Marking table for Access Control Systems installed to NCP 109 (Issue 4)

NSF 271 - Issue 3

October 2024

This marking table is for use by NSI when inspecting access control systems that have been installed by NSI NACOSS Gold and NSI Systems Silver approved companies to the requirements of NCP 109 (Issue 4).

Demerit points may be given for non-compliance with clauses of NCP 109 (Issue 4) for which no specific reference has been made in the table of deviations listed in this document

National Security Inspectorate
Sentinel House,
5 Reform Road
Maidenhead
SL6 8BY
Website: nsi.org.uk

NCP 109 (Issue 4) marking table

The NCP 109 (Issue 4) marking table is divided into Sections A to G as listed below.

Section	Title	Maximum points
A	NCP 109.4 Clause 4: Classification of Access Points	2
B	NCP 109.4 Clause 5: Design	2
C	NCP 109.4 Clause 6: Equipment Selection and Installation	2
D	NCP 109.4 Clause 7: Installation	2
E	NCP 109.4 Clause 8: Commissioning, handover	2
E	NCP 109.4 Clause 8.3: Documentation	1
F	NCP 109.4 Clause 9: Maintenance	2

Notes

1. Each deviation in this marking table is given a clause reference (for example 5.1), a Code (for example D2) and a Point score (for example 2 points).

3. NSI Inspection Reports detail deviations by Clause, Code, Description, Points.

   Example: NCP 109: 5.1 Access point(s) conflict with Building Regulations and/or Fire Safety regulations - 2 Points

4. Points are awarded for each individual deviation as shown in the marking table.

5. The total number of points awarded results in a grading (A to E). A = 0 points, B = 1-2 points, C = 3-5 points, D = 6-8 points and E = 9 points or more.

   The access control system will normally require a re-inspection if Grade D or E is achieved.

Clause	Code	Deviation	Points
A. NCP 109.4 Clause 4: Classification of Access Points			
4.1	A1	Access points are not classified accurately, with no adjustments for changing risks or the proper use of credentials.	1
4.2	A2	The risk assessment is incomplete or missing, failing to address potential threats from both accidental and malicious actions	1
4.3	A3	Door type and purpose have not been considered and those requiring compliance with EN 179 (Emergency), EN 1125 (Panic) and/or EN 13637 standards have not been identified.	2
4.4	A4	Access points are not correctly classified based on asset value or potential attacker skills.	1
B. NCP 109.4 Clause 5: Design			
5.1	B1	No survey including stakeholder was conducted before design, meaning the system may not reflect the needs of the building and/or end user.	1
5.1	B2	No evidence that the limitation of control for the interface with power sliding doors (provided by others) was neither established nor documented as required.	1
5.1	B3	The system has not been designed/installed to comply with fire or building regulations, potentially hindering safe egress in fire, emergency and/or panic situations.	1
5.1 a) to t)	B4	The survey provides no evidence that the controls, egress, and security requirements listed from a) to t) were considered when designing the ACS to address the identified risks.	2

Clause	Code	Deviation	Points
5.2	B5	Credentials such as memorised codes, tokens, and biometrics are not appropriately selected based on the classification type or operational needs. Battery-powered credentials are also not durable enough for the expected environment which could lead to access control failures.	2
5.3.1	B6	The anti-passback feature is not properly configured or implemented, allowing individuals to re-enter areas without first exiting, which compromises the system's integrity.	1
5.3.2	B7	Door release times are not correctly set for certain access points, leading to doors either remaining open for too long or closing too quickly which could compromise security or user convenience.	2
5.3.3	B8	Access point statuses are not properly monitored or reported, resulting in the system being unable to detect security breaches such as doors being forced open or held open.	2
5.3.4	B9	Critical security events are not being logged consistently or accurately which hampers the ability to audit access events and trace incidents.	2
5.3.5	B10	The system time is not properly synchronised, leading to discrepancies in event logging and potential issues with time-sensitive operations such as credential expiration or access scheduling.	2
5.3.6	B11	The system lacks adequate tamper protection for central control equipment and access point hardware. This leaves the system vulnerable to physical tampering, which could lead to unauthorised access or system malfunctions without proper detection and user notification.	2

Clause	Code	Deviation	Points
5.3.7	B12	The system lacks proper self-protection mechanisms such as tamper detection or secure communication between control units and ACS components which could leave critical parts of the system vulnerable to tampering and unauthorised access.	2
C. NCP 109.4 Clause 6: Equipment selection and installation			
6.1	C01	Control equipment cannot handle required functions, which may limit system performance.	2
6.2	C02	Installed hardware does not meet required classifications or manufacturer specifications. (ie wrong lock type, readers mounted to close)	2
6.2	D03	Readers/exit buttons/Emergency release mechanisms are: ➢ Incorrectly mounted. ➢ Hard to distinguish from Fire call point. ➢ Hard to reach or use.	1
6.2	C04	The physical strength of doors, locks, or frames has not been fully considered, making them vulnerable.	2
6.2	C05	Installed lock, latch, or plate does not meet fire resistance standards, potentially compromising the integrity of the fire-resisting door set. No documented confirmation from the fire door manufacturer regarding the impact of drilling or fixing cables and locks to the door, which could affect the door's fire resistance performance.	2

Clause	Code	Deviation	Points
6.3	C06	One or more of the following have been identified: ➢ Extra-low voltage and mains cables are routed through the same entry point. ➢ Equipment housings lack clear voltage markings. ➢ Cabling has not been installed according to manufacturer recommendations. These issues can lead to safety hazards, interference, and system inefficiency. ➢ The system is not connected to a dedicated mains circuit or un-switched fused spur, increasing the risk of accidental disconnection or failure.	2
6.4	C07	Power supplies are not securely installed making them susceptible to tampering which could disrupt system operations	2
6.4	C08	The power supplies do not meet the required load capacity, risking power failures during high-demand periods.	2
6.4	C09	Power supplies are not securely installed, making them susceptible to tampering which could disrupt system operations.	2
D. NCP 109.4 Clause 7: Installation			
7.1	D01	One or more of the following have been identified: ➢ Readers are not securely mounted or placed conveniently for all users, including those with disabilities. ➢ Fire door hardware installation did not follow manufacturer guidelines, potentially compromising safety. ➢ Control equipment is poorly positioned, leading to issues such as personal injury, poor ventilation, limited maintenance access, or noise. ➢ Security measures like visibility of sensitive data are inadequate. ➢ Incorrect door hardware fitted based on door type and purpose.	2

Clause	Code	Deviation	Points
7.1.1	D02	Fire-resistant fixings have not been used in the installation of some cables, which could cause them to fail prematurely in the event of a fire. The installation does not comply with BS 7671, leading to potential safety risks, including improper wiring, termination and/or insufficient insulation.	2
7.1.1	D03	One or more of the following have been identified: ➢ The cables used do not fully comply with manufacturer recommendations or required performance standards for connected devices. ➢ Some cables are not properly concealed or mechanically protected, leaving them vulnerable to damage or tampering. ➢ Extra-low voltage cable connections are not terminated securely within appropriate junction boxes, leading to potential system malfunctions.	2
7.1.2	D04	The selected cables do not meet the required performance standards required to handle data transfer rates and protect against electromagnetic interference, leading to potential data loss or system slowdowns.	2
7.1.2	D05	One or more of the following have been identified: ➢ Test results for wire mapping, short/open circuits are either incomplete or undocumented. ➢ Network cabling exceeds the recommended distances, ➢ No Cross-reference chart or running out diagram showing the relationship between cables and devices has been created and/or is not available to the maintenance engineer for complex networks topology.	1

Clause	Code	Deviation	Points
7	D06	➢ Components such as Cat 5e and Cat 6 cables/connectors are mixed, ➢ Termination does not comply with the required T-568B standard with no justification if using a different standard. ➢ Labelling of cables at termination points is either unclear or absent, complicating maintenance and servicing.	1
7.1.3	D07	The voltage and current at the end of some cable runs are insufficient to operate the equipment reliably, indicating that the cables are not rated properly for the required load and length.	1
7.2	D08	The system design or as-fitted document does not clearly assign responsibility for critical software and firmware updates, leaving the ACS vulnerable to known security issues due to outdated software.	1
7.2	D09	Insufficient security measures are in place to protect the ACS or network from unauthorised access. Firewalls, access controls, and malware protection are either missing/poorly configured or out of date, increasing the risk of cyber-attacks.	2
7.2	D10	➢ One or more of the following have been identified: ➢ Default login credentials were not changed, and/or wireless networks are inadequately secured, leaving the system exposed. ➢ External access points lack proper firewall and authentication protocols, increasing the risk of unauthorised access.	2

Clause	Code	Deviation	Points
7.2	D11	One or more of the following have been identified: ➢ VLANs or endpoint security measures were not implemented, and/or external devices were connected without documented customer permission. ➢ External devices also lacked up-to-date software and/or system updates. ➢ The customer IT policies were not fully considered, increasing the risk of network compromise.	1
E. NCP 109.4 Clause 8: Commissioning, handover			
8.1.1	E01	The following required checks have not been verified during commissioning: ➢ Wiring terminations, voltage checks, and hardware alignment with the specification were incomplete or incorrectly verified. ➢ Security functions, including emergency release mechanisms, door release times, and software updates, were either untested or improperly configured. ➢ Unused ports and protocols were not disabled, and permissions for user accounts and maintenance passwords were not documented.	1
8.2	E02	The handover process does not include all requirements a) to J) as such the handover process was incomplete: ➢ Inadequate user training on system operations and maintenance responsibilities, and failure to provide necessary documentation. ➢ Cybersecurity measures, backup procedures, and legal obligations (e.g., Data Protection Act, UK GDPR) were not fully explained. ➢ Software licenses, permissions for user codes, and remote access details were either not provided or documented,	1
8.2	E03	The correct NSI certificate not issued within the required timescale.	1

Clause	Code	Deviation	Points
E. NCP 109.4 Clause 8.3: Documentation			
8.3	E04	No documented risk assessment was produced as part of the design process, leaving potential risks unaddressed and impacting the overall effectiveness of the ACS	1
8.3	E05	The system design proposal did not fully account for all customer requirements, features, and any limitations or exclusions. User responsibilities were either unclear or missing from the documentation.	1
8.3	E06	The system design proposal failed to specify the required standby power duration or the number of activations per hour for relevant access points, risking insufficient power in case of mains failure.	1
8.3	E07	The system design proposal was not formally reviewed and agreed upon with the user or their representative, which may lead to misunderstandings or unmet expectations regarding system functionality.	1
8.3	E08	The as-fitted document is incomplete missing information detailed in 8.3 a) to l), lacking key information such as: ➢ Address of Installation ➢ Access point Locations and classifications, ➢ Power supply standby periods and details, ➢ Emergency override methods. ➢ Warning device positions ➢ Firmware/Software versions ➢ Manufacturer key documentation ➢ Configuration settings This could lead to operational ineffectiveness or safety risks.	1
F. NCP 109.4 Clause 9: Maintenance			
9.1.1	F01	The maintenance organisation lacks sufficient spare parts, documentation, or control over equipment necessary to comply with the Code of Practice, potentially leading to delays in system repairs and operational issues.	1

Clause	Code	Deviation	Points
9.1.1	F02	The customer has not been adequately advised to establish a maintenance agreement for fire exit access points or to consider a software Support/System Backup agreements for computer-based ACS systems.	1
9.1.2	F03	Service technicians do not have access to appropriate tools and equipment to maintain the ACS.	1
9.2.1	F04	Preventative maintenance visits not carried out every 12 months (+/- one month) from the date of commissioning.	1
9.2.2	F05	No evidence that the required preventative maintenance checks were carried out as detailed in a) to i).	1
9.2.2	F06	Lack of documentation: There is no documentation indicating the current versions of the installed software or firmware. No coordination with the customer: Where updates could not be applied during the inspection, no efforts have been made to coordinate with the customer for scheduling these necessary updates.	1
9.2.2	F07	Maintenance items not completed during the visit were not properly documented or agreed upon with the customer, and/or security reductions/faults identified were neither recorded nor addressed in a timely manner.	1
9.3	F08	A corrective maintenance facility is not organised and/or located to meet the agreed response times under normal circumstances.	1
9.4.3	F09	Preventative maintenance record(s) not available and/or do not contain the required information.	1
9.4.4	F10	Corrective maintenance record(s) not available and/or do not contain the required information.	1
9.4.5	F11	Temporary disconnection record(s) not available and/or do not contain the required information.	1