JUMBO BLOCK REPORT

Reporting obligations in an incident – NIS-2, KRITIS-DachG, CRA and GDPR



Manual · Version 1.0.0

October 2026

ZANNI GROUP · Andreas Zanni e.K. · Brauhof 12 · 44866 Bochum · jumboblock.org

Contents

1. Overview
2. Basic terms
3. Workflow
4. Creating and opening an incident file
5. Incident, obligations and significance
6. Deadlines and reporting channels
7. Creating and submitting reports
8. Timeline
9. Report
10. File, verification chain and signature
11. Interaction with other programs
12. Security and technology
13. Troubleshooting

1. Overview

REPORT helps entities and companies meet their reporting obligations in a security incident completely and on time. From the time of awareness, REPORT monitors all potentially applicable deadlines under NIS-2 (Sec. 32 BSIG), the German KRITIS umbrella act (Sec. 18 KRITIS-DachG), the Cyber Resilience Act (Art. 14 CRA) and the GDPR (Art. 33), creates the report texts with the statutory mandatory details and records every submitted report unalterably.

All details and actions are stored in an incident file. Every relevant action is recorded as an entry in a hash chain; the resulting integrity value appears in every report and every printout. The file therefore cannot be altered afterwards without detection.

Fully offline: REPORT runs in the browser, also directly from a USB stick (`file://`). There is no server connection, no account and no cloud. The incident file is encrypted with your password.

Working aid, not legal advice: REPORT reflects the reporting obligations according to the stated legal status. The legal texts and the specifications of BSI, BBK and supervisory authorities are authoritative. The reports themselves are submitted via the reporting portals of the competent bodies.

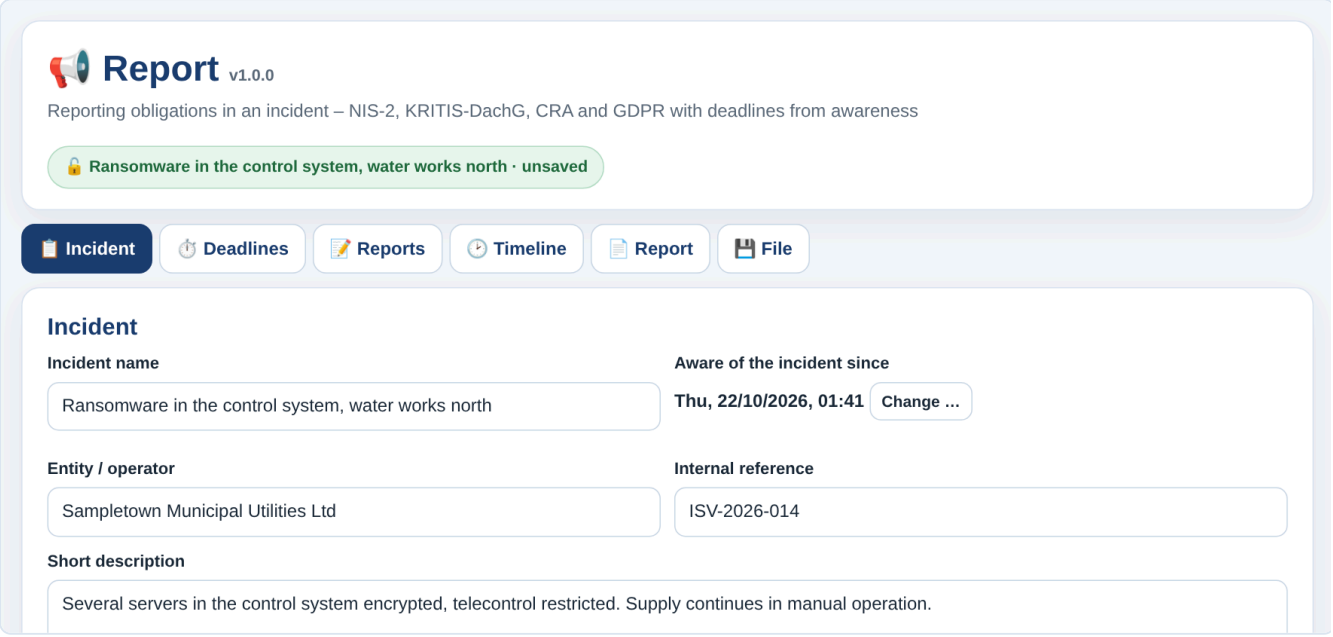


Fig. 1: REPORT work area with its six tabs

Area	Purpose
Incident	Incident details, awareness, potentially applicable reporting obligations and significance assessment
Deadlines	All reports with legal basis, latest submission and status; reporting channels
Reports	Create report texts, copy them and record them as submitted
Timeline	Events and measures, also from the JUMBO BLOCK LOGBOOK situation log
Report	Documentation of the incident for printing or as PDF
File	Save, lock, verification chain, signature and verification

2. Basic terms

Term	Meaning
Incident file	Encrypted file (.dbm) with all details, assessments, reports, timeline and verification chain of an incident
Awareness	Time at which the entity became aware of the incident. It starts all deadlines and can only be changed with a reason.
Significant security incident	Under Sec. 2 No. 11 BSIG an incident that has caused or can cause severe operational disruption or financial loss, or considerably affects third parties. Only significant incidents must be reported under Sec. 32 BSIG.
Report	One stage of a reporting obligation, e.g. early warning, incident notification or final report, with its own deadline and mandatory details
Report text	Text generated by REPORT with all mandatory details for transfer into the reporting portal
Submission	Recorded submission of a report with time, channel, reference number and exact wording. After that the report is unalterable.
Verification chain	Hash chain of all relevant actions in the incident file
Integrity value	Number and SHA-256 hash of the last entry of the verification chain, e.g. “No. 18 · SHA-256 dcc579…”. It appears in every report and printout.
Verification file	File with the hashes of the verification chain without content, signable with JUMBO BLOCK CRYPT

3. Workflow

1. **Create the incident file** – as soon as a security incident becomes known; record the time of awareness precisely (chapter 4).
2. **Determine obligations** – state the classification under NIS-2, KRITIS, CRA and GDPR and assess the significance (chapter 5).
3. **Monitor deadlines** – the *Deadlines* tab shows which report is due when (chapter 6).
4. **Report** – create the report text, transfer it into the reporting portal, record the submission with the reference number (chapter 7).
5. **Document** – keep events and measures in the timeline, import entries from the situation log (chapter 8).
6. **Secure the state** – save the file regularly; sign important states (chapter 10).
7. **Close** – submit final or progress reports, mark the incident as fully handled and create the report (chapter 9).

All reports are to be made without undue delay – the deadlines shown are maximum deadlines. If in doubt, report as a precaution within the deadline; the early warning can be given with the information available at that time.

4. Creating and opening an incident file

1. Under *New incident* enter the name, e.g. “Ransomware in the control system, water works north”.
2. Enter *Aware of the incident since* precisely – date and time.
3. Add the entity or operator and the internal reference.
4. Enter a password of at least 12 characters twice and click *Create incident file*.

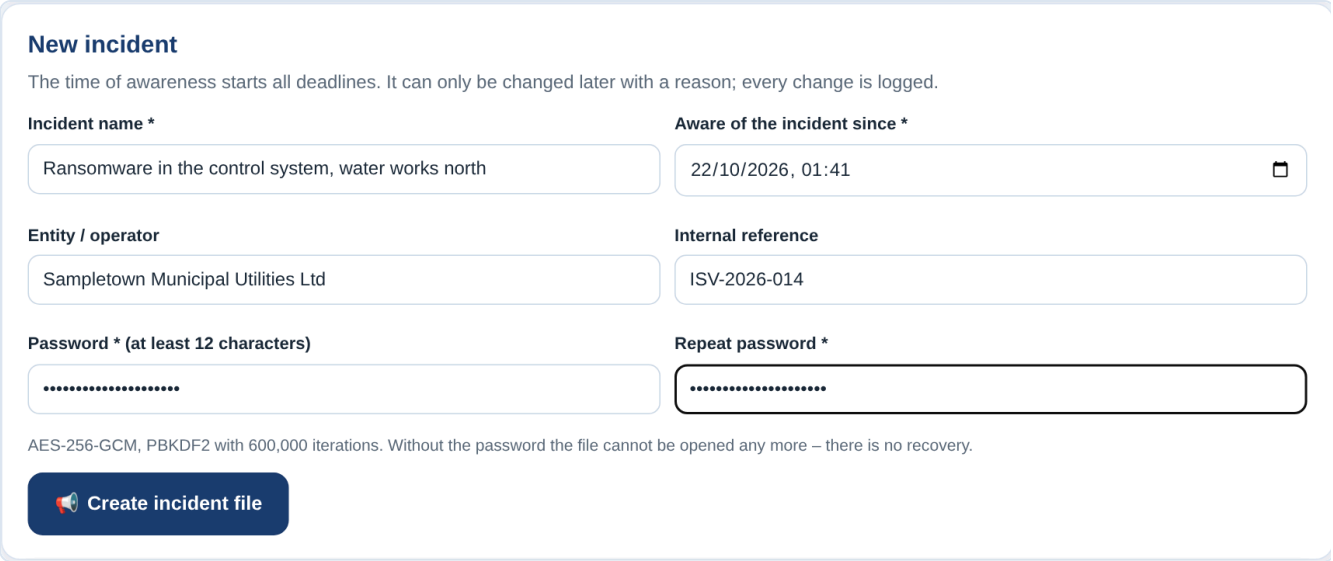


Fig. 2: Creating a new incident

> Without the password the file cannot be opened any more – there is no recovery.

The start page also shows the legal status of the rule table according to which REPORT calculates the deadlines.

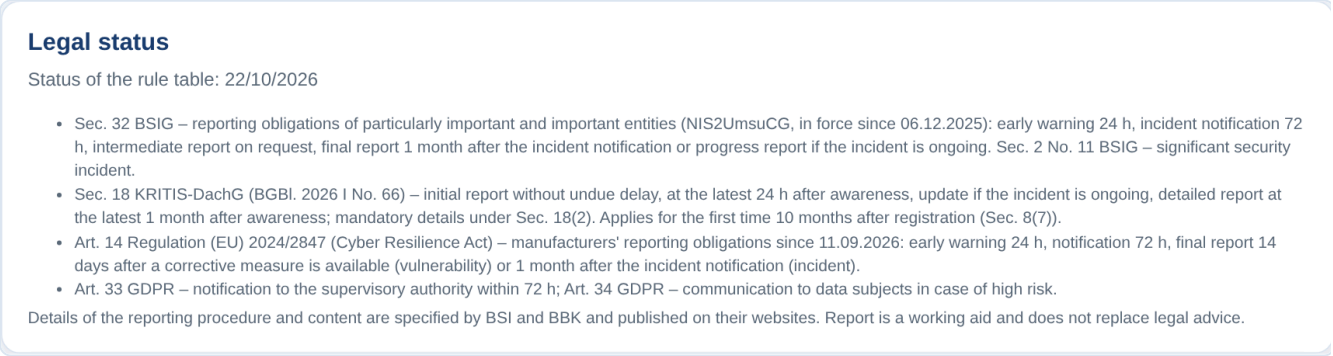


Fig. 3: Legal status of the rule table

Opening, locking, restoring

- *Open incident file* reads an existing file; the password is requested afterwards.
- The file locks after 15 minutes without input. The password is enough to continue.

- Until saved, the file is additionally cached encrypted in the browser. After a crash the start page offers the state for restoration.

5. Incident, obligations and significance

Incident

The *Incident* tab contains name, awareness, entity, reference, short description and the reporting contact for queries. These details are taken over into all report texts.

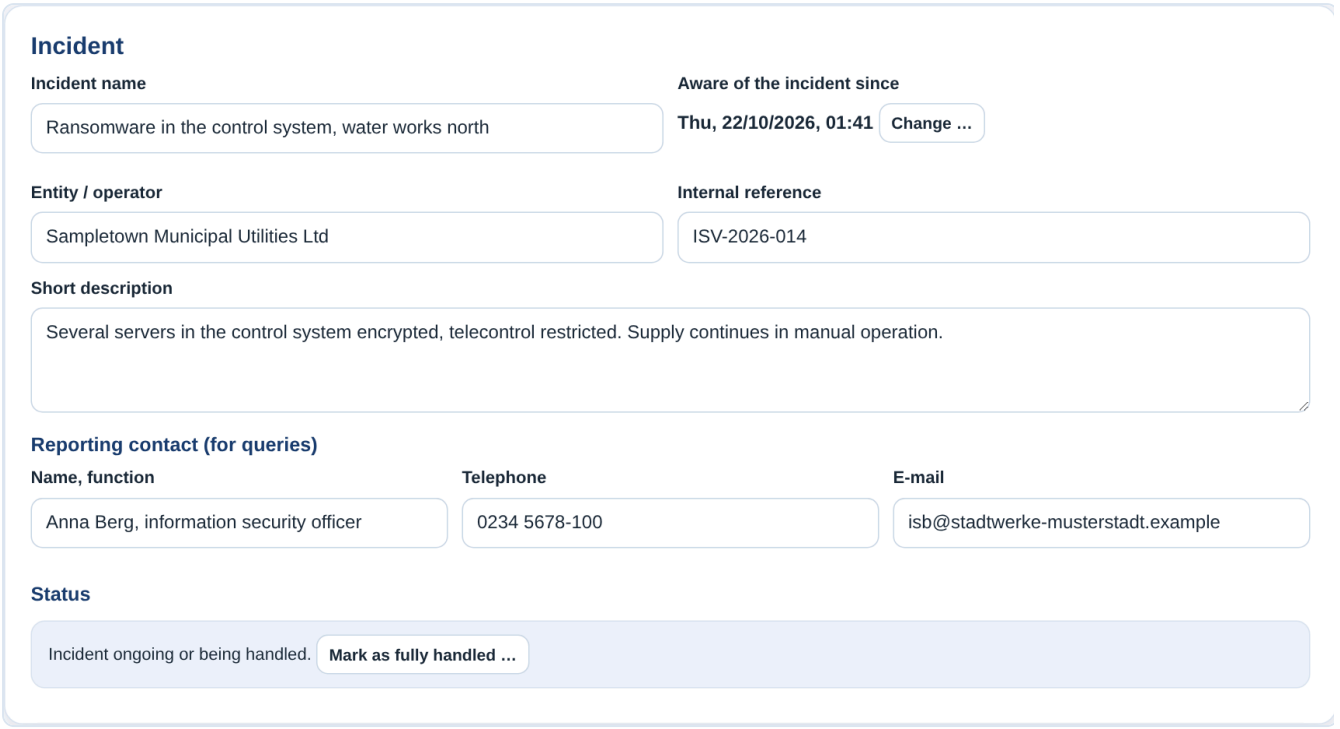


Fig. 4: Incident details

Change … next to the awareness requires a reason; the change is recorded in the verification chain with old and new time. All deadlines are recalculated.

Which reporting obligations may apply?

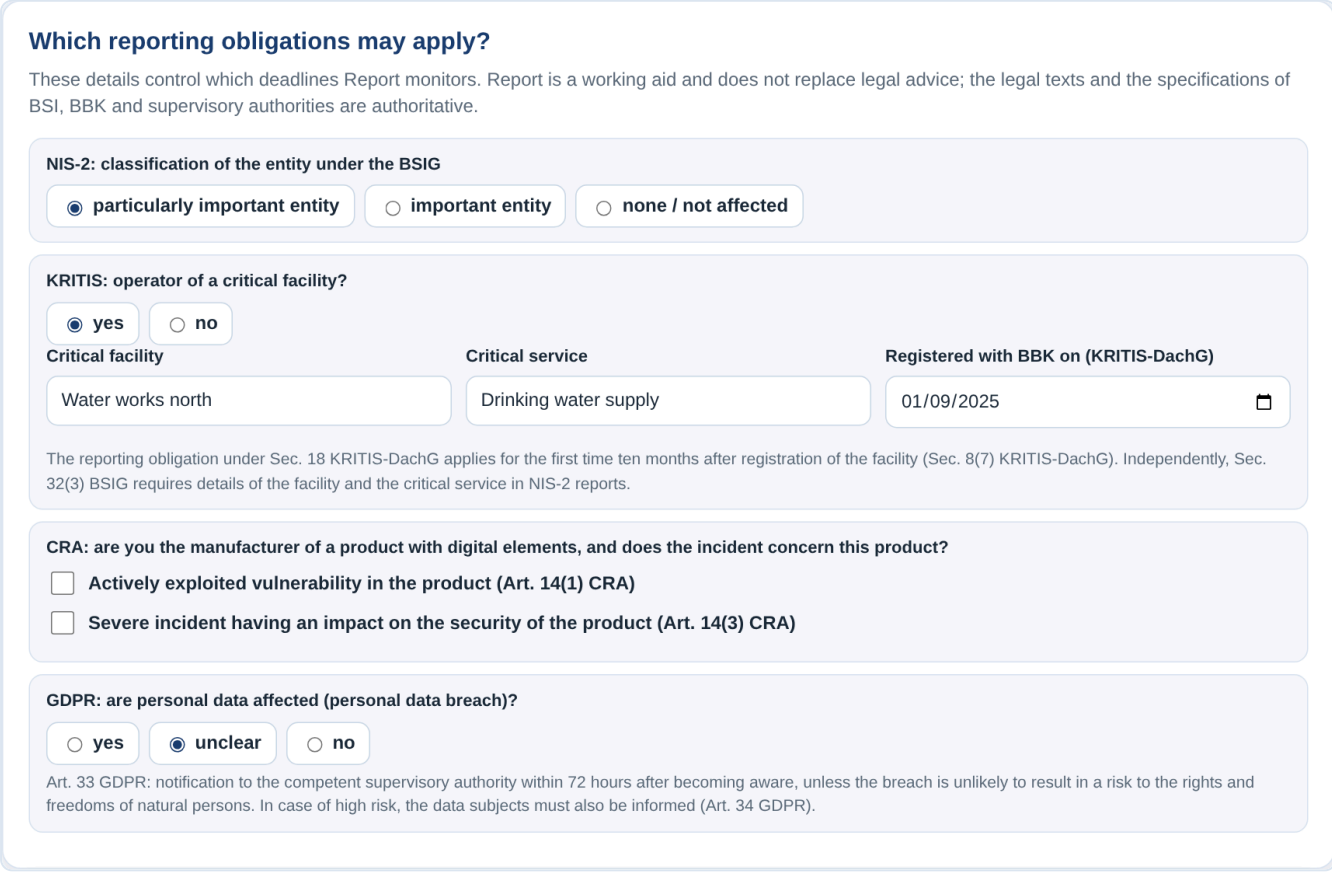


Fig. 5: Classification under NIS-2, KRITIS, CRA and GDPR

Question	Effect
NIS-2: classification under the BSIG	Particularly important or important entity – reporting obligations under Sec. 32 BSIG for significant security incidents
KRITIS: operator of a critical facility	Critical facility, critical service and date of registration with the BBK. The reporting obligation under Sec. 18 KRITIS-DachG applies for the first time ten months after registration; facility and service are also included in NIS-2 reports (Sec. 32(3) BSIG).
CRA	For manufacturers of products with digital elements: actively exploited vulnerability (Art. 14(1)) and/or severe incident (Art. 14(3)); plus product and time at which a corrective or mitigating measure is available
GDPR	Personal data breach: yes, unclear or no. For “unclear”, REPORT shows the deadline with the note “check obligation”.

Significance

The assessment follows Sec. 2 No. 11 BSIG: severe operational disruption, financial loss, considerable damage to third parties – for KRITIS facilities additionally the significant disruption of the critical service. Each question is answered with yes, no or not yet clear; REPORT shows the result immediately.

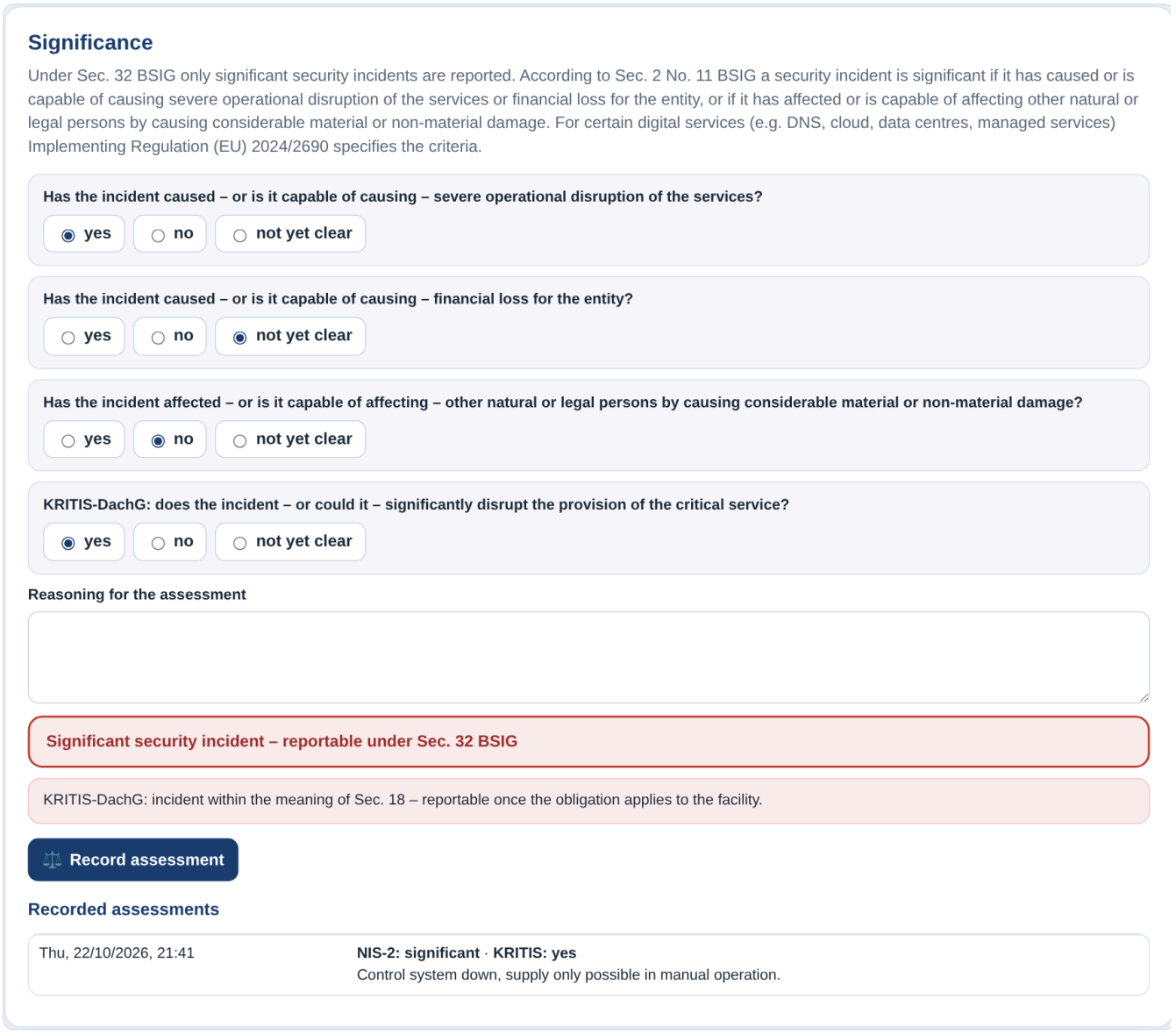


Fig. 6: Significance assessment with result and recorded assessment

Record assessment stores answers, result and reasoning with time in the verification chain. When new information becomes available, repeat the assessment; all assessments remain in the list of recorded assessments.

Status

Once the incident has been fully handled, mark it with *Mark as fully handled …*. This controls the final and progress reports. *Reopen* withdraws the mark; both are logged.

6. Deadlines and reporting channels

The *Deadlines* tab lists all reports resulting from the details, with legal basis, latest submission time and status. REPORT calculates monthly deadlines conservatively up to the same time on the corresponding day of the following month.

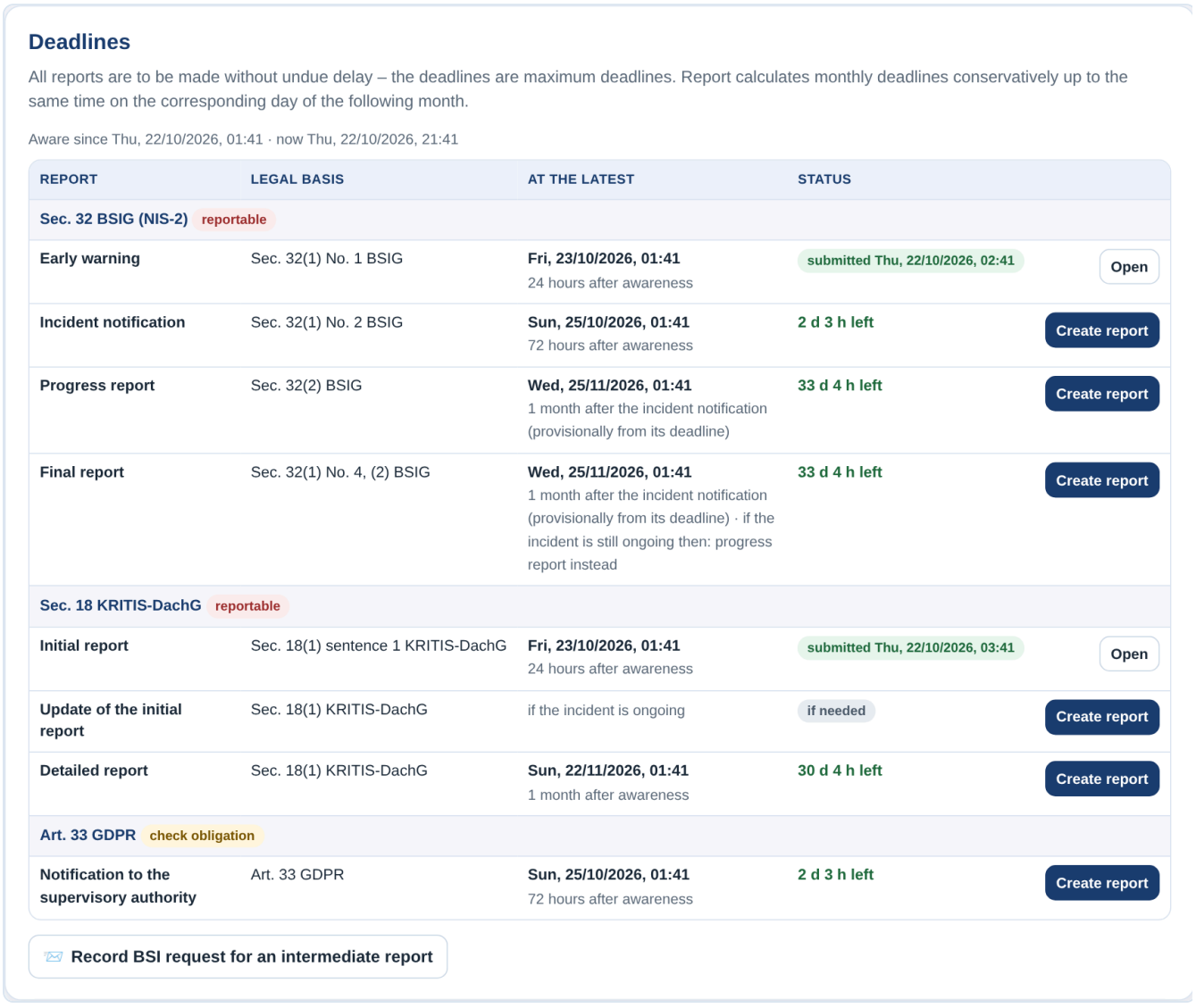


Fig. 7: Deadlines with status and buttons for creating the reports

Regulation	Reports and deadlines
Sec. 32 BSIG (NIS-2)	Early warning 24 h · incident notification 72 h · intermediate report at the request of the BSI · final report 1 month after the incident notification, or progress report while the incident is ongoing
Sec. 18 KRITIS-DachG	Initial report 24 h · update if the incident is ongoing · detailed report 1 month after awareness
Art. 14 CRA – vulnerability	Early warning 24 h · vulnerability notification 72 h · final report 14 days after a corrective or mitigating measure is available
Art. 14 CRA – incident	Early warning 24 h · incident notification 72 h · final report 1 month after the incident notification
Art. 33 GDPR	Notification to the supervisory authority 72 h

The *Status* column shows the remaining time, “overdue for …” or “submitted” with the time. If a deadline depends on an earlier report, REPORT calculates provisionally from that report's deadline and, after submission, from the actual time.

Intermediate report on request

If the BSI requests an intermediate report (Sec. 32(1) No. 3 BSIG), record the request with *Record BSI request for an intermediate report* – with date, deadline and note. The intermediate report then appears with this deadline.

Reporting channels

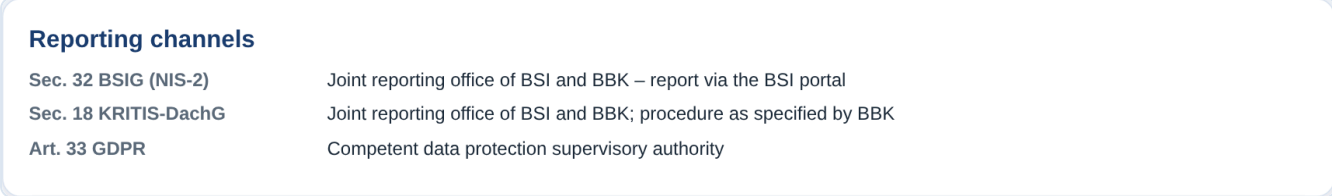


Fig. 8: Reporting channels of the applicable reports

7. Creating and submitting reports

A report is started in the *Deadlines* tab via *Create report* or in the *Reports* tab via the selection and *Create report*. The form contains the statutory mandatory details of the respective stage; mandatory fields are marked with *. Details from the *Incident* tab and from earlier reports are pre-filled.

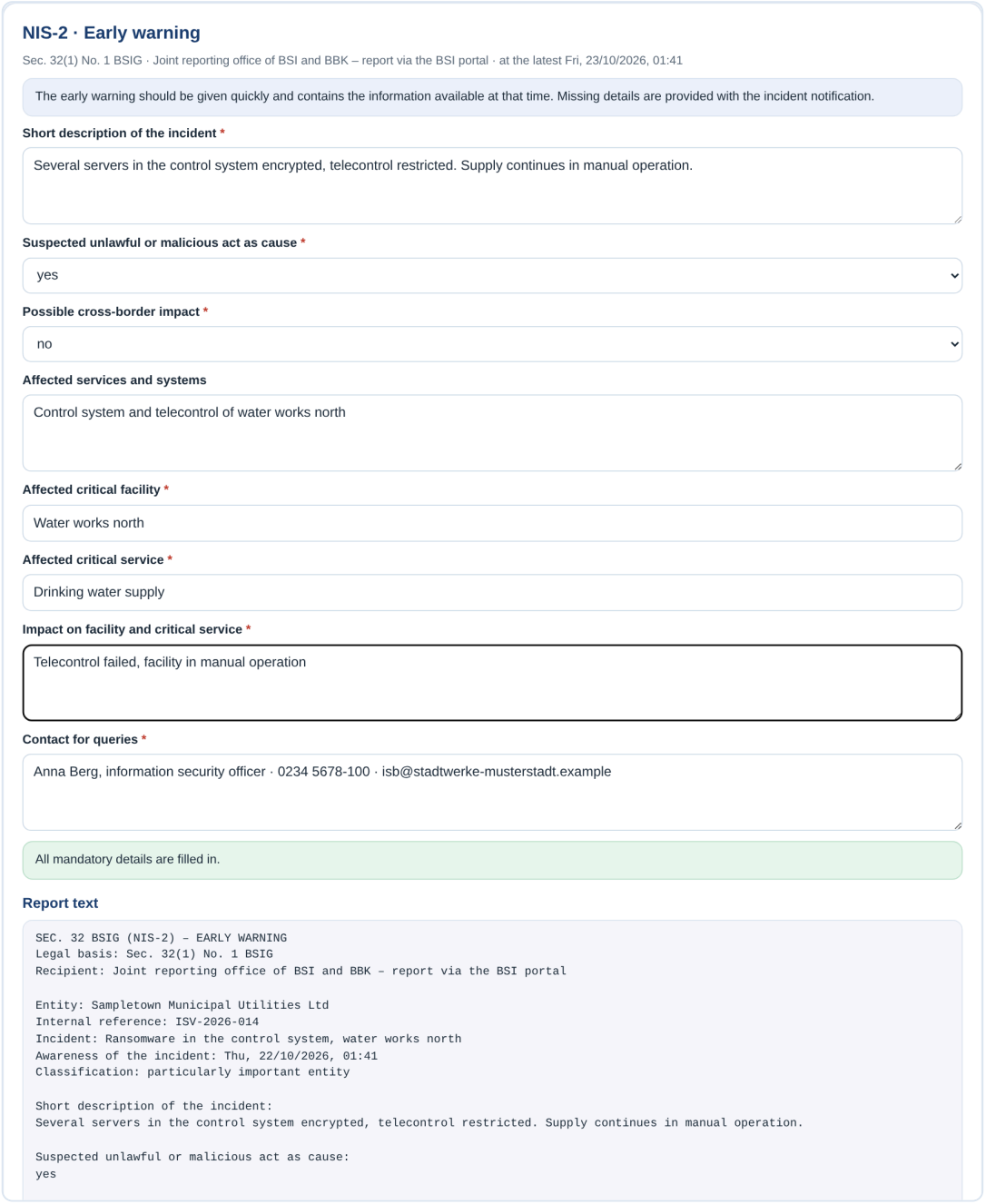


Fig. 9: NIS-2 early warning with mandatory details and report text

1. Fill in or check the fields. Below them REPORT shows whether all mandatory details are present.
2. The *Report text* is generated continuously from the details. It starts with legal basis, recipient and header data and ends with the line *Integrity value of the incident file*.
3. Click *Copy report text* and transfer it into the reporting portal. Please also transfer the integrity value line, e.g. into a free-text field – it anchors the state of the file with the receiving body.

4. After submission click *Record as submitted …*.

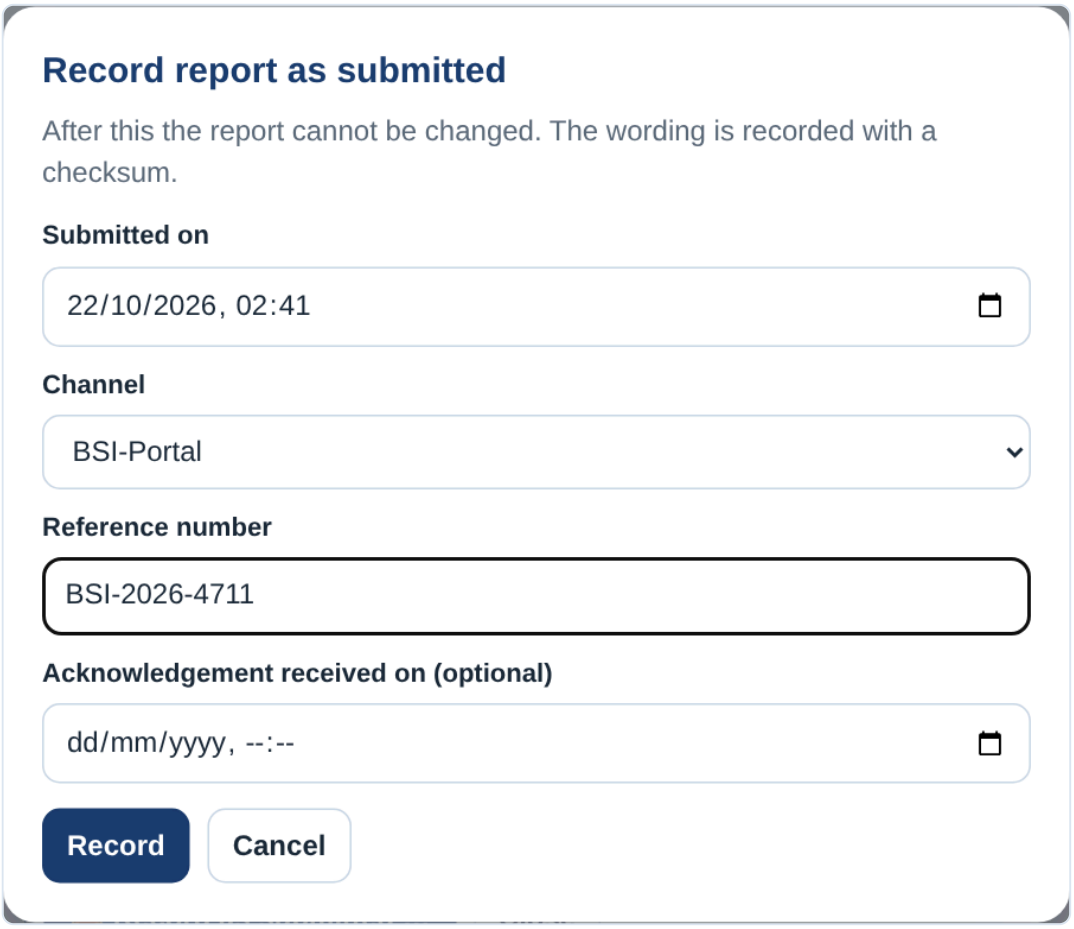


Fig. 10: Recording the submission with time, channel and reference number

In the dialog, enter the submission time, channel, reference number and, if applicable, the receipt of the confirmation. If the report text was copied and changed afterwards, REPORT asks which wording was submitted – the last copied or the current one. REPORT records exactly this wording with its checksum.

After that the report is unalterable. Reports that can be made several times, such as intermediate reports and updates, can be created again.

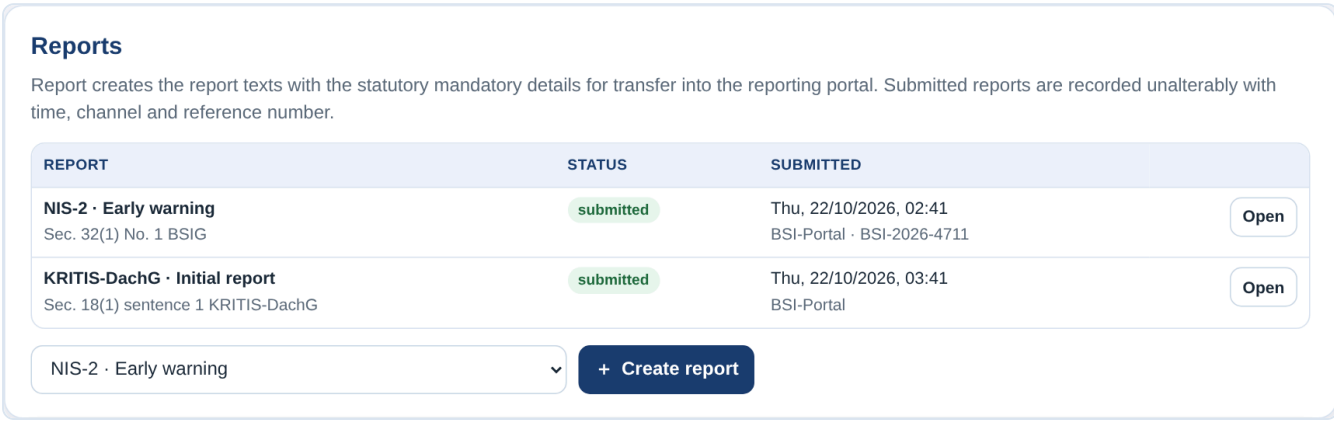


Fig. 11: Overview of the reports with status and submission

Reports not yet submitted remain as drafts in the file. Changes to drafts are kept when saving, but only the submission is recorded unalterably.

8. Timeline

The timeline collects events and measures for the reports and the final report. REPORT enters the awareness and submitted reports itself.

- Own entries with time, type (event, measure, decision, communication, report, other) and content via *Add entry*.
- Entries are not deleted but struck out with a reason. They remain in the verification chain.

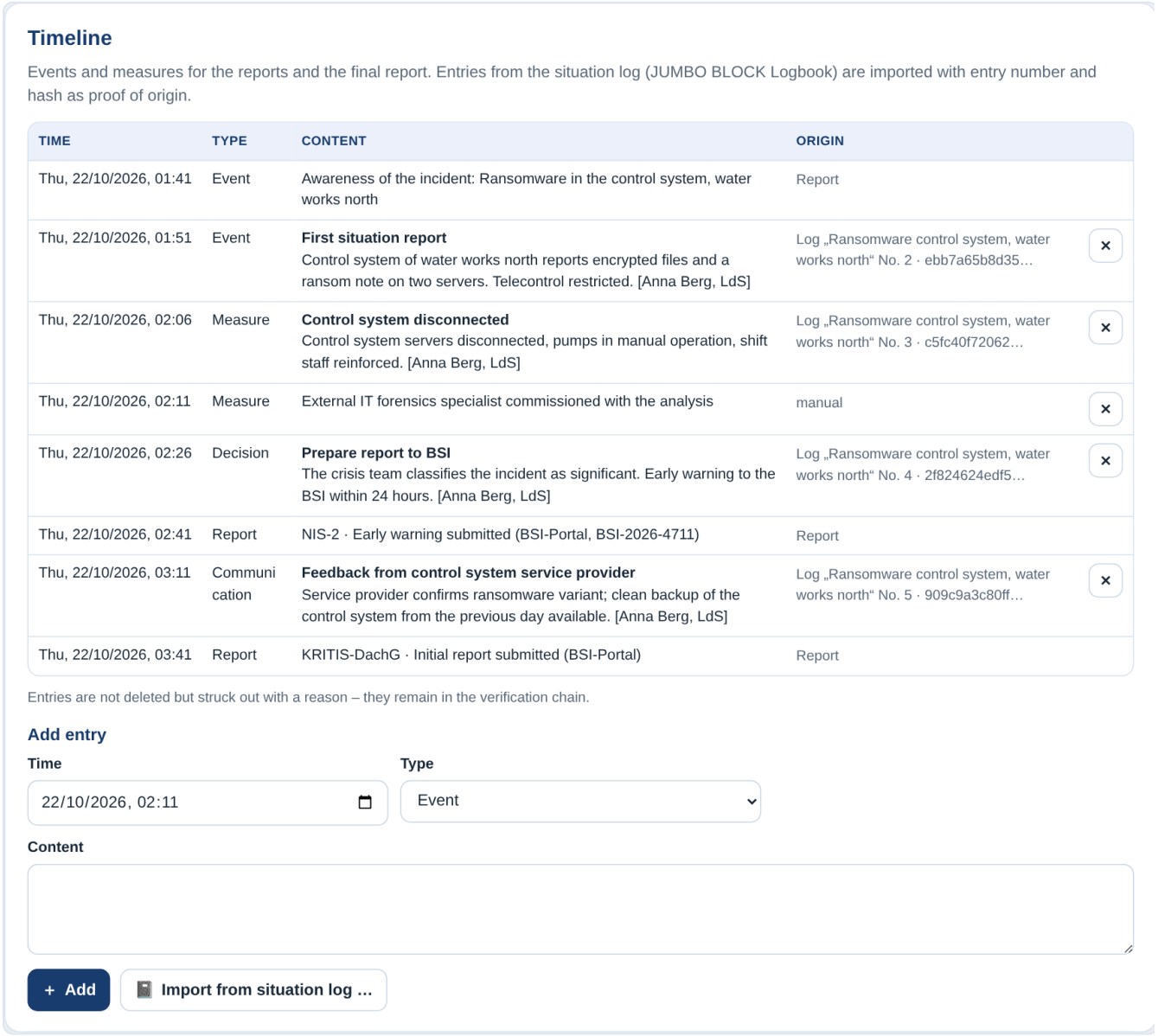


Fig. 12: Timeline with own entries and entries from the situation log

Importing from the situation log

Import from situation log … opens a JUMBO BLOCK LOGBOOK file with its password – read-only; the situation log is not changed. REPORT verifies the log's hash chain and lists the entries.

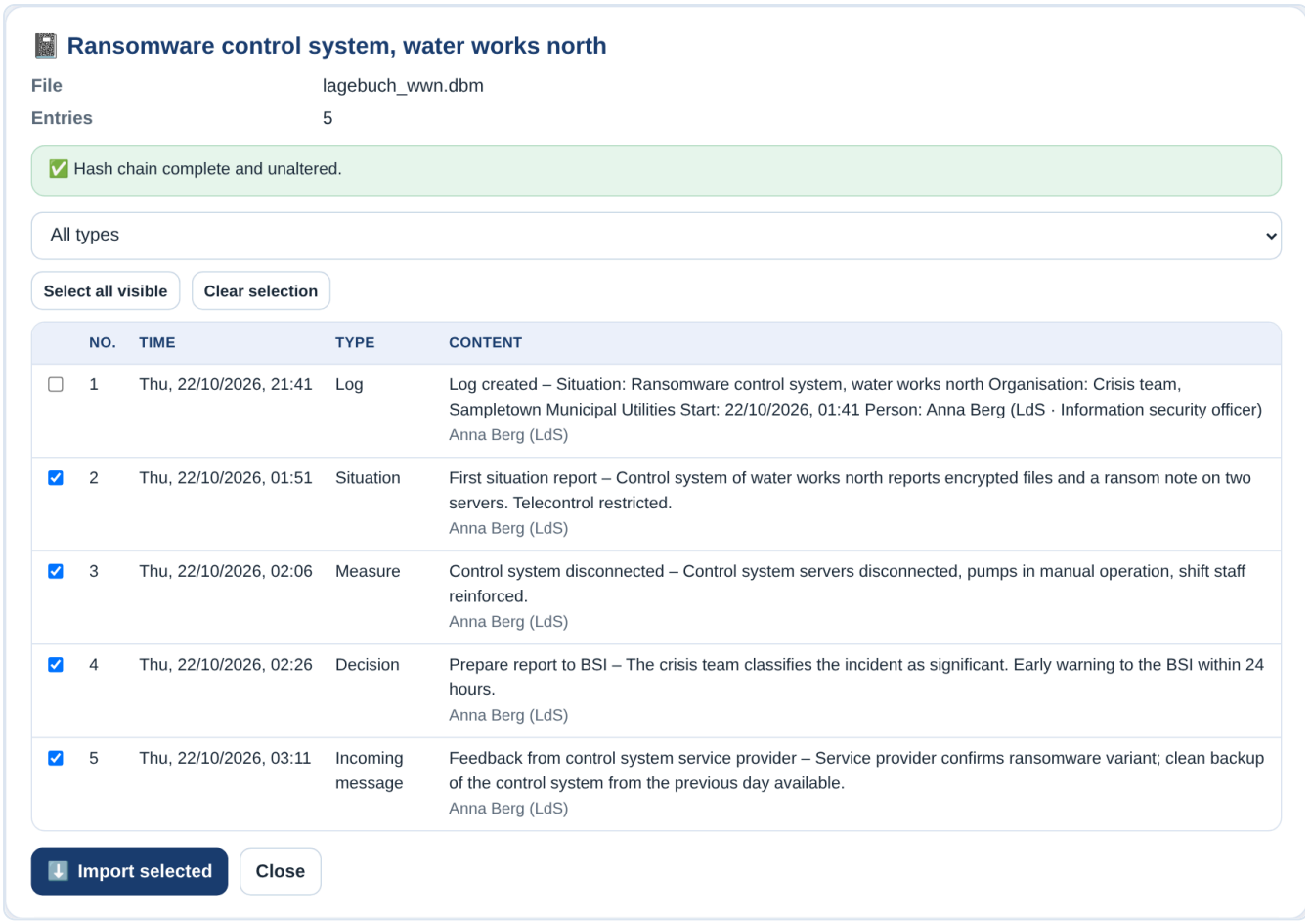
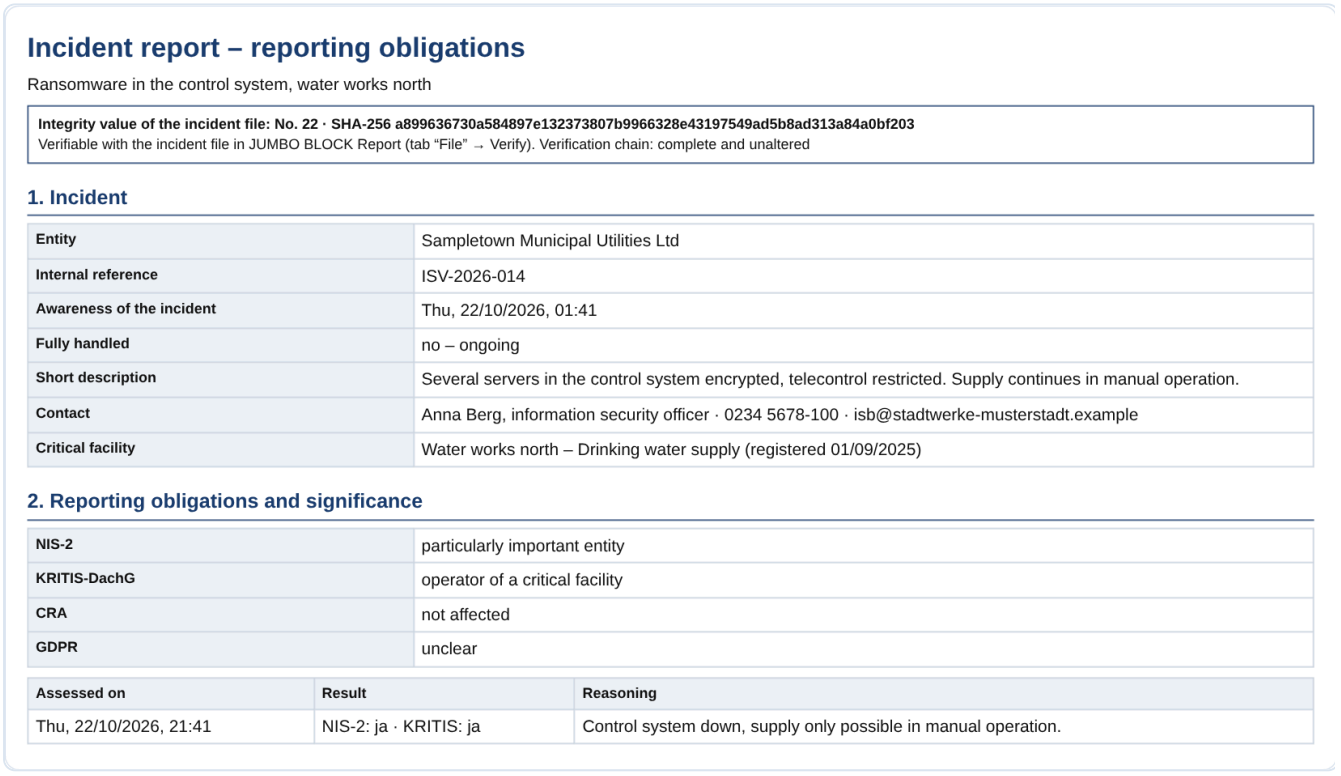


Fig. 13: Selecting entries from the situation log

Tick the desired entries (filter by type, *Select all visible*) and click *Import selected*. Every imported entry carries the log, number and hash as proof of origin. Entries already imported are not added twice.

9. Report

The *Report* tab creates the documentation of the incident. *Print / PDF* prints it or saves it as PDF.



Incident report – reporting obligations

Ransomware in the control system, water works north

Integrity value of the incident file: No. 22 · SHA-256 a899636730a584897e132373807b9966328e43197549ad5b8ad313a84a0bf203
Verifiable with the incident file in JUMBO BLOCK Report (tab “File” → Verify). Verification chain: complete and unaltered

1. Incident

Entity	Sampletown Municipal Utilities Ltd
Internal reference	ISV-2026-014
Awareness of the incident	Thu, 22/10/2026, 01:41
Fully handled	no – ongoing
Short description	Several servers in the control system encrypted, telecontrol restricted. Supply continues in manual operation.
Contact	Anna Berg, information security officer · 0234 5678-100 · isb@stadtwerke-musterstadt.example
Critical facility	Water works north – Drinking water supply (registered 01/09/2025)

2. Reporting obligations and significance

NIS-2	particularly important entity
KRITIS-DachG	operator of a critical facility
CRA	not affected
GDPR	unclear

Assessed on	Result	Reasoning
Thu, 22/10/2026, 21:41	NIS-2: ja · KRITIS: ja	Control system down, supply only possible in manual operation.

Fig. 14: Incident report with integrity value line

Section	Content
1. Incident	All incident details, awareness, status, reporting contact
2. Reporting obligations and significance	Classification and all recorded assessments
3. Deadlines	All reports with deadline and status, legal status of the rule table
4. Submitted reports verbatim	Every submission with time, channel, reference number and exact text
5. Timeline	All entries not struck out, with origin
6. Signatures	Signed states of the file
7. Verification chain	All entries of the verification chain with hash

Every page carries the integrity value of the file at the time of printing in its footer.

10. File, verification chain and signature

Saving the incident file

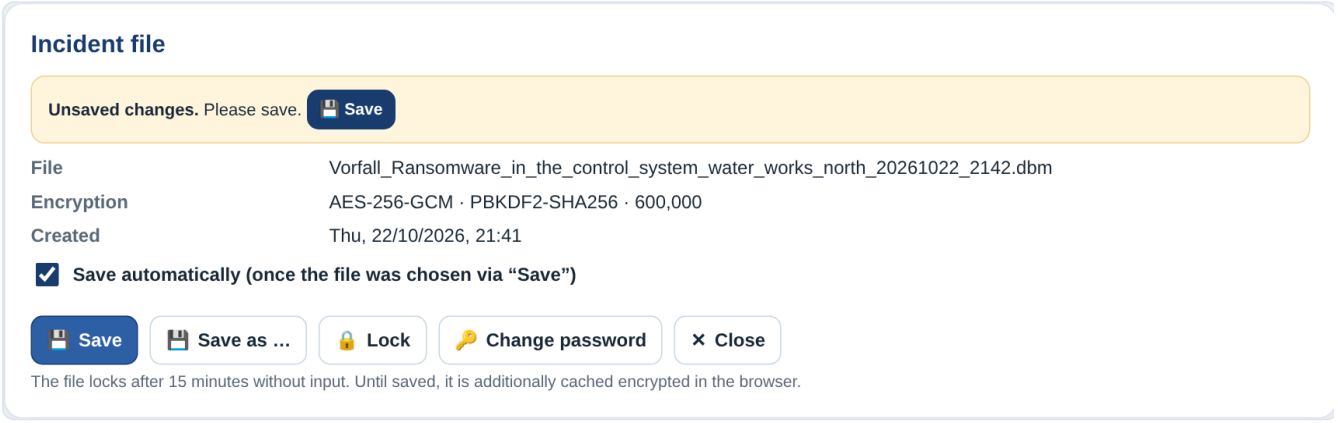


Fig. 15: Incident file with save, lock and automatic saving

Button	Effect
Save / Save as …	Saves the file encrypted. In Chrome and Edge the same file is overwritten on the next save; with *Save automatically* after every change.
Lock	Removes the key from memory
Change password	New password; save afterwards
Close	Closes the file; REPORT asks if there are unsaved changes

Verification chain and integrity value

Every relevant action – creation, details, awareness, assessment, request, timeline, strike-out, submission, closure, password change, signature – is recorded as an entry with time and SHA-256 hash. The integrity value is the hash of the last entry. Once it is held by an authority, in the situation log or in a signature, the file cannot be altered afterwards without detection.

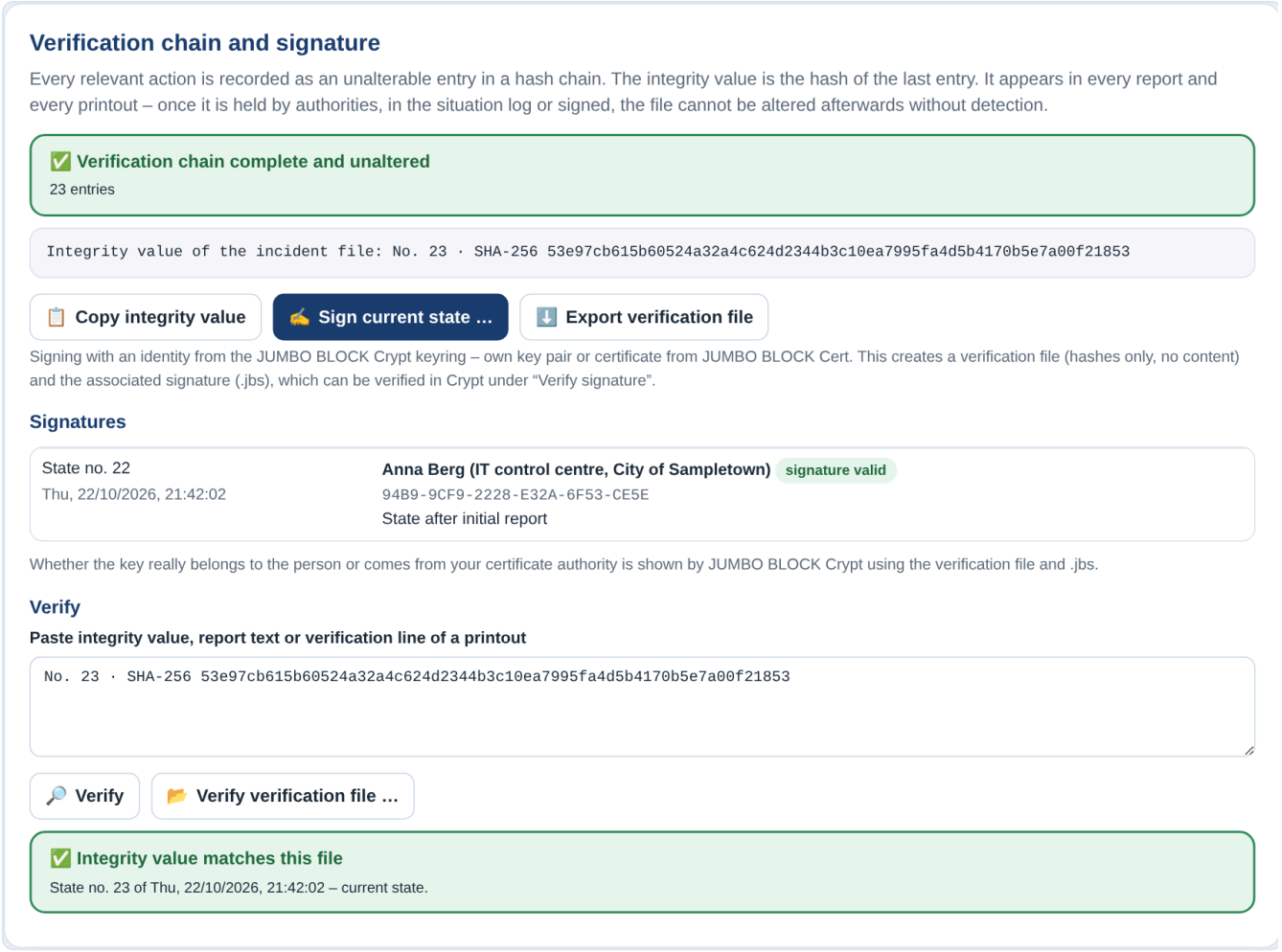


Fig. 16: Verification chain, signature and verification

Signing the current state

Sign current state … opens a JUMBO BLOCK CRYPT keyring (read-only) and signs the current integrity value with an identity – own key pair or certificate from JUMBO BLOCK CERT. Optionally a note is given, e.g. “State after initial report”.

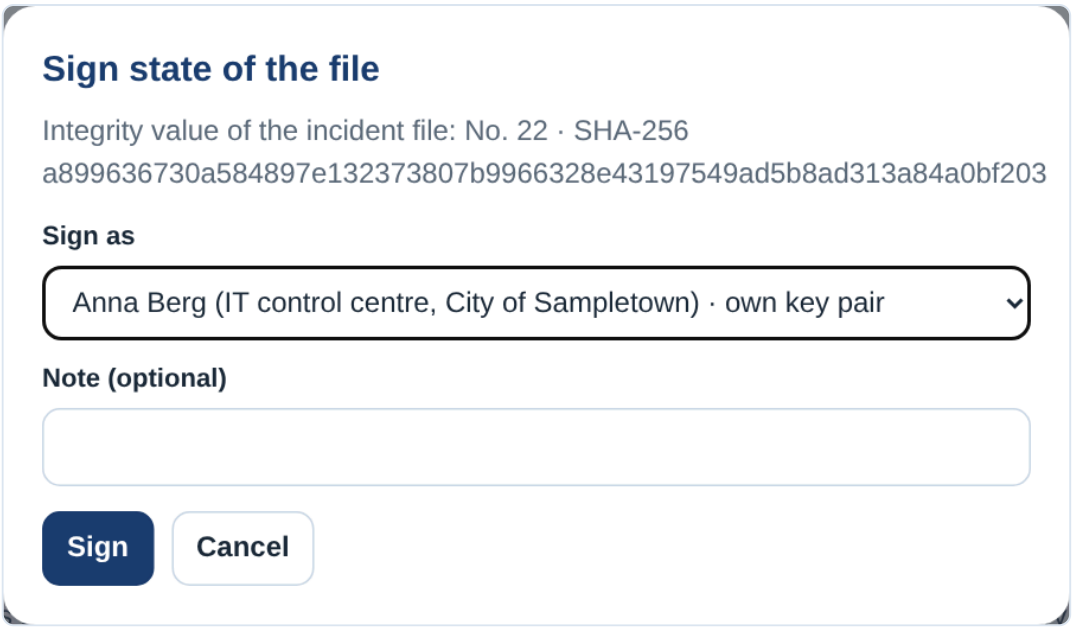


Fig. 17: Signing the state of the file

This creates a **verification file** (hashes only, no content) and the associated **signature file (.jbs)**. Both can be passed on – e.g. to management, supervisory authority or insurer – and verified in CRYPT under *Verify signature*. The signature is also recorded in the file.

Verifying

Under *Verify* an integrity value, a complete report text or the verification line of a printout can be pasted. REPORT shows whether the integrity value matches this file and – for a report text – whether the wording matches a submitted report. *Verify verification file …* compares a verification file with the incident file. *Export verification file* creates a verification file without signature.

Verification chain (log)

NO.	RECORDED	ACTION	HASH
23	Thu, 22/10/2026, 21:42:02	State no. 22 signed by Anna Berg – State after initial report	53e97cb61 5b60524…
22	Thu, 22/10/2026, 21:41:59	Timeline: Thu, 22/10/2026, 03:11 – Feedback from control system service provider – Service provider confirms ransomware variant; clean backup of the control system from the previous day available [Log „Ransomware control system, water works north“ No. 5 · 909c9a3c80ff…]	a89963673 0a58489…
21	Thu, 22/10/2026, 21:41:59	Timeline: Thu, 22/10/2026, 02:26 – Prepare report to BSI – The crisis team classifies the incident as significant. Early warning to the BSI within 24 hours. [Anna Berg, LdS] [Log „Ransomware control system, water works north“ No. 4 · 2f824624edf5…]	ab9b8016c 3ec39b3…
20	Thu, 22/10/2026, 21:41:59	Timeline: Thu, 22/10/2026, 02:06 – Control system disconnected – Control system servers disconnected, pumps in manual operation, shift staff reinforced. [Anna Berg, LdS] [Log „Ransomware control system, water works north“ No. 3 · c5fc40f72062…]	aa8a4c924 d7eca66…
19	Thu, 22/10/2026, 21:41:59	Timeline: Thu, 22/10/2026, 01:51 – First situation report – Control system of water works north reports encrypted files and a ransom note on two servers. Telecontrol restricted. [Anna Berg, LdS] [Log „Ransomware control system, water works north“ No. 2 · ebb7a65b8d35…]	4ec4bbad8 6dc0ffc…
18	Thu, 22/10/2026, 21:41:54	Timeline: Thu, 22/10/2026, 02:11 – External IT forensics specialist commissioned with the analysis	5de39fe8e aefa058…
17	Thu, 22/10/2026, 21:41:52	Timeline: Thu, 22/10/2026, 03:41 – KRITIS-DachG · Initial report submitted (BSI-Portal)	660b90fad 4a2c0a7…
16	Thu, 22/10/2026, 21:41:52	Report submitted: KRITIS-DachG · Initial report – Thu, 22/10/2026, 03:41 · BSI-Portal · SHA-256 22ec3020f93b4324…	4070a4aed ac4b928…
15	Thu, 22/10/2026, 21:41:51	Timeline: Thu, 22/10/2026, 02:41 – NIS-2 · Early warning submitted (BSI-Portal, BSI-2026-4711)	75ee08965 0833a84…
14	Thu, 22/10/2026, 21:41:51	Report submitted: NIS-2 · Early warning – Thu, 22/10/2026, 02:41 · BSI-Portal · BSI-2026-4711 · SHA-256 53a3dae597b97ea4…	7588a556f d86a8b3…
13	Thu, 22/10/2026, 21:41:47	Significance assessed: NIS-2 ja · KRITIS ja – Control system down, supply only possible in manual operation.	f2afa0044 df88c09…
12	Thu, 22/10/2026, 21:41:47	Detail: dsgvo = unklar	4cb502f00 12e4cf5…
11	Thu, 22/10/2026, 21:41:47	Detail: registriert = 2025-09-01	81f03df9f

Fig. 18: Verification chain (log)

11. Interaction with other programs

Program	Interaction
JUMBO BLOCK LOGBOOK	Situation log entries are imported into the timeline with number and hash. The log is only read.
JUMBO BLOCK CRYPT	Keyring identities sign the state of the file; verification file and signature are verified in CRYPT.
JUMBO BLOCK CERT	Personal certificates of your own certificate authority as identities in the keyring
JUMBO BLOCK KRITIS	Background and self-assessment on KRITIS-DachG, NIS-2 and CRA before an incident

12. Security and technology

Area	Implementation
Incident file	AES-256-GCM, PBKDF2-SHA-256 with 600,000 iterations; additional SHA-256 checksum of the file
Verification chain	SHA-256 per entry over the canonically ordered content including the predecessor's hash; starting with “GENESIS”
Submissions	Wording and SHA-256 checksum of the submitted report text
Signature	ECDSA or RSA with the identity from the CRYPT keyring; format compatible with CRYPT
Deadlines	Rule table with legal status 22/10/2026; hour and day deadlines exact, monthly deadlines up to the same day and time of the following month
Privacy	No network connection, no telemetry; caching only encrypted

Limits

- REPORT does not replace a legal review. Details of the reporting procedures and content are specified by BSI, BBK and the supervisory authorities.
- REPORT does not transmit reports itself; submission takes place via the portals of the competent bodies.
- The deadlines depend on the correctly recorded awareness and on the device clock.
- Changes in the law after the stated legal status are not taken into account.

13. Troubleshooting

Problem	Cause and solution
An expected report is missing from the deadlines	Check the details in the *Incident* tab: classification, significance, KRITIS registration (obligation only 10 months later), CRA boxes, GDPR.
CRA final report without deadline	Enter the time of the available corrective or mitigating measure in the *Incident* tab.
“The time lies before awareness”	Check the submission time or correct the awareness with a reason.
“Integrity value does NOT match this file”	The value belongs to another file or was transferred incorrectly. Format: “No. 12 · SHA-256 …”.
“The wording does not match any report recorded as submitted”	The pasted text was changed or the submission has not yet been recorded.
Situation log cannot be imported	Check the log's password. If the log's hash chain is broken, REPORT shows a note.
“signer does not match key”	Verification file and signature file do not belong together. Use both files from the same signing process.
File lost after a crash	Reload the start page; the cached state is offered for restoration.