SGS

Management System Certification
Audit Summary Report
Certifikácia systému riadenia
Súhrnná správa z auditu

Organization: Organizácia:	Tepláreň Košice, a.s. v skratke TEKO, a.s.				
Address: Adresa:	Teplárenská 3, 042 92 Košice				
Standard(s): Norma(y):	ISO/IEC 27001:2013 System documentation		Accreditation Body(s) / Akreditačný orgán): UKAS		
Representative: Kontaktná osoba:	Mária Marcinová				
Site(s) audited: Auditovaná prevádzka (-y):	Košice, SR		Date(s) of audit(s): Dátum auditu:	19.06.2020	
EAC Code: EAC kód:	25, 27	NACE Code: NACE kód:	40, 41	Technical Area code: Kód technickej oblasti:	ISBC5
Effective No.of Personnel: Počet zamestnancov:	364		No. of Shifts: Počet zmien:	4	
Lead auditor: Vedúci auditor:	Róbert Bodnár		Additional team member(s): Ostatní člen(ovia) tímu:	-	
Additional Attendees and Roles: Ďalší účastníci a funkcie	-				

1. Audit objectives/ Ciele auditu

The objectives of this audit were:
To determine conformity of the management system, or parts of it with audit criteria and its:

- *ability to ensure applicable statutory, regulatory and contractual requirements are met,*
- *effectiveness to ensure the client can reasonably expect to achieve specified objectives, and*
- *ability to identify as applicable areas for potential improvement.*

Cieľom tohto auditu bolo:
Určiť zhodu systému riadenia alebo jeho častí s kritériami auditu a jeho:

- *schopnosť preukázať, že spĺňa príslušné zákonné, regulačné a zmluvné požiadavky,*
- *účinnosť zaručiť, že klient môže celkovo očakávať dosiahnutie stanovených cieľov a*
- *schopnosť identifikovať vhodné oblasti pre potenciálne zlepšenie.*

2. Scope of certification/ Predmet certifikácie

Production, sale and distribution of heat and electric energy.
Statement of applicability issued on 22.5.2018.
Exclusions: None

Výroba, predaj a distribúcia tepelnej a elektrickej energie.
Vyhlásenie o aplikovateľnosti vydané 22.5.2018.
Výnimky: Žiadne

Has this scope been amended as a result of this audit? *Zmenil sa predmet certifikácie na základe tohto auditu?*	☐ Yes / Áno	☒ No / Nie
This is a multi-site audit and an Appendix listing all relevant sites and/or remote locations has been established (attached) and agreed with the client. *Toto je audit vykonaný na viacerých prevádzkach a príloha uvádza všetky relevantné prevádzky a/alebo vzdialené sídla a odsúhlasené klientom. (pozri prílohu).*	☐ Yes / Áno	☒ No / Nie

For integrated audits, confirm the current level of the client's IMS integration:
Pre integrované audity, potvrdiť aktuálnu úroveň integrácie klientovej IMS:
☒ N/A/ *neaplikovateľné* ☐ Basic/*základná* ☐ High/*vysoká*

3. Current audit findings and conclusions/ / Súčasné zistenia a závery z auditu

The audit team conducted a process-based audit focusing on significant aspects/risks/objectives required by the standard(s). A sampling process was used, based on the information available at the time of the audit. The audit methods used were interviews, observation of activities and review of documentation and records. The structure of the audit was in accordance with the audit plan and audit planning matrix included as an annex to this summary report.

Audítorsky tím vykonal audit procesov zameraný na dôležité aspekty/ riziká/ ciele požadované normou/ normami. Pri audite boli použité metódy rozhovorov, pozorovanie činnosti a preverenie dokumentácie a záznamov. Na základe údajov, prístupných v čase konania auditu, bol použitý proces výberu vzoriek. Štruktúra auditu bola v súlade s plánom auditu a matica plánu auditu je priložená ako príloha k tejto súhrnnej správe.

The audit team concludes that the organization ☒ has ☐ has not established and maintained its

Tím audítorov usudzuje, že organizácia ☒ má ☐ nemá *zavedený a udržiavaný*
management system in line with the requirements of the standard and demonstrated the ability of the system to systematically achieve agreed requirements for products or services within the scope and the organization's policy and objectives.
systém riadenia v súlade s požiadavkami normy a preukázal schopnosť systému systematicky dosahovať dohodnuté požiadavky na produkty alebo služby v rámci predmetu činnosti a politiky a cieľov spoločnosti.

Number of nonconformities identified: 0 Major 0 Minor
Počet identifikovaných nezhôd: _____ *Závažné* _____ *Nezávažné*

Therefore the audit team recommends that, based on the results of this audit and the system's demonstrated state of development and maturity, management system certification be:

Preto audítorský tím, na základe výsledkov z auditu a preukázania stavu vývoja a schopnosti systému, odporúča, aby bol certifikát systému riadenia:

☐ Granted / udelený ☒ Continued /ďalej platný ☐ Withheld /pozastavený ☐ Suspended until satisfactory corrective action is completed/ Zrušený až do vyhovujúceho nápravného opatrenia.

4. Previous Audit Results / Výsledky z predchádzajúceho auditu N/A

The results of the last audit of this system have been reviewed, in particular to assure appropriate correction and corrective action has been implemented to address any nonconformity identified. This review has concluded that:
Výsledky z predchádzajúceho auditu boli preverené, hlavne primerané zavedenie nápravného opatrenia na pomenovanie každej identifikovanej nezhody. Z tohto preverovania vyplynulo, že:

☐ Any nonconformity identified during previous audits has been corrected and the corrective action continues to be effective. (Refer to Section 6 for details)
každá nezhoda identifikovaná počas predchádzajúcich auditov bola odstránená a nápravné opatrenia sú ďalej účinné. (Detaily popísané v časti 6)

☐ The management system has not adequately addressed nonconformity identified during previous audit activities and the specific issue has been re-defined in the nonconformity section of this report.
Systém manažérstva neriešil dostatočne nezhodu identifikovanú počas činností pri predchádzajúcom audite v dôsledku čoho bola predefinovaná nezhoda v príslušnej časti tejto správy.

5. Audit Findings / Zistenia auditu

The audit team conducted a process-based audit focusing on significant aspects/risks/objectives. The audit methods used were interviews, observation of activities and review of documentation and records.
Audítorsky tím viedol audit procesov zameraný na dôležité aspekty/ riziká/ ciele požadované normou/ normami. Pri audite boli použité metódy interview, pozorovanie činnosti a hodnotenie dokumentácie a záznamov.

The management system documentation demonstrated conformity with the requirements of the audit standard and provided sufficient structure to support implementation and maintenance of the management system. *Systém riadenia dokumentácie preukázal zhodu s požiadavkami normy auditu a poskytol potrebnú štruktúru na podporu zavádzania a udržiavania systému riadenia*	☒ Yes/ Áno	☐ No/ Nie
The organization has demonstrated effective implementation and maintenance / improvement of its management system and is capable of achieving its policy objectives, as well as and the intended results of the respective management system(s).	☒ Yes/ Áno	☐ No/ Nie

Organizácia preukázala efektívne zavedenie a udržiavanie/ zlepšovanie svojho systému manažérstva a je schopná dosiahnuť svoje ciele politík tak isto ako aj predpokladané výsledky príslušného systému manažérstva.

The organization has demonstrated the establishment and tracking of appropriate key performance objectives and targets and monitored progress towards their achievement. *Organizácia preukázala zavedenie a sledovanie plnenia príslušných hlavných cieľov a úloh a sledovanie pokroku na ich dosiahnutie.*	☒ Yes/ Áno	☐ No/ Nie
The internal audit program has been fully implemented and demonstrates effectiveness as a tool for maintaining and improving the management system. *Program interných auditov bol plne zavedený a slúži ako efektívny nástroj pri udržiavaní a zlepšovaní systému manažérstva.*	☒ Yes/ Áno	☐ No/ Nie
The management review process demonstrated capability to ensure the continuing suitability, adequacy and effectiveness of the management system. *Proces preskúmania manažmentom preukázal schopnosť zabezpečiť neustálu účelnosť, primeranosť a efektívnosť systému manažérstva.*	☒ Yes/ Áno	☐ No/ Nie
Throughout the audit process, the management system demonstrated overall conformance with the requirements of the audit standard. *Počas vykonávania auditu preukázal systém manažérstva celkovú zhodu s požiadavkami normy auditu.*	☒ Yes/ Áno	☐ No/ Nie
Certification claims are accurate and in accordance with SGS guidance and the organization is effectively controlling the use of certification documents and marks. *Referencie na certifikáciu sú vedené správne a v súlade s manuálom SGS a organizácia efektívne kontroluje používanie certifikačných dokumentov a značiek.* ☐N/A	☒ Yes/ Áno	☐ No/ Nie

6. Significant Audit Trails Followed / Dôležité súvislosti sledované počas auditu

The specific processes, activities and functions reviewed are detailed in the Audit Planning Matrix and the Audit Plan. In performing the audit, various audit trails and linkages were developed, including the following primary audit trails, followed throughout:
Preverované špecifické procesy, činnosti a výkony sú rozpísané v plánovacej matici auditu a v pláne auditu. Počas realizácie auditu boli priebežne sledované a preskúmané rôzne súvislosti a väzby auditu, vrátane nasledovných základných súvislostí:

- Relating to Previous Audit Results/ Vzťahujúce sa na výsledky predchádzajúceho auditu:

There were no requirements for corrective actions raised during the previous audit.

- Relating to this Audit; including any significant changes (eg: to key personnel, client activities, management system, level of integration, etc.): / Vzťahujúce sa na tento audit; vrátane všetkých závažných zmien (týkajúcich sa napr. kľúčových zamestnancov, činností zákazníka, systému riadenia, úrovne integrácie, atď.)

Planning, Operation
Procedure - TEKO/M2.2.6/SM-002.02 Information security TEKO, a.s.
Register of information security risks – updated on 10.6.2020
Information security risk assessment:

- Personal assets
- Buildings and spaces
- Physical assets

- Electronic assets

Risk and compliance team was in interaction with all departments within the company. Everybody could raise a risk with the team. High level risk register was used to record and manage the risks within the organisation. There was a close relationship between the business and the risk management process owners.
Risk methodology, defined in the Procedure - TEKO/M2.2.6/SM-002.02 Information security TEKO, a.s. was evidenced. This document was found explaining the risk management process and risk assessment methodology.
List of possible threats and their evaluation: 18 types
Example of threat types:

- natural disaster (flood, earthquake, landslide, ...)
  storms, lightning strikes
  frost, heat
- personnel threats (worker migration, unavailability, shortage, strike)
- natural threats

Threat evaluation is expressed through the probability of occurrence of the threat: low, middle, high

Assessing the asset's vulnerability: low, middle, high

Functional Impact of Threat on Assets: low, middle, high

Information security risk treatment plan – 10.6.2020

Approval of the information security risk treatment plan – 10.6.2020

List of residual information security risks – 10.6.2020

Acceptance of the residual information security risks – 10.6.2020

Actual risk assessment was evidenced. It was observed that the process was followed. Risk owners were defined. Risk assessment was a regular review and individual risks were reviewed on a regular basis. Regularity of risk assessments is determined for at least once a year. Last risk assessment was performed on 10.6.2020.
Risks and opportunities which were identified were actioned. Continuous monitoring log was used for this purpose. Sampled risks were reviewed.
Risk analysis and risk assessment is one of the inputs to ISMS's Management review report.

Organization of information security
Leadership, Information security policies, Support
Documented information
Control documents - available in data directory at server
Control of external documentation – saved in data directory at server
Procedures for control of documents and records. „0"copy of procedures in printed version.
ISMS policy – 1.06.2020
IMS objectives for 2020
IMS objectives for 2019 - evaluation
IMS Manual – TEKO/M2.2/ZSM – 002 – 10.05.2017
Statement of applicability issued on 22.05.2018 – verified and accepted by the auditor, last review on 10.6.2020
Assignment of responsibility for information security – all employees
IMS management representative – Pavol Šimkovič – 15.6.2020
ISMS Management representative – Ing. Peter Mihaľov, PhD. – 08.06.2015
ISMS-IIS (Integrated information systems) Management representative – Ing. Viktor Balušeskul – 08.06.2015

ISMS-TIS DS (Technological information systems - Dispatching systems) Management representative – Ing. Miroslav Pitko – 08.06.2015
ISMS-TIS RS (Technological information systems – Control systems) Management representative – Ing. Marek Ivanoc – 08.06.2015
Cybersecurity manager – Karol Kovalčík - appointment decree, 12.04.2019
IT Administrators – Mr. Peter Matejkov - IT security specialist, Mr. Jaroslav Timko - Administrator of OS and IIS applications, Mr. Marek Spišák - Administrator of OS and IIS applications, Mr. Pavol Zelinka – IIS support technician
Confidentiality agreements
Security requirements in third party contracts
Segregation of duties

Human resource security
Procedure TEKO/PR – 14/2018 – Staff Regulations and Code of Ethics
Personal file – Work contract – Mr. Pavol Zelinka – IIS support technician, Qualification requirements, job description, Secrecy agreement
Personal file – Work contract – Mr. Jaroslav Timko – Administrator of OS and IIS applications, Qualification requirements, job description, Secrecy agreement, record from rap sheet
Training plan for 2020
Evaluation of individual trainings
Certificate - Peter Basaráb - The Personal Data Protection Act – 25.08.2016
Training – ISMS awareness training – Principles of information security– 14.06.2019

Asset management
Asset inventory list, Asset ownership, Authorization process for information processing facilities. Acceptable use of assets, List of forbidden usage of assets, Classification of assets- rules.
Confidential information stored in the paper and digitalized form. Paper confidential documents are stored in the safe.
Group of assets: personnel assets, buildings and areas, physical assets, electronic assets
Defining priorities for asset management – low, middle, high
Group of assets vs. threats
Inventory is performed annually
Inventory - HW a SW – EXCEL – updated on 10.6.2020

- Buildings and areas
- Personal assets
- Physical assets
- Electronic assets

Handover protocol – Mrs. Lenka Smreková – Lenovo ThinkPad Yoga X1 – 11.6.2020
Protocol on the disposal of data media – 19 pcs of HDD used for back-up – 30.04.2018

Access control
Procedure TEKO/P7.1/SM-005.05 - Allocation, modifying, and deleting user access to the information systems of personal data
Procedure TEKO/P7.1/MNA-005.00-01 - Operating instructions for INTERNET and INTRANET in TEKO, a.s.
Access to internet, intranet – defined rules
General rules and policies for using of information systems
Register of users, groups and accesses
Active directory users and computers
Active Directory
Damas Default IE Policy
Damas Default Organization Policy

Default IE Policy
Default Software Distribution Policy
Special Software Distribution Policy
Special TEKO Policy – IE Settings
Policy for assignment of passwords – password complexity rules, changing of passwords every 180 days
Policy of clean desk and clean screen (lock of workstation after 10 minutes)
Policy for assignment of passwords
Methodical instruction No. TEKO / P7.1 / MNA - 005.00-05 - Storing and accessing administrator passwords – 01.06.2013
Administrator password – in safe deposit - in sealed envelope
Review of Administrator password – 15.5.2020
Reviewed:
MagicDesk
Yearly review of access rights by supervisors:
Authorization matrix of SAP FI-CO module – 16.06.2020
Authorization matrix of SAP BOBJ module – 16.06.2020
Authorization matrix of SAP TM module – 16.06.2020
Authorization matrix of SAP FI module – 16.06.2020
Authorization matrix of SAP SD module – 16.06.2020
Authorization matrix of SAP FI-AA module – 16.06.2020
Module authorization matrix SAP PM – 16.6.2020
Module authorization matrix SAP IMPS – 17.6.2020
Module authorization matrix SAP PM – 16.6.2020
Module authorization matrix SAP PM – 16.6.2020
Module authorization matrix SAP ODT – 17.6.2020
Module authorization matrix SAP HR – 16.6.2020
List of application users – ROVET MES – 16.6.2020
List of application users – ROVET SELT – 16.6.2020
List of application users – UniDIS – 16.6.2020
List of application users – ODM – 16.6.2020
List of application users – Dymos – 12.6.2020
List of application users – Optimization algorithm - Taures – 12.6.2020
VPN accesses – 15.6.2020
Creation of Access rights – Mr. Š. Kapusta – Section 1000 Specialist, 02.01.2019
Creation of Access rights – SAP FI-CO – Mrs. Lenka Ragaňová – 09.05.2019
Request for an exception from a policy on the use of USB devices – Mr. Ľ. Kačmár, 05.02.2019
SAP – role description
Lotus Notes – role description
Yearly review of access rights by supervisors – Authorization matrix of Lotus Notes module – 16.06.2020
Yearly review of access rights by supervisors – Authorization matrix of SVYDO module – 16.06.2020
Yearly review of access rights by supervisors – Authorization matrix of Aktion – 16.06.2020
Yearly review of access rights by supervisors – Authorization matrix of GPS TDM – 18.06.2020
Issuance of the supplier's ID card and entry of motor vehicles – Emerson – Mr. Jiří Budín – 13.12.2019
Teleworking – NB – VPN, Citrix–mobile internet

Cryptography

Lotus Notes – support 1024-bit RSA key – encryption of internal correspondence

Physical & Environmental Security

Procedure No. TEKO / P7.1/SM – 005.03 - Physical and IIS system security

Procedure No. TEKO / P3.3/SM – 022.01 - Physical and TIS system security
Procedure No. TEKO / PR – 11/2018 - Access systems - rules on the entry and movement of persons, vehicles, export and import of material and parking in TEKO, a.s.
Procedure No. TEKO / PR – 12/2018 - Procedure for reported damage as a result of theft and property damage in TEKO, a.s.
Procedure No. TEKO / PR – 13/2018 - Measures related to reporting of crime and anti-social activities
Procedure TEKO/P5/MNA-010.00-01 - Operation of the digital camera system
List of buildings – T GIS application
All area is fenced; all entry gates are controlled by the security service - company SHS s. r. o. – Contract no. 460002127 – 30.05.2019, An agreement on the processing of personal data of intermediaries
Multilevel entrance safety – internal/external employees – proximity card – system Aktion (plus functions as a generator of employees' attendance), visitors – entry registration - visitors' cards, visitors permanently accompanied by internal employees during the whole visit. All offices equipped with locks, EPS
Clear screen, clear desk policy applied. All sensitive information is locked in cabinets, safes, archives...

Table showing authorized accesses for external companies.

Zones with enhanced security - authorized persons entrance only:
Integrated Information System: Server room 1.1/114, Server room 1.1/115, Server room 1.9/217, Server room 1.9/218
Integrated Information Systems – Control systems, Integrated Information Systems – Dispatcher systems: Machinery room, Server room, Switchboard, RRB, High-speed printer, Dispatching, UB

All server rooms – secured by the UPS. Equipped with redundant air conditioning systems. Temperature is permanently monitored by the control centre. UPS checked regularly – recorded to application MagicDesk "Operator logbook"
Alarm system in case of violation – electronic alarm system in case of violation - motion alarm (in internal premises - corridors, offices, server rooms), monitoring camera system (motion scanning – activated after 7 PM), cash desk, personnel department, payroll department, server rooms (broken glass sensors) – all connected (through GSM signal and phone line) to the permanent central desk of security service on the premises – company SHS s. r. o.

Monitoring camera system – 102 CCTVs – entry points, fence areas, recording 24/7 - central desk of security service, playback system – back up for 72 hours
Preventive and service maintenance – assured by the external companies.
Reviewed:
Service contract – GALARMTECH spol. s r.o. - Implementation of prescribed periodic revisions, conducting post-warranty service and repair of security systems - Digital camera system, Central security desk, Surge protection, Electronic security alarm - 10.09.2019
Inspection report – CCTV – company GALARMTECH spol. s r.o. – 4.6.2020
Electric appliance inspection and revision cards – date of last inspection – 10.3.2020

Operations security
Administrator:
Forcepoint NGFW – Antispam first level - Attack by Service, Attacks by Severity, Sys Events by severity, Critical attack report – Policy violation, Top attacks by source, Top attacks by hour of day
TEKO MailGuard – Quarantine Area – second level of Antispam
ESET Remote Administrator Console
ESET Smart Security 6
Virus definition Not Up-to-date

Out-of-Date Clients Triggering Notification

Technological unit: CHP
Backup of application of operator workstation
Disk mirroring of operator workstation
Program backup of control system DEMI ControlLogix
Program backup of control system DEMI do FLASH
Program backup of control system Silikostat SLC
Program backup of control system Silikostat do FLASH
Program backup operator panel DT2 PanelView
Program backup operator panel DT3 PanelView
Prevention operator workstation
Prevention of rack-u in control centerCHP
Prevention of fuseboard DT1
Prevention of fuseboard DT2
Prevention of fuseboard DT3
Prevention of fuseboard Silikostat
Quest-Intrust – log management system

Checked servers:
tekolx10, Server (3) 3032, DNS primary
tekolx11, Server (3) 3032, DNS secondary
lxcstm1, Server (3) 3032, time server 1
lxcstm2, Server (3) 3032, time server 2
lxwb01, Server (2) 3032, intranet server – www1
lxmng01, Server (1) 3032, disk backup
wdc01, Server (3) 3032, windows DC1, AD
wvps01, Virtual server (3) 3032, Print server

Checked PCs:
Service Performance Reports:
Inspection of PC92011 – Frnaková, 8.6.2020
Inspection of PC92009 – Kanpova, 4.6.2020

Plan of data back up: Integrated Information System
HP OpenView Storage Data Protector Manager – data backup
Backup of systems is performed on two data centers – automated backup process. Backup copies – magnetic tapes, securely stored in safes.
Backup frequency: Daily backup – automatic back up on magnetic tape – LTO library – incremental backup
Weekly backup – automatic system
Monthly backup
Yearly backup
Responsibilities, frequency and ways of backups are defined for particular systems
All activities are recorded in MagicDesk application – Operator log
Reviewed the records from log – 01-06/2020

Communications security
Internet connection – Contract No. 46000346 – DELTA ONLINE spol. s r.o. - Internet Access – 4 x 2 Mbit/s, CISCO NE 3400, switch ME 3400, 10BaseT – 28.05.2010
Architecture of company network:
INTERNET ISP: Firewall – DMZ (mail servers, time server, web servers, citric gateway, TDM, proxy server, IDS servers) – Technological network TIS

McAfee Firewall Enterprise Administrator Console
LAN TEKO
Primary datacenter:
SAN, Windows infrastructure, Back up – LOT, IBM ds3512, Control of network access: DNS, DHCP Management, Time servers
Backup datacenter:
SAN, Windows infrastructure, Back up – LOT, IBM ds3512, Control of network access: DNS, DHCP Management, Time servers

Technological LAN TEKO
Core Backbone – LAN Manag, LAN ROVET2, ROVET firewall - LAN IIS, LAN ROVET, LAN LFC, LAN Microscada, Firewall CiscoASA – DMZ 2 KOM, DMZ 1 WEB, Firewall CiscoUBDTS – MAN UB, LAN ROVET Servers, LAN Operator, LAN DAS /SrvDAS1, SrvDAS2)
DAS Backbone – LAN Kom
Technological LAN TEKO (ROVET)
Telemetric transfers TEKO
TEKO MAN
T-Com - ISDN – 2 MBs (SIEMENS HIPATH 4000 – switchboard)
8 direct telephone links
GTS Slovakia – internet radio transfer – 8 MBs

System acquisition, development and maintenance
Reviewed:
Integrated Information Systems – Control systems:
Contract no. 46002199 – Vision IT Solutions, a.s. - Upgrade of DMW IIS-TEKO infrastructure
Handover protocol – Data storage NetApp E2824, HPE ProLiant DL325 Gen 10 8SFF, Installation and configuration works, Training of administrators, Delivery of technical documentation, Extended warranty

Supplier relationships
Procedure TEKO/P1/ZSM-020 Purchasing
Security requirements within supplier agreements:
LYNX – spoločnosť s ručením obmedzeným Košice – service – HW, SW - SLA
Contract no. 46001991 - AutoCont SK a.s. – Exchange of IIS-TEKO virtual infrastructure servers– SLA, 02.10.2018
PosAm, spol. s r.o. – Maintenance, application and technical support of KIS, IBM Lotus – SLA
Contract no. 46002047NESS Slovensko, a.s. - Maintenance, application and technical support of infrastructure – SLA, 18.05.2018
Contract No. 46000346 – DELTA ONLINE spol. s r.o. - Internet connection, SLA
HATRIX, s.r.o. - security service – Contract no. 460001763 - 15.05.2017
Contract no. 460002127 – SHS s. r. o. - An agreement on the processing of personal data of intermediaries - 30.05.2019
Supplier evaluation – 06/2020

Information security incident management
Information systems failures:
Recorded in SAP for Integrated Information Systems – Control systems
Recorded tin application - Liberum HelpDesk for Technological Information Systems – Dispatcher systems
Recorded in application - MagicDesk – Operator log
Reviewed incident: HelpDesk ID 23348 – Failure of connectivity of the guard service workplace to the ISS TEKO LAN network
Reviewed incident: HelpDesk ID 23957 – Failure of menu functionality on the portal www-teko.sk

Information Security Aspects of Business Continuity management

Schedule for testing of business continuity plans for 2020 – ISS, 22.7.2019

Operational plans - ISS

IT disasters recovery plan – Backup power supplies – outages after DC and AC power failure – 22.7.2019

Record from testing of IT disasters recovery plan - Backup power supplies – outages after DC and AC power failure – 16.6.2020

IT disasters recovery plan – srvDAS1, srvDAS2 – scheduled restart of services, automatic pop-up control – 22.7.2019

Record from testing of IT disasters recovery plan - srvDAS1, srvDAS2 – scheduled restart of services, automatic pop-up control – 16.6.2020

IT disasters recovery plan – Process network – Checking of automatic recovery after failure of the optics-metallic converter– 22.7.2019

Record from testing of IT disasters recovery plan - Process network – Checking of automatic recovery after failure of the optics-metallic converter– 15.6.2020

IT disasters recovery plan – Operator workplace– planned restart of the visualization workplace – 22.7.2019

Record from testing of IT disasters recovery plan - Operator workplace– planned restart of the visualization workplace – 15.6.2020

IT disasters recovery plan – Operator workplace OC/DC/RUT – unplanned failure of the operator's workplace, failure of 3 monitors – 6.9.2019

Record from testing of IT disasters recovery plan - Operator workplace OC/DC/RUT– unplanned failure of the operator's workplace, failure of 3 monitors – 6.6.2019

IT disasters recovery plan – Operator workplace – Required restart, HMI malfunction, slow interface, need of restart at full operation – 17.1.2020

Record from testing of IT disasters recovery plan - Required restart, HMI malfunction, slow interface, need of restart at full operation – 17.1.2020

IT disasters recovery plan – Failure of the primary firewall – 12.12.2019

IT disasters recovery plan – Failure of central SAP ERP of TEP system – 12.12.2019

IT disasters recovery plan – Recovery of server WVWSUS01 – 12.12.2019

IT disasters recovery plan – Recovery of workstation – 12.12.2019

IT disasters recovery plan – Recovery of server WVWSUS01 – 12.12.2019

IT disasters recovery plan – Failure of server WVWSUS01 – 12.12.2019

IT disasters recovery plan – VMHOST server downtime – 12.12.2019

IT disasters recovery plan – VSESXi server power outage – 12.12.2019

IT disasters recovery plan – Recovery of AKTION virtual server wvacl01 after damage – 12.12.2019

Schedule for testing of business continuity plans for 2020 - Technological Information Systems - Control Systems

Operational plans - Technological Information Systems - Control Systems

IT disasters recovery plan – PC – dispatching center – malfunction, non-functionality – 26.1.2020

Record from testing of IT disasters recovery plan - PC – dispatching center – malfunction, non-functionality – 17.2.2020

IT disasters recovery plan – PC – IS UniDIS – application centre – malfunction, non-functionality – 10.04.2019

IT disasters recovery plan – Virtual Cluster - host server outage simulation – 11.06.2019

IT disasters recovery plan – Air-condition – malfunction, non-functionality – 04.06.2019

Compliance

List of all applicable local laws & regulations:

- 18/2018 Z. z.- Personal data protection Act
- The EU General Data Protection Regulation (GDPR);
- 185/2015 Z. z. - Copyright Act
- 541/2004 Z. z. - Nuclear Regulation Act
- 251/2012 Z. z. - Energetic Act

- 513/2009 Z. z. - Law on Railways
- 236/2016 Z. z. - Electricity regulation and distribution Act
- 364/2004 Z.z. - Water Law

Evaluation of conformance to legal and other requirements (local laws & regulations) from June 2020 - accepted as complete by the audit team and all exclusions were justified
Control of licenses:
SW inventory – PCinfo Magic EYE
All purchased software licensed
Record of the audit SW and HW – performed in 23rd calendar week of 2020 – totally 198 PCs audited
Protocol on the disposal of personal data – Application Aktion - visitor registrations – 03.06.2019
Protection of records – Procedure – Control of records
Penetration tests of web servers – performed in 11th week of 2017
Procedure TEKO/M1.4/ZSM-001 – Protection of personal data

Internal audits

Procedure TEKO/M.2.3/ZSM-016 Internal audits, 5.6.2020
Plan of internal audits – 2019 - evaluation
Plan of internal audits – 2020, 9.12.2019

- Report from internal audit No. 05/2020 from 28.5.2020 – Auditors: Mrs. Andrea Szásziová, Mrs. Mária Marcinová, Mrs. Iveta Makankevičová, Mrs. Diana Kozáková
  - Clauses audited: 4, 5, 5.2, 6.2, A,.5, A.6.1, A.8, 6.1, 8.2, 8.3. 7.5, 7.4, A.11, 7.1, A.13, A.12, A.14, A.15, A.6, 7.2, 7.3, A.7, A.9, A.10, A.14, A.15, A.16, A.17, A.18, 9.1, 9.2, 9.3, 10
- Report from internal audit No. 4/2020 from April 2020 – Auditors: Mrs. Lívia Knapová, Mr. Lukáš Sedlá, Mr. Zsigmondy
  - Clauses audited: 4, 5, 5.2, 6.2, A,.5, A.6.1, A.8, 6.1, 8.2, 8.3. 7.5, 7.4, A.11, 7.1, A.13, A.12, A.14, A.15, A.6, 7.2, 7.3, A.7, A.9, A.10, A.14, A.15, A.16, A.17, A.18, 9.1, 9.2, 9.3, 10
- Report from internal audit No. 3/2020 from March 2020 – Auditors: Mrs. Mária Marcinová, Mr. Ján Sedlický
  - Clauses audited: 4, 5, 5.2, 6.2, A,.5, A.6.1, A.8, 6.1, 8.2, 8.3. 7.5, 7.4, A.11, 7.1, A.13, A.12, A.14, A.15, A.6, 7.2, 7.3, A.7, A.9, A.10, A.14, A.15, A.16, A.17, A.18, 9.1, 9.2, 9.3, 10

Corrective actions requests – reviewed from internal audits - 01/2020, 02/2020

Management review

Management review – 15.6.2020

7. Nonconformities / Nezhody

NonConformity N° _0_ of _0_ ☐ Major/Závažná ☐ Minor/Nezávažná
Nezhoda č.
Department / Function:
Oddelenie/ oblasť
Document Ref.:
Dokumentácia/smernica:
Standard Ref./Norma:
Issue / Rev. Status:
vydanie/revízia:

Details of Nonconformity:
Detaily nezhody:

Client Proposed Action to Address Minor Non-Conformances Raised at this Audit: / Klient navrhol opatrenia na odstránenie nezávažnej nezhody zistenej počas tohto auditu:

- No requirements for corrective action from this audit.

Nonconformities detailed here shall be addressed through the organization's corrective action process, in accordance with the relevant corrective action requirements of the audit standard, including actions to analyse the cause of the nonconformity and prevent recurrence, and complete records maintained.
Nezhody uvedené v tejto časti musia byť riešené procesom nápravných opatrení organizácie, v súlade s príslušnými požiadavkami normy auditu na nápravné a preventívne opatrenia a kompletnou údržbou záznamov vrátane analýzy príčiny nezhody a opatrení zabraňujúcimi opakovaniu nezhody.

☐ Corrective actions to address identified major nonconformities shall be carried out immediately including a cause analysis, and SGS notified of the actions taken within 30 days. An SGS auditor will perform a **follow up visit** within 90 days to confirm the actions taken, evaluate their effectiveness, and determine whether certification can be granted or continued.
Nápravné opatrenia pre riešenie identifikovaných závažných nezhôd musia byť vykonané ihneď vrátane analýzy príčiny *a SGS musí byť s nimi oboznámená v priebehu 30 dní. Audítor SGS vykoná na potvrdenie prijatých opatrení* ***následný audit*** *do 90 dní a ohodnotí ich efektívnosť a určí či bude certifikát udelený, resp. či bude ďalej platný.*

☐ Corrective actions to address identified major nonconformities shall be carried out immediately **including** a cause analysis and records with supporting evidence sent to the SGS auditor for close-out within 90 days. *Nápravné opatrenia pre identifikované závažné nezhody budú ihneď vykonané* vrátane analýzy príčiny *a záznamy s podpornými dôkazmi budú zaslané do 90 dní audítorovi SGS na uzatvorenie.*

☐ Corrective Actions to address identified minor non conformities including a cause analysis, shall be documented on a action plan and sent by the client to the auditor within 90 days for review. If the actions are deemed to be satisfactory they will be followed up at the next scheduled visit. *Nápravné opatrenia pre identifikované nezávažné nezhody vrátane analýzy príčiny musia byť zdokumentované v akčnom pláne a zaslané audítorovi klientom do 90 dní na preverenie. Ak budú opatrenia posúdené ako vyhovujúce, ich realizácia bude preverená pri ďalšom plánovanom dohľadovom audite.*

☐ Corrective Actions to address identified minor non-conformities including a cause analysis, have been detailed on an action plan and the intended action reviewed by the Auditor, deemed to be satisfactory and will be followed up at the next scheduled visit.
Nápravné opatrenia pre identifikované nezávažné nezhody vrátane analýzy príčiny sú detailne spracované v akčnom pláne, plánované opatrenia pre ich odstránenie boli posúdené audítorom ako vyhovujúce a budú preverené počas ďalšieho plánovaného dohľadového auditu.

☐ Appropriate cause analysis immediate corrective and preventive action taken in response to each non-conformance as required.
Pre každú nezhodu bola okamžite vykonaná analýza príčiny a príslušné nápravné a preventívne opatrenia na jej odstránenie.

Note:- Initial, Re-certification and Extension audits – recommendation for certification cannot be made unless check box 4 is completed. For re-certification audits the time scales indicated may need to be reduced in order to ensure re-certification prior to expiry of current certification.
Note: At the next scheduled audit visit, the SGS audit team will follow up on *all* identified nonconformities to confirm the effectiveness of the corrective actions taken.
Poznámka: - certifikačný, recertifikačný a rozširovací audit – odporúčanie pre certifikáciu nemôže byť vydané, kým nie je ukončené štvrtý bod vyššie uvedeného zoznamu. Pri recertifikačných auditoch môže byť potrebné skrátiť stanovený časový limit aby sa zabezpečilo ukončenie recertifikácie pred uplynutím platnosti existujúceho certifikátu.
Poznámka: - pri všetkých ostatných plánovaných auditoch, audítorský tím SGS bude sledovať všetky zistené nezhody, aby potvrdil efektívnosť prijatých nápravných opatrení.

8. General Observations & Opportunities for Improvement/ / Všeobecné odporúčania a príležitosti na zlepšenie

To increase the security of remote access, we recommend installing a certification server for dispatching technology systems. / Odporúčame pre zvýšenie bezpečnosti vzdialených prístupov inštalovať certifikačný server pre dispečerské technologické systémy.

To increase network security, we recommend the deployment of central Log management - centrally collecting and evaluating logs from Firewalls, connecting log sources (including "SCADA" systems and other proprietary information systems) and periodically evaluating logs. / Pre zvýšenie bezpečnosti siete odporúčame nasadenie centrálneho Log managementu – centrálne zbierať a vyhodnocovať logy z Firewallov, napojiť zdroje logov (vrátane „SCADA" systémov a ďalších proprietárnych informačných systémov) a periodicky logy vyhodnocovať.

9. Opening and Closing Meeting Attendance Record/ / Záznam o účasti na úvodnom a záverečnom stretnutí

Name/ Meno	Position/ Pozícia	Opening/ Úvod	Closing/ Záver
Ing. Lenka Smreková, FCCA	Member of the Board, Chief Financial Officer		x
Ing. Lívia Knapová	Head of Human Resources	x	x
RNDr. Mária Marcinová	Specialist of Department 1020	x	x
Ing. Viktor Balušeskul	Head of IT dept.	x	x

SGS Slovakia spol. s r.o.
Kysucká 14
040 01 KOŠICE