Sample audit programme

Email security

12 audit steps · BSI, ISO 27001, RFC

12 audit steps with criterion, reference, procedure and expected evidence. 8 documents to request and the typical findings.

BSI APP.5.3 · ISO/IEC 27001:2022 Annex A 5.14 · RFC 7208 · RFC 6376 · RFC 9989 · RFC 9990 · BSI TR-03108 · ISO/IEC 27001:2022 Annex A 8.7 · ISO/IEC 27001:2022 Annex A 8.7 and 8.23 · § 30(2) no. 10 BSIG · ISO/IEC 27001:2022 Annex A 8.5 · ISO/IEC 27001:2022 Annex A 8.15 · ISO/IEC 27001:2022 Annex A 6.8 · § 147(1) nos. 2 and 3 AO

Audit objective and scope

The audit assesses whether the organisation secures its email communication technically and organisationally: sender authentication for its own domains, encrypted transport, filtering of malware and phishing, secure configuration of the mail platform such as Exchange Online and a working reporting path for suspicious messages. It also assesses whether retention of business email is governed.

SCOPE

- All email domains of the organisation, including those not used for sending
- Mail platform (for example Exchange Online or Exchange Server) and upstream filtering services
- External services that send email on behalf of the organisation, such as newsletters or ticket systems
- Out of scope: end-to-end encryption in individual specialist procedures, unless agreed separately

Audit steps 1 to 3

Step 01 — BSI APP.5.3; ISO/IEC 27001:2022 Annex A 5.14

A policy governs business use of email, sending confidential information and forwarding to external addresses.

Procedure Read the policy, check approval and compare it with the technical forwarding settings.

Evidence Email policy, rules on information transfer

Step 02 — RFC 7208

Every domain publishes an SPF record that permits only authorised senders; non-sending domains exclude sending.

Procedure Query DNS records for all domains and compare the listed senders with the actual sending services.

Evidence Domain list, DNS query, list of sending services

Step 03 — RFC 6376

Outgoing messages are signed with DKIM; keys have an adequate length and are rotated.

Procedure Analyse headers of test messages from every sending path and ask about key length and the last key rotation.

Evidence Headers of test messages, DKIM configuration

Audit steps 4 to 6

Step 04 — RFC 9989; RFC 9990

A DMARC policy is published and set to reject or quarantine; reports are analysed.

Procedure Query the DMARC record, establish the policy level and review the analysis of reports for the last three months.

Evidence DNS query, DMARC report analysis, actions on misconfigurations

Step 05 — BSI TR-03108

Transport between mail servers is encrypted and protected against downgrade, for example through DANE or MTA-STS with TLS reporting.

Procedure Review the transport configuration and test the encryption of the own mail servers with an external tool.

Evidence External test result, connector configuration, TLS reports

Step 06 — ISO/IEC 27001:2022 Annex A 8.7; BSI APP.5.3

Incoming messages are scanned for malware; dangerous attachments are blocked or opened in isolation.

Procedure Review filter rules and blocked file types and analyse detection statistics for the last three months.

Evidence Filter configuration, list of blocked file types, detection statistics

Audit steps 7 to 9

Step 07 — ISO/IEC 27001:2022 Annex A 8.7 and 8.23

Links in messages are checked when clicked, external senders are tagged and sender spoofing is detected.

Procedure Review settings for link checking, external tagging and impersonation protection and trace them with a test message.

Evidence Phishing protection configuration, tagged test message

Step 08 — BSI APP.5.3

The mail platform is hardened: automatic forwarding to external addresses is restricted and legacy authentication is disabled.

Procedure Read settings for forwarding, mailbox rules and authentication methods and list mailboxes with external forwarding.

Evidence Tenant configuration extract, list of mailboxes with forwarding

Step 09 — § 30(2) no. 10 BSIG; ISO/IEC 27001:2022 Annex A 8.5

Sign-ins to mailboxes and to platform administration are protected with multiple factors.

Procedure Review multi-factor rules and have accounts without a second factor listed with justification.

Evidence Conditional access policies, factor registration report, exception list

Audit steps 10 to 12

Step 10 — ISO/IEC 27001:2022 Annex A 8.15

Mailbox access and administrative changes are logged, and logs are retained long enough.

Procedure Check that mailbox auditing is enabled and its retention period, and have a log retrieval demonstrated.

Evidence Logging settings, example of a log retrieval

Step 11 — ISO/IEC 27001:2022 Annex A 6.8

Staff can report suspicious messages easily; reports are analysed and answered.

Procedure Have the reporting path demonstrated and trace handling, assessment and feedback for five reports.

Evidence Description of the reporting path, handled reports

Step 12 — § 147(1) nos. 2 and 3 AO

Retention of business email that counts as commercial or business correspondence is governed and technically implemented.

Procedure Review retention rules and the archiving solution and check whether mailbox deletions could undermine retention.

Evidence Retention policy, archiving configuration

Document request list

Request these 8 documents before you start

1. Email policy
2. List of all domains and of services sending on behalf of the organisation
3. DNS records for SPF, DKIM and DMARC and the DMARC report analysis
4. Configuration of transport encryption, filtering and phishing protection
5. Tenant or server configuration extract of the mail platform
6. Multi-factor authentication report with exceptions
7. Description of the reporting path for suspicious messages
8. Email retention policy

TYPICAL FINDINGS

- The DMARC policy stays at monitoring permanently, reports are not read.
- Unused domains have no record and can be abused for spoofing.
- External sending services are not included in SPF or DKIM.
- Automatic forwarding to private addresses is allowed.
- Some mailboxes and service accounts can be reached without a second factor.
- Reported phishing messages are neither analysed nor answered.

Sample audit programme library

29 sample audit programmes online

proauditmap.com/en/audit-programs/

Full audit package in ProAuditMap

proauditmap.com

ProAuditMap

Sample provided without warranty and not legal advice. Laws, regulations and standards appear only as references, no normative text is reproduced. Adapt scope and depth to your organisation, your risks and the current version of the provisions that apply to you before use.
Last updated: 13 October 2026