It-audit

Appendix 6.2

Version: May 2022

VISMA

Contents

Introduction

This appendix describes the processes for IT auditing and covers the following in the software suite My Visma: Visma Løn, Visma HR, My Visma app and Datahub.

Information Security

The responsibility for carrying out the IT audit is placed in the Information Security department, which has reference to the top management.

Visma Enterprises Information Security Officer is responsible for:

- Facilitation of internal audit
- Facilitation of external audits
- Implementation, maintenance and continuous improvement of the management system for information security (ISO/IEC 27001: 2013).

Information Security and audit

Information Security is described in appendix 6.1 – Information Security.

Internal audit

Internal audits are carried out at planned intervals to examine whether the requirements of the international standard ISO/IEC 27001:2013 Information technology - Security techniques - Information management systems - Requirements (hereinafter ISO 27001) are effectively implemented and maintained.

Internal audit reports are classified and are not distributed to customers.

External audits

ISO/IEC 27001:2013 certificate

In 2019, Visma's Services ISO/IEC 27001:2013 was certified. And requirements for ongoing monitoring, measurement, analysis and evaluation of the management system for information security have been implemented.

The ISO / IEC 27001: 2013 certificate is available at Visma Community and from www.vismaenterprise.dk.

ISAE 3402 type 2

Visma Enterprise receives an annual ISAE 3402 Type 2 performed by an independent third party. The auditor's statement is performed in accordance with "ISAE 3402' Assurance Reports on Controls at a Service Organization', and additional requirements applicable in Denmark".

The control environment is built on the basis of ISO/IEC 27001:2013 annex a, where parts of or entire areas are included:

- Information security policies
- Organization of information security
- Human ressource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communication security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance.

The audit statement covers one year and is offered to customers who have used the audited Services in whole or in part during the audit period.

Audit statements can be ordered on the webshop.

Auditors' statements from suppliers

Supplier relationships are defined and implemented in accordance with ISO/IEC 27001 a.15. Suppliers with a 'high' rating provide an annual auditor's report prepared by an independent third party. The auditor's statement is prepared according to different standards depending on the service, e.g. ISAE 3402, ISAE 3000 or ISRS 4400.

Auditor's statements from supplier relationships are not handed out to customers.

--