itm8®

Independent Assurance Audit

Deviations Report – ISAE 3000

13.02.2024

Introduction

This report provides an overview of the findings from the ISAE 3000 Independent Assurance Audit for the period of January 1, 2023, to December 31, 2023, and describes the measures IT Relation has implemented in response. Our goal is to refine our operational processes and service delivery to align with industry standards. This document shares the steps we've taken to address the audit's observations, highlighting our effort to refine our practices and maintain high-quality service for our clients and stakeholders.

The audit has offered valuable insights for our improvement and development. Within this document, you'll find a detailed review of the corrective actions we've put in place following the audit's recommendations. These measures are part of our ongoing strategy to enhance our services, improve operational efficiency, and bolster our security protocols.

We view the audit's results as a chance to improve our organization. Prompt action has been taken to address the areas identified for improvement, with a commitment to pursuing long-term initiatives aimed at boosting our operational effectiveness. This report explains our approach to the audit findings and our continuous improvement strategy across the company.

We invite our stakeholders, clients, and partners to examine this report. It demonstrates our commitment to being open, accountable, and focused on improving our IT services and solutions. Through a positive response to feedback and a dedication to quality, IT Relation seeks to uphold and enhance our role in the IT sector.

Deviation Reports

B.6 Wrongly assigned access rights

Root Cause:

The observation identified incorrect role assignments to employees during the process of transferring work-related tasks. This issue arose when IT Relation replicated an existing role profile to assign to an employee who was taking over another's tasks. The copied role profile contained access rights that were not necessary for the new assignee's intended responsibilities. This misalignment occurred due to the direct replication of role profiles without adequately tailoring the access rights to match the specific needs of the new task assignments.

Corrective Actions:

We have implemented a robust control mechanism to ensure the accuracy of access rights assignments. This control process has been further enhanced in terms of both frequency and scope, aiming to meticulously correct and prevent any recurrence of incorrect access rights allocation.

Responsibility for Correction:

The User Management department at IT Relation has been tasked with enhancing the existing procedures to prevent the recurrence of similar incidents. Additionally, the Compliance & Security department is assigned the responsibility of overseeing the implementation of the newly introduced control activities, ensuring their effective integration and completion.

Status:

The observation has been corrected, the corrective actions implemented, and the control activities are continuously operating.

I.3 Security Incident Procedure

Root Cause:

The root cause of the observation stems from the handling of a security incident, which did not meet the expected standards of quality and adequacy as outlined in IT Relation's Security Incident Procedure. This shortfall resulted in delayed feedback, communication and response concerning some security incidents. The underlying issue was the procedural inadequacy, specifically, the failure to comprehensively consider various factors necessary for accurately determining the security and scope of the security incident.

Corrective Actions:

We have refined our procedure to ensure that the qualitative steps required to ascertain the severity of a security incident are now an integral component of the procedure, rather than relying on the subjective assessment of the individual employee managing the security incident. Additionally, we have developed new security incident templates to incorporate these adjustments. To further enhance our response to security incidents, we have also initiated comprehensive training aimed at improving the proper handling of such incidents.

Responsibility for Correction:

The Compliance & Security department have been imposed to refine the procedure to ensure continued adequately handling of security incidents.

Status:

The observation has been corrected, the corrective actions implemented, and the newly introduced procedure is operational.

Conclusion

This report presents the findings from the ISAE 3000 independent assurance audit, including the identified issues, their causes, and the steps our organization has taken to address them. In response, we have made adjustments to our security procedures, roles, and training programs.

Our response has included the introduction of stronger control mechanisms and updates to our security incident management processes. These actions are part of our ongoing efforts to evolve and respond to the changing demands of IT security.

To conclude, we see the results of the audit as a chance to learn and grow, and we remain committed to upholding high standards of service and earning the trust of our community.

Contact

If additional information is needed, of if the report raises further questions. Please direct your inquiries to the Compliance & Security department of itm8 at: compliance@itm8.com