Revision	Date	Modification notes
A	**29.03.2023**	First Issue
B	**21.07.2023**	Secondary Version Issue

Table of contents

1.0 Purpose

The purpose of this document is to set out the rules of engagement and accepted practices for auditing of Information Technology (IT) and Information Security Management Systems (ISMS) at GKN Automotive. GKN Automotive has a defined Policy [REF1] (and procedure) that sets out the requirements (and approach) for Information Security Auditing. The practices set out in this document are supportive of that policy.

Who should read this procedure document?

You should read this procedure document if

1. You are a representative of an organisation intending to carry out any auditing of GKN Automotive’s IT and or ISMS.
2. You are a GKN Automotive member of staff or department who is required (or intending) to carry out any auditing of GKN Automotive’s IT and or Information Security Management System.
3. You are leading or supporting activities involving the audit of any part of GKN Automotive’s IT/ISMS
4. You are supporting, responding to or responsible for any IT / ISMS Audit compliance related tasks that support GKN Automotive’s objective of meeting its legal, regulatory, contractual, and internal requirements.

2.0 Scope

This document applies to:

- All information security compliance, assurance and audit activities across GKN Automotive IT, engineering, physical, prototype and personnel assets including those owned, contracted, leased, or operated by GKN Automotive and its subcontractors and third parties (e.g., cloud services and externally hosted systems).
- All internal audit activities across GKN Automotive.
- Third parties, contractors and suppliers who are providing services to GKN Automotive or its parent company.
- Customers of GKN Automotive or its parent company.
- Audit reports issued by any external party that have a requirement to audit GKN Automotive (e.g. Investors, External Auditor, International Automotive TaskForce (IATF) Auditor, Trusted Information Security Assessment Exchange (TISAX) Auditor, customers, owners etc); and
- GKN Automotive employees.

This document is a supporting component of the GKN Automotive Information Security Management System (ISMS). Adherence to the procedures outlined within is recommended and will support adherence to the associated information security audit policy.

Where can I find out more information about GKN Automotive’s information security Audit policies and procedures?

If you require additional information regarding GKN Automotive’s information security policies, or need further assistance, please email GSO.Audit@GKNAutomotive.com

3.0 Rules of Engagement for IT and ISMS Auditing

The guidelines and principles below outline the expectations of GKN Automotive for any organisations or departments wishing to carry out a review on its IT or Information Security Management System.

3.1 Audit notification

To increase the chances of successful and valuable audit taking place, any request for audit to be carried out on our IT or ISMS must be officially raised **at least 1 month before the audit** is carried out to our Global Security Office Audit Team at the below email:

GSO.Audit@gknautomotive.com

The audit notification should outline clearly:

- The organisation/body requesting the audit.
- The main organisational contact representative for the audit programme.
- The reason for the audit.
- Any compliance requirements.
- The objective of the audit (what is the intended outcome).
- Where possible, outline the impact of the audit not being carried out (financial/regulatory penalties).
- The expected audit timelines (start and completion date).
- Where possible there should be a note about any similar previous audits done and who the main contact was at GKN Automotive.

3.1.1 Timely Audit notification for non-IT/ISMS Audits

Where the audit being requested/carried out is not centrally driven by IT/ITSMS but includes some IT/ISMS related requests/queries, the GSO Audit office must be notified within 24 hours of the audit notification being received by the relevant GKN Automotive team.

3.2 Audit Introductory (opening) meetings

It is strongly recommended that there is an introductory meeting between the auditing organisation and the GKN Automotive audit office to help clarify the audit requirements or information requested. Equally this will help agree or establish:

- Any challenges that could prevent the audit objectives being met.
- Audit schedule.
- Audit methods (remote/onsite).
- Audit information sharing.
- Communication channels for the duration of the audit.
- The authority of the organisation requesting, to conduct the audit.

- The extent of the disclosure and the treatment of confidential information for the duration of the audit.
- Any legalities required to be put in place to satisfy non-disclosure agreements between the requesting party and GKN Automotive.
- Any need for guides/translators if the audit is not to be conducted in English (or where documentation may not be available in English).
- The impact of audit findings or audit results (possible penalties or contract breaches).

4.0 Roles, Responsibilities and Competence

GKN Automotive requires that the individual(s) managing any requested audits on our IT/ISMS have the necessary competence to manage the programme of activities and its associated risks and external (or internal) issues effectively, including knowledge of:

a) Audit principles methods and processes;
b) Management system standards, other relevant standards and reference/guidance documents;
c) Information regarding GKN Automotive and its context (e.g., external/internal issues, relevant interested parties and their needs and expectations, business activities, products, services and processes of the auditee);
d) Applicable statutory and regulatory requirements and other requirements relevant to the business activities of the auditee.
e) As appropriate, knowledge of risk management, project and process management, and information and communications technology (IT) may be considered.

4.1 Audit Code of Ethics

As a principle, any individuals hired to carry out auditing of our IT/ISMS should adhere to best practice and recommended ethical principles. The auditor must:

- Perform their work ethically, with honesty and responsibility;
- Carry out audit duties and post audit activities in line with the confidentiality agreed in NDA
- Only undertake audit activities if competent to do so;
- Be sensitive to any influences that may be exerted on their judgement while carrying out an audit;
- Fairly present findings in his reporting (audit results must reflect transparency and honesty);
- Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the audit activities with consideration for any obstacles encountered during the audit that could impact

4.1.1 Audit Confidentiality

All external audits must only be commenced following the agreement and signing of a Non-disclosure Agreement (NDA) between GKN Automotive and the external Auditor. The use of NDAs ensures that the audit process remains confidential and that the information obtained during the audit is not disclosed to unauthorized parties. This is critical because security audits often reveal vulnerabilities that can be exploited by malicious actors if they become public knowledge.

GKN Automotive information and documentation must be handled in line with the GKN Automotive Information Classification, Marking and Handling procedure (Ref 2).

5.0 Scope and Objectives for the Audit

The audit objective should be clear and understood by both the auditing organisation and the GKN Automotive team. It must be defined and agreed right at the very instant of audit notification, what the objective is.

- Why this audit is being requested (the legal, regulatory or compliance drivers)
- What is the intended outcome/output of the audit
- What questions this audit is seeking to answer

The audit scope should equally be consistent with the audit objectives. The audit scope must define key factors as locations, teams and processes to be audited, as well as the time period covered by the audit.

6.0 Audit Criteria

The auditing organisation must clearly define audit criteria that is intended to be used as a reference against which any expected conformity is determined. Audit criteria will be reviewed at the initial/introductory meeting to ensure there is agreement as to their applicability for the context of GKN Automotive's operations. Audit criteria may include applicable policies, processes, procedures, performance criteria including

6.1 Scope, objective or criteria changes

In the event of any changes to the audit objectives, scope or criteria, the auditing organisation must formally notify GKN Automotive, and where applicable, a meeting put in place to discuss the reason for the scope/objective change. Sufficient / reasonable time must be offered to GKN Automotive to review the impact of the scope / objective changes on resource or operational plans and feasibility of continuing with the new audit scope.

7.0 Secure and appropriate collection, sharing and verification of information requested

GKN Automotive will agree with the auditing organisation (during the introductory meeting) what the most appropriate mechanism for collection / sharing of information will be. Where applicable, secure file transfer storage areas may need to be provided by the auditing organisation.

Should any information requested be deemed as highly confidential to GKN Automotive, agreement will be made on the most reasonable mechanism for providing visibility of this to the auditing organisation. E.g. Penetration Testing Reports are usually able to be presented during the audit sessions but are not typically shared.

8.0 Requests for Testing

GKN Automotive reserves the right to establish the risks to it's environment of any testing that is requested by a third party or partner. In order to safeguard the confidentiality, availability and integrity of our data, and that of our customers, we are committed to ensuring comprehensive and effective risk management procedures are carried out in advance of any testing that is deemed a requirement for an audit request.

Should our risk assessments demonstrate a level of risk beyond our defined risk tolerance, we will collaborate with auditors to review alternative solutions to achieve the audit objective.

9.0 Traceability and reporting of findings during the Auditing Process

Depending on the scope of the audit, audit sessions may last up to several days/weeks as information is collected and reviewed by the auditing organisation. GKN Automotive therefore recommends that during the Auditing process:

- Audit sessions (meetings) minutes are recorded by the auditing organisation to ensure clarification as to when and how certain findings were derived
- Findings or observations raised to GKN Automotive’s team are presented in a format that enables direct traceability to the auditing query / criteria that initiated the finding
- Findings are reported in alignment with a qualitative/quantitative risk profile – to easily describe the findings according to a risk priority level
- Any expectations or recommendations for each finding are clearly annotated in the report, e.g., Expected remediation timelines for findings raised

10.0 Audit Reporting and Follow up Meeting

The audit report should be issued within an agreed period. If it is delayed, the reasons should be communicated to GKN Automotive’s GSO Audit Manager.

Upon receipt of the Audit Reporting output, a meeting must take place to officially review the output of the audit carried out and communicate the next expected steps for both parties. This could be considered as the ‘closing meeting’. During this meeting it should be clearly communicated by the auditing organization:

- The organisation’s expectations as to timelines and next steps for how the audit findings should be addressed based on the agreed process
- Possible consequences of not adequately addressing the audit findings
- Agreed mechanisms for continuous sharing of information or updates where applicable
- If follow up sessions are required based on findings or the previous sessions
- Any diverging opinions regarding the audit findings or conclusions between the auditing organization and GKN Automotive’s team should be discussed and, if possible, resolved. If not resolved, this should be recorded for escalation through the relevant routes where necessary.

11.0 References

Ref 1: Information Security Audit Management Policy - DL-06-PY-202
Ref 2: Information Security Classification, Marking and Handling procedure- DL-06-PR-200-ENG