement of supervised subsystem and submits it to the IT management group for approval;



STATISTICS
LITHUANIA
STATE DATA
AGENCY

STATISTICS
LITHUANIA
STATE DATA
AGENCY

We are grateful for the opportunity to participate in the Twinning project, and we hope that this mission will enhance IT security in our organizations.