Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/maritime-assessment-deliverables/

PREVIEW THE RECORD BEHIND A MARITIME CYBERSECURITY ASSESSMENT

Maritime Assessment Deliverables, So You Know the Report Before You Commission It

A report management can act on states what was examined, what the evidence supports, which questions are open and who owns each correction. This preview shows you that kind of report, and (800) 868-8189 reaches the people who write it.

A Record Built to Support the Next Decision

Every section of the report makes clear what was examined, what the evidence supports and which questions are open, and its structure connects each technical condition to the operation it affects, the person accountable for correcting it and the evidence that will verify the result. That structure gives a terminal manager, a Cybersecurity Officer and an insurer a record each of them can use for a different decision on a single reading.

Use this preview to discuss the outputs of an engagement before it is agreed. It describes, in general terms, the eight records an engagement produces, which are the ones an auditor reviewing the engagement later will expect to find. Client findings belong in an engagement's own report, and regulatory compliance determinations rest with the officials the rule names.

If management is weighing what to do after an earlier report, describe the decision it had to support and a senior practitioner will explain how this record would be structured for it.

Scope and Responsibility Record

The record states the assessment purpose, the facilities, systems and boundaries covered and the relevant dates, and it identifies the owner, operator, tenants, vendors and contacts responsible for authorization and operating safeguards. When a port authority commissions the work and a tenant owns the crane controls, this is where that arrangement and the tenant's own approval are written down, with the signature date beside each.

It describes the methods used, the operating conditions, the exclusions and the areas left for later testing. A technical workstream or a gap review is identified accurately as what it is, and the vessel systems that sat outside the work while the ship was alongside are listed here as exclusions, so the asset count stays complete.

In practice the section covers the purpose, operating boundary and responsible parties; the authorized methods and the evidence reviewed with its dates; the excluded systems, third party boundaries and operating constraints; and the scope changes and open evidence items recorded as the work progressed. A reader can tell from this section alone the scope each conclusion in the rest of the report rests on.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Who authorizes what is the question the preparation guide helps you settle before the scope record is written.

Asset, Access and Dependency Record

This section summarizes the relevant assets, the supporting IT services, the communications and the outside connections, and it identifies which records support each described relationship and which relationships are marked for further verification. Each asset relationship is marked as observed, taken from a configuration export or supplied by a vendor or operator, because those three carry different weight when a finding built on them is challenged.

The detail covers the network boundaries between the business network, the terminal operating system, the crane and yard control networks and the vessel interfaces, the vendor access paths and the gateways they pass through, the identity dependencies that operational workstations rely on, and the systems a selected operating function such as gate processing or crane operation depends on. Restricted architecture and configuration information belongs in the controlled technical material, separate from the summary that circulates.

Operators who already hold an asset inventory and a current diagram can call (800) 868-8189 and have the dependency record scoped around them.

Findings That Separate Fact From Inference

Each finding identifies the observed condition and its source, the affected systems and the relevant operating consequence. It explains how that consequence was inferred and which assumptions and untested areas bound the conclusion, so every reader can tell observation from inference and weigh the finding accordingly, including a vendor asked to respond to it.

Severity and priority reflect the agreed operating context of the terminal or vessel. A finding that a crane control network is reachable from the business network is written at the level the evidence supports: an allowed rule, an observed session or a demonstrated reach are three different findings.

A complete finding carries the observed condition and its supporting evidence identifiers, the collection or review date and method, the affected assets and operating dependencies, the reasoned consequence with its stated confidence and assumptions, and the recommended next step with the evidence needed to verify it. Status is Observed, Suspected or Unresolved, and the three words are used as defined.

Ask us how severity would be agreed for your terminal before the first finding is written; that is settled in the scoping call.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Corrective Actions With an Owner and a Verification Path

The action register connects each finding to a responsible owner, the proposed corrective work, its priority and the evidence that will show completion. It records the dependencies and operating constraints that affect scheduling, which in a port usually means the crane vendor's availability, the next vessel call and the gate's peak hours.

A recommended change, an implemented change and a verified result are kept distinct with their own dates. Retesting or configuration validation is defined as follow up work with its own approval, and open items stay visible on the register until someone closes them with evidence. The register a terminal can stand behind a year later is the one where every closure rests on evidence.

Each entry carries the finding reference and corrective objective, the responsible party and any vendor or engineering dependency, the priority, target date and operating conditions, the implementation status with its supporting evidence, and the verification criteria, results and remaining issues.

Vendor windows and vessel movements belong in the scoping conversation, so raise them when you describe the facility and the register will be built around them.

Recovery and Evidence Readiness Record

The record documents the selected restoration dependencies, the available backup and configuration evidence and the access, software, licensing and vendor support a recovery of the terminal operating system or a control network would require. If a representative recovery procedure was examined, it states the conditions, the result and the scope of that work, and it distinguishes a restore that was demonstrated from one that was described.

It records the logging, time synchronization, isolation and preservation arrangements, and it identifies where adding evidence sources or extending retention would support a later incident examination. A readiness review records which systems have been restored and tested, so management knows exactly where recovery stands.

Want to know how much of your recovery evidence already exists? Call (800) 868-8189 and walk a senior practitioner through the backup and vendor arrangements you have today.

Technical Material for Planning and Review

Where the engagement agrees it, the report provides a requirements and evidence crosswalk, technical plan support material and an unresolved issue register for the owner, the Cybersecurity Officer and the relevant advisers, and it states the scope of the technical contribution so the plan author knows exactly which evidence it may rely on.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Plan authorship, filing, independent audit and regulatory approval are separate responsibilities that stay with the owner and the officials the rule names. The crosswalk sets out the evidence and the open items against each requirement, marks the requirements the engagement examined and those outside its scope, and leaves compliance certification and approval with those officials.

Management Summary and Restricted Technical Readout

Management needs the operating implications, the priorities, the ownership and the decisions required of it, in a document that can be read in the time between two meetings. Technical teams need enough controlled evidence to understand each finding and perform the authorized follow up work, including configuration versions, affected boundaries and the exact acceptance criteria for closure. The two readouts serve different readers and are written that way.

The audience, the handling restrictions and the review process are agreed before delivery, and the restricted readout is marked and delivered through the controlled exchange. Completion means the contracted outputs and the review are finished, with the scope of the conclusions and the remaining risks stated.

Tell us who will read each readout when you describe your maritime assessment, and we will agree on the handling restrictions before the first draft.

Choose the Output Your Facility Requires

An initial assessment, a validation of selected controls and a recurring assurance program each need different deliverables. Bring the decision, the operating boundary and the work that already exists to a scope discussion, and we will agree on the evidence and the review that purchase needs. The first consultation is free, and the preparation guide shows what to gather first.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.