ManageEngine

A quick guide to BIO2

Baseline Information Security for Government 2 — Netherlands, v1.3 final, January 2026

The Baseline Information Security for Government 2 (BIO2) is the mandatory information security framework for all Dutch government entities, issued by the Ministry of the Interior and Kingdom Relations (BZK) and managed by the Center for Information Security and Privacy Protection (CIP).

Version 1.3 (January 2026) aligns with ISO/IEC 27001:2023 and ISO/IEC 27002:2022, and incorporates obligations from the Dutch Cybersecurity Act (Cyberbeveiligingswet, Cbw).

Sl.no	Requirement area	Measures	Controls required
1	ISMS governance and risk	§5–7	• Establish ISMS scope covering critical systems • Produce Statement of Applicability (SoA) • Define and apply formal risk management methodology • Maintain risk register with accepted risks
2	Policy, roles, and accountability	5.01–5.02	• Adopt information security policy at board level • Review policy at least annually • Appoint CISO with independent advisory mandate • Define roles for board, CISO, line management
3	Identity and access management	5.16–5.18	• Maintain formal user registration and deprovisioning procedure • Prohibit unapproved group accounts • Review all access rights anually
4	Authentication and credential security	5.17	• Enforce MFA for digital work, internet-facing, and privileged accounts • Apply passwordless or password + second factor • Provide password manager to all employees • Automate password policy enforcement
5	Supply chain and third-party security	5.19–5.23	• Include security requirements in all procurement contracts • Require annual third-party compliance evidence • Ensure requirements flow to all subcontractos • Govern CSPs with triennial policy review
6	Incident management and reporting	5.24–5.28	• Operate a low-threshold incident notification desk • Publish CVD procedure • Report incidents to CSIRT within statutory deadlines • Retain incident data for a minimum of three years

Source: www.bio-overheid.nl/media/5vklffpe/20260325-baseline-information-security-for-government-2-bio2-v13-final.pdf

SL.No	Requirement area	Measures	Controls required
7	Monitoring, logging, and detection	8.15–8.16	• Collect structured logs with actor, timestamp, action, and object fields • Set retention based on risk • Deploy detction and response solution for continuous monitoring • Protect log integrity; alert on tampering
8	Vulnerability management and testing	8.08	• Mitigate high-severity vulnerabilities within one week • Continuously scan internet-facing systems • Perform automated penetration tests at each major release • Test all internet-facing systems at least annually
9	Backup, continuity, and cryptography	8.13, 8.24	• Define backup policy with ransomware protection • Test recovery procedure at least annually • Establish cryptography policy covering standards and key management • Align cryptographic strength to SCSC/AIVD recommendations
10	Monitoring, compliance, and annual reporting	5.30, 5.36	• Test continuity plans annually • Produce annual In Control Statement under CISO coordination • Maintain annual audit plan with system-specific audit types • Report on information security within P&G cycle

Souruce: www.bio-overheid.nl/media/5vklffpe/20260325-baseline-information-security-for-government-2-bio2-v13-final.pdf

BIO2 and ManageEngine

ManageEngine offers solutions that help government organisations govern identities, detect threats, and demonstrate compliance. AD360, ManageEngine's IAM solution, covers identity life cycle management, MFA, access certification, and governance reporting. Log360, its SIEM solution, provides centralised log collection, continuous threat detection, incident management, and compliance evidence generation. Together, they address the principal software-enforceable controls required under BIO2.

How can ManageEngine help you implement the KRITIS-Dachgesetz?

Identity life cycle management

Automate user provisioning and deprovisioning across AD, Microsoft 365, and Exchange with approval-based onboarding and offboarding workflows.

Helps with 5.16.01, 6.02.01.

Multi-factor authentication

Enforce adaptive MFA, passwordless (FIDO2, smart card, biometric), and password plus second factor for digital work environment, internet-facing, and privileged accounts.

Helps with 5.17.01.

Access certification

Run periodic access rights review campaigns for all accounts; schedule quarterly reviews for privileged accounts with documented certification decisions.

Helps with 5.18.02, 8.02.01.

Continuous log monitoring

Collect structured, timestamped logs from on-premises systems, cloud, OT, and network devices into a centralised SIEM with configurable, risk-based retention periods.

Helps with 8.15.01–8.15.06.

Threat detection and incident response

Detect attacks and anomalies in real time using correlation rules, UEBA, and threat intelligence; automate incident escalation and CSIRT notification through SOAR playbooks.

Helps with 5.24.07, 8.16.03.

Compliance reporting

Generate audit-ready compliance reports and In Control Statement evidence on a scheduled basis aligned to the Planning and Control cycle.

Helps with 5.36.01, 5.35.02.

Risk posture management

Identify misconfigurations, over-privileged accounts, and security gaps across Active Directory and monitored infrastructure to feed BIO2's mandatory risk assessment cycle.

Helps with Part 1 §6, 5.08.01.

Supply chain monitoring

Track external supplier account access; detect credential leaks through dark web monitoring; monitor cloud service provider activity and shadow IT.

Helps with 5.20.03, 5.21.03, 5.23.01.

Backup and recovery

Protect AD, Entra ID, and Microsoft 365 data with automated scheduled backups and recovery testing; detect ransomware activity before backups are compromised.

Helps with 8.13.01–8.13.04.

For more information, contact sales@manageengine.com