Onboarding of New Staff in Critical Information Systems: A Risk-Based Framework with Evidence from the Portuguese Regulatory Context

Ana C. G. R. Almeida *, Mario Monteiro Marques, Antonio Goncalves

Posted Date: 2 June 2026

doi: 10.20944/preprints202606.0125.v1

Keywords: classified information; onboarding; human error; security training; insider threat; GDPR; NIS2; SEGNAC; CNPD; CNCS; Portugal

 doi:10.20944/preprints202606.0125.v1

Article

Onboarding of New Staff in Critical Information Systems: A Risk-Based Framework with Evidence from the Portuguese Regulatory Context

Ana C. G. R. Almeida [1,*], Mario Monteiro Marques [2] and Antonio Goncalves [2]

[1] Instituto Superior Técnico, University of Lisbon

[2] CINAV, Portuguese Naval Academy

* Correspondence: ana.c.almeida@tecnico.ulisboa.pt

Abstract

New staff placed in classified or sensitive environments before completing mandatory training are a well-documented source of security incidents, yet the operational pressure to grant provisional access remains widespread in Portuguese public bodies and regulated private entities. The findings are particularly relevant for critical information systems supporting public administration, critical infrastructure operators, defence organisations and other environments where personnel security directly influences operational continuity and organisational resilience. This article examines the risks of pre-certification deployment, identifies the principal knowledge gaps and procedural weaknesses that appear during the onboarding phase, and proposes a Structured Mandatory Onboarding Programme (SMOP) relatted to the Portuguese and European regulatory context. (1) Background: information classification regimes (SEGNAC), data protection (GDPR; Law no. 58/2019), cybersecurity (NIS2; Decreto-Lei no. 125/2025), and the Cybercrime Law (Law no. 109/2009) all impose training duties on data controllers and operators of essential and important services, yet these duties are frequently underdelivered, with new staff routinely receiving system access before completing the prescribed training pathway. (2) Methods: the study combines a documentary review of European and Portuguese regulatory instruments, a risk assessment grounded in the Human Factors Analysis and Classification System (HFACS), and a case-based review of recent enforcement decisions adopted by the Comissão Nacional de Proteção de Dados (CNPD) in Portugal. (3) Results: untrained new staff consistently underperform across four core competency domains — information classification and handling, chain of custody, incident detection and reporting, and secure use of IT systems — and account for a disproportionate share of knowledge-based non-compliance events, with risk peaking in the first thirty days of employment. (4) Conclusions: a front-loaded, competency-gated onboarding programme with formal assessment, signed Security Commitment, refresher schedule and auditable records is the principal proportionate control against this risk. The SMOP architecture proposed here is directly transposable to Portuguese public and private entities operating under SEGNAC, the GDPR and NIS2 and provides a concrete starting point for the personnel-security component of organisational compliance programmes.

Keywords: classified information; onboarding; human error; security training; insider threat; GDPR; NIS2; SEGNAC; CNPD; CNCS; Portugal

1. Introduction

The amount of sensitive and classified information handed by Portuguese public bodies, defence contractors, financial institutions, healthcare providers and critical infrastructure operators has grown substantially over the last two decades. The digital transformation of public administration, the expansion of cross-border information sharing within the European Union, and the rising volume of personal data processed by public and private entities have produced an environment in which

 doi:10.20944/preprints202606.0125.v1

the protective measures applicable to sensitive information have to be applied by a much larger and more heterogeneous workforce than ten or twenty years ago [1,2].

Contemporarily, workforce mobility has increased: employment periods have shortened in many sectors, contracted and temporary engagements have become more common, and inter-departmental and inter-organisational mobility within the public sector has accelerated as digital projects pull together personnel from multiple proveniences. The combined effect is that organisations have to continuously absorb new staff who arrive without prior familiarity with internal security culture, classification schemes or procedural controls, and who must reach a working level of compliance under significant time pressure. Failures during this absorption phase are predictable and recurrent, and they account for a measurable share of the security incidents recorded in classified and sensitive environments.

The legal framework that governs the handling of classified and sensitive information in Portugal operates on several overlapping levels. At the European Union level, the main instruments are the General Data Protection Regulation (GDPR) [3], the NIS2 Directive on cybersecurity [4], the ISO/IEC 27001:2022 information security management standard [5], and Council Decision 2013/488/EU on the protection of EU classified information [6]. At the national level, the key instruments are Law no. 58/2019, which executes the GDPR in Portugal and provides the specific contraordenação and criminal regime for breaches [7]; Decreto-Lei no. 125/2025, which transposes NIS2 and approves the new Cybersecurity Legal Framework [8]; Law no. 109/2009 (the Cybercrime Law) [9]; and the Sistema de Gestão da Segurança das Matérias Classificadas (SEGNAC), supervised by the Gabinete Nacional de Segurança (GNS), which defines the national classification regime (RESERVADO, CONFIDENCIAL, SECRETO, MUITO SECRETO) and its handling obligations. The Comissão Nacional de Proteção de Dados (CNPD) acts as the national data protection authority, and the Centro Nacional de Cibersegurança (CNCS) acts as the national cybersecurity authority [10].

Each of these instruments contains an explicit or implicit training duty. Article 39(1)(b) of the GDPR places the responsibility for staff training on the data protection officer, and Article 5(2) places the burden of demonstrating compliance on the controller — a duty that is impossible to discharge without auditable training records. Decreto-Lei no. 125/2025 requires essential and important entities to provide periodic cybersecurity training to management and to staff. ISO/IEC 27001:2022 Annex A control 6.3 requires the organisation to maintain information security awareness, education and training and to update it as necessary. Council Decision 2013/488/EU requires Member States and EU bodies to ensure that personnel who handle EU classified information receive appropriate security training. SEGNAC, in turn, conditions access to classified material on the completion of a formal personnel security clearance process that includes security indoctrination.

Despite this dense layer of training obligations, operational pressure often leads to new staff being given provisional access to physical spaces, IT systems or document repositories before they have completed the required training. Empirical evidence indicates that this gap is associated with a three-to-seven-fold increase in the rate of security incidents during the first ninety days of employment compared to organisations with structured onboarding, and that approximately 68% of insider-threat incidents involving new hires are attributable to procedural ignorance rather than malicious intent [11,12]. Two recent enforcement decisions in Portugal — further discussed in Section 3 — illustrate how these risks materialise in practice. They also illustrate that the consequences of onboarding failures are not confined to security incidents in the technical sense: they can translate into administrative liability, criminal liability and substantial financial penalties for the organisation.

This article makes three contributions. First, it maps the principal knowledge gaps observed in new staff against the Portuguese and European regulatory baseline, identifying the specific articles and obligations that are routinely contravened by undertrained staff. Second, it applies the HFACS taxonomy to characterise the temporal and typological distribution of human-error events in the onboarding phase, showing why a front-loaded training architecture is the proportionate response. Third, it proposes a Structured Mandatory Onboarding Programme (SMOP) — eight modules, a formal assessment, a signed Security Commitment, a refresher schedule and an auditable records

 doi:10.20944/preprints202606.0125.v1

architecture — designed to be directly applicable in Portuguese organisations regardless of sector. The remainder of the article is organised as follows: Section 2 sets out the materials and methods; Section 3 presents the results of the knowledge-gap analysis, the risk register, the temporal-risk profile, the non-compliance typology and the illustrative cases; Section 4 discusses the implications and presents the SMOP design; and Section 5 concludes.

2. Materials and Methods

The study combines three methodological strands: a documentary review of European and Portuguese regulatory instruments, a risk assessment grounded in a human-factors taxonomy, and a case-based review of recent enforcement actions in Portugal. The three strands are complementary: the documentary review establishes the normative baseline against which compliance is measured; the human-factors framework provides the analytical lens through which non-compliance events are categorised; and the case-based review provides empirical anchoring for what would otherwise be a purely theoretical argument.

2.1. Documentary Review

European and Portuguese regulatory instruments were reviewed with attention concentrated on the provisions that impose training obligations or that create personal or organisational liability for breaches connected to undertrained staff.

The European instrumentsconsidered were the GDPR [3], the NIS2 Directive [4], Council Decision 2013/488/EU [6], and the relevant Council Recommendations on personnel security in EU bodies. The Portuguese instruments reviewed were Law no. 58/2019 [7], Decreto-Lei no. 125/2025 [8], Law no. 109/2009 [9] and the SEGNAC regime as published by the GNS. Technical standards reviewed were ISO/IEC 27001:2022 [5] and ISO/IEC 27002:2022. Good-practice guidance came from the UK CPNI / NPSA Personnel Security Effective Practice Guide [13] and CNCS sector guidance [10]. The objective of the review was not an exhaustive legal commentary but the identification of training-related obligations, supervisory expectations and the structure of enforcement powers.

Specific attention was given to the notification timelines defined under European and Portuguese law, because these timelines define what staff have to be able to do under operational pressure. Under the GDPR, personal data breaches must be notified to the supervisory authority — the CNPD in Portugal — within 72 hours of the controller becoming aware of the breach. Under NIS2, transposed by Decreto-Lei no. 125/2025, essential and important entities must issue an early warning to the CNCS within 24 hours of becoming aware of a significant incident and a more complete notification within 72 hours, followed by a final report within one month. These short windows mean that new staff who fail to recognise an incident as reportable can, by their omission, cause the organisation itself to breach a statutory duty.

2.2. Human Factors Framework

The risk assessment uses the Human Factors Analysis and Classification System (HFACS) [14], a taxonomy derived from Reason's Swiss Cheese Model of accident causation [15]. HFACS identifies four levels of human failure, each of which can contribute to the eventual incident: unsafe acts (errors and violations by individuals); preconditions for unsafe acts (environmental factors, personal factors, and the condition of the individual at the moment of the act); unsafe supervision (failures in oversight, planning and correction); and organisational influences (resource management, organisational climate and operational process).

In the onboarding context, the absence of training operates simultaneously as an organisational influence (a failure of resource and process management), as a precondition - the individual is in a state of imperfect knowledge - and as an unsafe-supervision failure (the individual is not adequately oversight-corrected during the period of provisional access). It is therefore an unusually high-leverage point of intervention.

 doi:10.20944/preprints202606.0125.v1

Risk ratings in this article are expressed on a 3 × 3 matrix (Likelihood × Impact: High / Medium / Low), with residual risk assessed assuming implementation of the SMOP controls. Within HFACS, non-compliance events are categorised into skill-based errors (automatic behaviours producing unintended results), rule-based mistakes (the misapplication of a rule that the individual believes they understand), knowledge-based mistakes (failure to apply the correct behaviour because the relevant rule is unknown), and exceptional violations (deliberate departure from rules, typically rationalised as situationally justified). This categorisation is used in Section 3.3 to characterise the distribution of non-compliance events among untrained new staff.

2.3. Case-Based Review

Two enforcement decisions of the CNPD were selected to illustrate how onboarding-related deficiencies materialise in Portuguese practice.

The first is the 2021 decision against the Câmara Municipal de Lisboa (coima of EUR 1,250,000) following the unauthorised transfer to foreign embassies of personal data of organisers of a protest in front of the Russian embassy [16]. The second is the 2022 decision against the Instituto Nacional de Estatística (INE) (coima of EUR 4,300,000) connected to the conduct of the 2021 Census [17].

Both decisions are publicly reported and have generated extensive professional commentary; both involve breaches that turn substantially on the operational practice of staff handling personal data; and both have been adopted in the post-GDPR period under Law no. 58/2019. A third illustrative case, presented as a composite based on anonymised internal incidents, captures a recurrent pattern observed in Portuguese public administration: a newly hired technical officer extracting beneficiary data to a personal email account in good faith during the initial weeks of employment, before the role-specific data protection training has been delivered.

2.4. Scope and Limitations

The study covers Portuguese public and private organisations whose staff routinely handle information at RESERVADO level or above under SEGNAC, or personal data of a sensitive nature under the GDPR. Findings are drawn from publicly available incident reports, academic research, regulatory guidance and anonymised case data. The study does not cover technical cybersecurity controls except where they intersect with staff behaviour. The illustrative cases are drawn from public CNPD decisions and a small set of anonymised internal incidents.

3. Results

3.1. Knowledge Gap Analysis

Knowledge gaps were assessed across four core competency domains identified, in the documentary review and in the human-factors literature, as the primary failure points in classified environment incidents:

(a) information classification and handling;
(b) chain of custody;
(c) incident detection and reporting; and
(d) secure use of IT systems.

The four domains are not equally weighted across all sectors — for example, chain of custody is critical in defence environments handling SECRETO and MUITO SECRETO material but less salient in financial sector environments handling personal data — but together they capture the bulk of the procedural compliance burden that falls on new staff during the onboarding phase.

3.1.1. Information Classification and Handling

Classification systems encode the sensitivity of information and prescribe the protective measures applicable at each level. New staff, even those with prior clearances from other

 doi:10.20944/preprints202606.0125.v1

organisations, may encounter unfamiliar classification schemes, different marking conventions, or organisation-specific handling rules that deviate from the SEGNAC baseline. Common problems observed in this domain include the inability to correctly identify the classification level of unmarked or partially marked documents; misapplication of protective markings when originating new documents; failure to apply appropriate physical security to classified material (locked storage, clear-desk policy); unawareness of aggregation risk — the principle that combining individually low-sensitivity items can create a higher-sensitivity product; and confusion between classification level or handling instructions such as the distribution lists applied to EU classified documents.

The 2022 CNPD deliberation against the INE [17] is illustrative. Set out across 66 pages and more than 400 points, the decision identified breaches across five separate areas of the GDPR. The two largest parcels of the coima were EUR 2.4 million for unlawful international transfers of personal data and EUR 1.6 million for breach of duties of information to data subjects. The case is widely quoted as showing how staff handling sensitive personal data at scale require formal training on the specific legal regime governing their activity; operational good faith and reliance on the operational practice of previous campaigns were not a defence. The deliberation also illustrates how the consequences of inadequate training cascade: a misclassification or misapplication of a transfer rule made by an individual staff member becomes, at the level of a national statistical operation, a multi-million-euro breach reaching millions of data subjects.

3.1.2. Chain of Custody

Chain of custody refers to the documented chronological record of who has handled, accessed, transferred or stored a specific item of classified material. Failures in this area are particularly consequential because they undermine the organisation's ability to detect and investigate unauthorised access or loss after the fact.

Without a complete custody record, it is often impossible to determine whether a loss has occurred at all, much less when and by whom. New staff frequently lack awareness of the requirement to log access in physical or electronic registers, of proper procedures for transmission of classified material (including approved carriers, sealing requirements and confirmation of receipt), of controls on reproduction - restrictions on photocopying, photographing or digitising classified documents - , of end-of-day and end-of-visit security checks applicable to staff without a permanent secure workspace, and of procedures for the return, archival or destruction of classified material, including the requirement to obtain a certificate of destruction for material above a defined threshold.

3.1.3. Incident Detection and Reporting

Security incident reporting systems are only as effective as the willingness and ability of staff to recognise and report anomalies.

New staff exhibit consistently lower rates of incident reporting due to a combination of cognitive and cultural factors: they are less likely to recognise that an event constitutes a security incident, more likely to rationalise anomalous events as normal features of an environment they are still learning, and more susceptible to the social pressure to avoid appearing incompetent in front of more experienced colleagues.

Specific deficiencies observed include the inability to distinguish a security incident (which must be formally reported) from a minor procedural deviation; uncertainty about the reporting chain — who to tell, in what timeframe, and using which form; fear of negative professional consequences from reporting, particularly self-reporting; unawareness of near-miss reporting obligations and the systemic value of near-miss data; and lack of familiarity with the behavioural indicators of possible insider-threat behaviour in colleagues.

The legal reporting domain has been amplified by the entry into force of Decreto-Lei no. 125/2025 [8]. Essential and important entities are now subject to a 24-hour early-warning duty and a 72-hour full-notification duty to CNCS, in addition to the pre-existing 72-hour notification duty to CNPD under the GDPR. A new staff member who fails to recognise an event as reportable can therefore

 doi:10.20944/preprints202606.0125.v1

cause the entity itself to fall outside the statutory window — converting what might have been a recoverable technical incident into a regulatory breach with its own enforcement consequences. Module 3 of the SMOP is designed specifically to close this gap.

3.1.4. Secure Use of IT Systems

Classified information environments typically involve IT systems with security controls that differ substantially from commercial off-the-shelf software. Passphrase policies, session management, removable media controls, network segregation rules and printing restrictions are common areas of non-compliance by new staff who are not familiar with the specific environment.

The principal gaps in this domain include non-compliance with passphrase requirements and secure login procedures; inappropriate use of removable media, including the transfer of data to personally owned devices; failure to observe system separation rules, particularly attempts to transfer information between classified and unclassified networks; inadequate log-off and screen-lock behaviour in shared or open-plan environments; and misuse of email — attaching classified material to messages sent via unclassified channels, or forwarding it to uncleared recipients.

The criminal aspect of this domain is significant. Under Article 6 of the Cybercrime Law (Law no. 109/2009) [9], unauthorised access to a computer system is a criminal offence punishable with imprisonment of up to one year or a fine of up to 120 days, raised to imprisonment of up to three years or a fine of up to 360 days where the access involves a breach of security rules. Where the access yields knowledge of trade secrets or other legally protected confidential data, or where the benefit obtained is of considerably high value, the penalty is raised further. Staff who exfiltrate beneficiary data to a personal account in good faith — the pattern of the composite case in Section 3.4 — expose themselves not only to administrative consequences within the organisation but to criminal liability under Article 6, even where there is no malicious intent in the colloquial sense.

3.2. Risk Register and Temporal Profile

Table 1 summarises the principal onboarding-phase risks identified in the analysis, with the assessed likelihood and impact under the assumption that no targeted training control is in place, together with the primary SMOP module designed to mitigate each one. Residual risk after SMOP implementation is assessed in Section 4.

Table 1. Onboarding-phase risk register with primary SMOP controls.

Risk	Likelihood	Impact	Primary Control (SMOP)
Misclassification of originated documents	High	High	Module 1
Unauthorised disclosure via email misrouting	High	High	Modules 4 & 5
Loss of physical classified material	Medium	High	Module 2
Failure to report a security incident	High	Medium	Module 3
Inappropriate use of removable media	High	High	Module 5
Chain-of-custody log omissions	High	Medium	Module 2

 doi:10.20944/preprints202606.0125.v1

Risk	Likelihood	Impact	Primary (SMOP)	Control
Aggregation creating higher-classification product	Medium	High	Module 1	
Social engineering against new staff	Medium	High	Module 7	
Non-compliant destruction of classified waste	Medium	High	Module 2	
Breach of clear-desk policy	High	Medium	Module 6	
Password breaches / shared credentials	Medium	High	Module 5	
Inadvertent disclosure in informal conversation	Medium	Medium	Module 8	

Empirical data from the CERT Insider Threat Center [11] and the CPNI [13] indicate that the risk of human-error-driven security incidents is not uniformly distributed across the employment lifecycle.

The sharpest elevation occurs in the first thirty days — the orientation gap — when the individual is navigating an entirely unfamiliar environment with minimal procedural confidence. Risk remains significantly elevated through to approximately ninety days, then declines as procedural habits become established, provided that the habits formed in that window are themselves compliant.

Three phases are identifiable.

- The Critical Phase, days 1 to 30, presents the maximum exposure: staff are processing large volumes of new information simultaneously, security training competes for attention with role-specific technical training, logistics and relationship-building, and error rates in classified environments during this window are estimated at four to six times the baseline for experienced staff.
- The Consolidation Phase, days 31 to 90, presents diminishing but still elevated risk: procedural knowledge is being applied but is not yet automatic, compliance is deliberate and an effort and can break down under pressure, and incident rates remain at approximately two to three times baseline.
- The Stabilisation Phase, days 91 to 180, is the phase at which compliant or non-compliant patterns become habitual; non-compliant habits formed in the Critical Phase become entrenched and are significantly harder to correct.

The implication of the temporal evidence is unequivocal. Every day of delayed training during the Critical Phase represents an unmitigated risk period, and habits formed in that window become harder to remediate as the employment progresses.

The SMOP proposed in Section 4 is therefore designed for the core training to be completed within the first ten working days of employment, with progression to unsupervised access conditional on a formal competency gate.

3.3. Non-Compliance Typology

Applying the HFACS taxonomy [14] to non-compliance events observed among new staff in classified environments yields four broad categories with characteristic frequency and severity profiles:

 doi:10.20944/preprints202606.0125.v1

- Skill-based errors: automatic behaviours that produce unintended results, such as attaching a file to a reply without reviewing its classification, or hitting reply-all on a thread that has acquired a sensitive attachment. These are the highest-frequency category but typically have the lowest average severity, because they are usually caught at the next procedural checkpoint (data loss prevention, recipient verification, line-manager review).
- Rule-based mistakes: misapplication of a rule that the individual believes they understand but has not internalised correctly, such as applying a RESERVADO marking to a CONFIDENCIAL document because both are perceived as "government-internal", or applying the GDPR's legitimate-interest basis to a processing operation that requires explicit consent. These have moderate frequency but variable severity, depending on whether the misapplied rule moves the operation closer to or further from compliance.
- Knowledge-based mistakes: failure to apply appropriate behaviour because the correct rule is simply unknown — for example, not logging a document access because the requirement was never communicated, or not notifying CNCS within 24 hours because the staff member was unaware that NIS2 imposes such a deadline. These are disproportionately frequent in untrained new staff and are directly solvable through training; in trained staff they are comparatively rare.
- Exceptional violations: deliberate deviation from rules, typically rationalised as situationally justified at the moment of the act, such as using a personal device because the secure device is unavailable, or sending a document to a personal email account to work from home. Low frequency but high consequence; the composite case in Section 3.4 belongs to this category, even though the individual perceived themselves as acting in good faith.

For untrained new staff, the typology is skewed heavily towards knowledge-based mistakes and skill-based errors, with rule-based mistakes accounting for the bulk of the moderate-severity events and exceptional violations contributing a small but disproportionately damaging tail. This distribution is significant because, unlike skill-based errors (which require ongoing reinforcement) and exceptional violations (which require cultural and disciplinary work), knowledge-based mistakes are directly and almost entirely addressable through formal training delivered before unsupervised access begins.

3.4. Illustrative Cases

In 2021 the CNPD applied a coima of EUR 1,250,000 to the Câmara Municipal de Lisboa following the unauthorised disclosure of personal data of the organisers of a protest in front of the Russian embassy [16]. The data — names, addresses and contact details — was forwarded to the embassies of the three countries whose nationals were involved in the protest, including the Russian embassy. The case was driven not by malicious intent at the operational level but by routine office procedure being applied to information that, in the post-GDPR context, should never have left the council. It illustrates how, in the absence of role-appropriate training, staff treat sensitive personal data — including, in this case, data revealing political opinions, a special category under Article 9 of the GDPR — as ordinary correspondence. The decision is also a reminder that the data protection regime applies to public bodies acting in administrative capacities, not only to commercial controllers.

In a composite case based on anonymised internal incidents, a newly hired technical officer at a Portuguese public agency was granted access to a personal data system in week one, three weeks before completing the mandatory data protection training. Within ten days the officer extracted a list of beneficiaries and emailed it to a personal Gmail address with the subject line "work file — to finish over the weekend". There was no malicious intent in the colloquial sense; the officer believed personal email was a private channel and that the file was not particularly sensitive. The incident was caught by the organisation's data loss prevention controls and reported to the CNPD as a personal data breach under Article 33 of the GDPR [3].

The officer faced internal disciplinary proceedings and was the subject of a notification to the Ministério Público, given the potential applicability of Article 6 of Law no. 109/2009 (unauthorised

 doi:10.20944/preprints202606.0125.v1

access with breach of security rules) [9]. The case illustrates the pattern most directly addressed by the SMOP: a knowledge-based mistake (unawareness that personal email is not an authorised channel for processing) combined with an exceptional violation (transfer to a personal device) committed in the Critical Phase, by an officer who had not yet received the training that would have prevented the event.

These two cases share three features that recur throughout the broader case literature reviewed for this article. First, the proximate cause is a procedural act by a single staff member, not a sophisticated external attack. Second, the staff member's subjective state at the moment of the act was not malicious; it was uninformed. Third, the organisational consequence was disproportionate to the apparent gravity of the act in question, because the act crystallised a latent compliance failure into an external enforcement outcome. These three features together define the population of incidents that the SMOP is designed to prevent.

4. Discussion

The pattern observed in the documentary and case-based review is consistent across sectors: untrained new staff produce a non-compliance profile in which knowledge-based mistakes are disproportionately represented, and the temporal concentration of these events in the first thirty to ninety days of employment is robust across studies [11–13]. This distribution carries an important practical implication.

Unlike skill-based errors, which require ongoing reinforcement, and unlike exceptional violations, which require cultural and disciplinary intervention, knowledge-based mistakes are directly and almost entirely addressable through formal training delivered before unsupervised access begins. The proportionate response is therefore an onboarding programme designed around three structural principles: front-loading, competency-gating and auditability.

4.1. Design Principles of the SMOP

Front-loading means that core mandatory modules are delivered within the first two working weeks of employment, before any independent access to classified systems or material.

The temporal evidence demonstrates that every day of delayed training during the Critical Phase represents an unmitigated risk period, and habits formed in that window become harder to remediate later.

Competency-gating means that progression to subsequent modules, and to independent access, is conditional on demonstrated competence rather than mere attendance. The act of passing a formal assessment is itself an evidential record that the individual is informed; in legal terms, this is the difference between an organisation that can demonstrate compliance with Article 5(2) of the GDPR and one that cannot.

Auditability means that every training event, every assessment and every certification decision is recorded in a tamper-evident training management system, so that the records can be produced on demand to CNPD, CNCS or to an internal compliance audit.

The programme is also calibrated to two further principles drawn from the educational literature. Contextualised learning, drawn from adult learning theory [19], requires content to be role-specific and to use scenarios drawn from the actual operating environment, not generic compliance vignettes. Multimodal delivery requires a combination of instructor-led sessions, e-learning, practical exercises and observed task performance, to accommodate diverse learning styles and to consolidate procedural knowledge through use rather than through passive exposure.

4.2. Programme Architecture

The proposed programme architecture comprises eight modules covering classification fundamentals, physical handling and custody, incident reporting, chain-of-custody systems, secure IT use, physical security and clear-desk policy, insider threat awareness, and security culture and

 doi:10.20944/preprints202606.0125.v1

legal obligations. Total taught time is twenty-four hours, delivered through a combination of instructor-led sessions, practical exercises and observed task performance over the first ten working days of employment.

Each module ends with a formal assessment scored against an 80% threshold on the written component and a satisfactory rating on the observed practical component. One immediate retake is permitted following a failed attempt; a second failure triggers a full module repeat with additional supervised practice before re-assessment.

- Module 1 (Classification Fundamentals and Marking Standards, four hours) provides a foundational grounding in the organisation's classification scheme, its interaction with SEGNAC and with the EU classified information rules under Council Decision 2013/488/EU, the application of protective markings, the consequences of misclassification, and the principle of aggregation risk.
- Module 2 (Physical Handling, Custody and Destruction, four hours) addresses the lifecycle of classified material from receipt through storage, use, transfer and destruction, including the operation of secure storage facilities, custody log completion, double-envelope protocols, clear-desk and clear-screen requirements, and the certification of destruction.
- Module 3 (Incident Detection and Reporting, three hours) develops participants' ability to recognise, categorise and report security incidents within the statutory deadlines under the GDPR and NIS2, including practical scenarios.
- Module 4 (Chain-of-Custody Management Systems, two hours) ensures participants can operate the physical and electronic logging systems accurately.
- Module 5 (Secure IT Systems and Acceptable Use, four hours) provides hands-on training in passphrase policy, session management, removable media controls, network segregation, email security and printing restrictions.
- Module 6 (Physical Security Controls and Clear-Desk Policy, two hours) covers the access control architecture, visitor management and the clear-desk regime.
- Module 7 (Insider Threat Awareness and Reporting Culture, three hours) builds understanding of the insider threat landscape and develops a reporting culture.
- Module 8 (Security Culture, Legal Obligations and Ethics, two hours) contextualises all prior learning within the broader frame of individual legal responsibility, including the criminal liability framework under Law no. 109/2009 and the administrative liability framework under Law no. 58/2019.

Two design choices warrant specific comment because they distinguish the SMOP from generic security awareness training widely available on the market.

The first is the explicit linkage between the written assessment and an observed practical component for each module. Written knowledge of a marking convention or of a passphrase policy is necessary but not sufficient to demonstrate operational competence; the practical observation, conducted by a certified assessor under representative conditions, captures whether the participant can in fact apply the rule in their own workspace. The combination of written and practical assessment also produces an evidential record that is robust against the criticism — frequently raised in administrative proceedings — that compliance training is a paper exercise without operational effect.

The other design choice is the use of sanitised material drawn from the actual operating environment in the practical exercises of Modules 1, 2, 4, 5 and 6, rather than generic vignettes. This approach is consistent with adult learning theory [19] and substantially improves retention because the participant is solving problems that closely resemble those they will encounter in their first weeks of unsupervised work. The cost of this choice is the additional preparation effort required to produce and maintain a portfolio of sanitised exercises, but this cost is largely one-off and is amortised across all subsequent trainings.

4.3. The Security Commitment and Competency Gate

 doi:10.20944/preprints202606.0125.v1

Progression to unsupervised independent access to classified material or systems is conditional on a formal competency gate. The criteria are cumulative: completion of all eight SMOP modules (attendance confirmed in the Training Management System); pass mark in the assessment for all eight modules at or above the 80% threshold; satisfactory performance on every practical observation; signed Security Commitment on file; and Security Officer sign-off on the SMOP Completion Certificate. No individual is granted unsupervised access until all five criteria are recorded as met. Where operational necessity requires earlier provisional access, a documented risk acceptance must be signed by the Head of Security and countersigned by the line manager, specifying the access scope, supervision arrangements and target completion date — converting the provisional access from a default to a deliberate managerial decision with a documentary trail.

The Security Commitment is a formal signed document by which the new staff member acknowledges their understanding of, and personal commitment to, the organisation's security obligations. It serves three functions. The legal evidential function is to establish that the individual was informed of their obligations under Law no. 58/2019 [7], Law no. 109/2009 [9], Decreto-Lei no. 125/2025 [8] and, where applicable, the SEGNAC regime — closing off the "I did not know" defence in subsequent enforcement or disciplinary proceedings. The behavioural function is that the act of signing creates a psychological commitment effect, shown in the security training literature to improve subsequent compliance [13]. The administrative function is to provide a milestone marker in the personnel security record, which can be retrieved on demand for audit purposes.

4.4. Refresher Training and Continuous Development

Refresher training is calibrated to the role tier.

Tier 1 (general staff with access to sensitive personal data) require a full annual refresher of four hours, with the incident-reporting module repeated annually as a fixed element.

Tier 2 (staff with CONFIDENCIAL access) require two refreshers per year, totalling six hours, with Modules 3 and 7 repeated every six months.

Tier 3 (staff with SECRETO or MUITO SECRETO access) require quarterly training of two hours with role-specific scenario content.

Tier 4 (security personnel) require quarterly training and continuing professional development, including coverage of new legislation, CNCS and GNS advisories and insider threat intelligence.

Trigger-based refreshers are mandated for five categories of event: incident involvement (any staff member directly involved in or associated with a recorded security incident must complete targeted refresher training within ten working days); role change (transfer to a role with different or higher classification access requires completion of the relevant SMOP modules for the new access level before unsupervised access is granted); return from extended absence (staff returning from absence of 90 days or more — including parental leave, long-term sick leave or secondment — must complete a condensed refresher of at least four hours before resuming access); significant regulatory or system change (where new legislation such as the 2025 NIS2 transposition, a classification scheme revision or a major system change is introduced, all affected staff must complete a targeted briefing within thirty days); and adverse vetting information (where new security-relevant information about a staff member comes to light during ongoing personnel security review, a refresher element may be required as part of the management action plan).

Beyond mandatory refresher training, the organisation should maintain a continuous development pathway. This includes advanced courses on information assurance, access to CNCS resources, participation in national security awareness campaigns and mentorship pairing new staff with experienced cleared colleagues. While not mandatory for the general population, completion of continuous development should be recognised in performance evaluations and treated as a prerequisite for progression into Tier 3 or Tier 4 roles.

4.5. Documentary Records and Audit Architecture

The records architecture is designed to satisfy four requirements.

 doi:10.20944/preprints202606.0125.v1

- Auditability requires that every training and compliance event be traceable to a verifiable source record.
- Completeness requires that no staff member appear as access-authorised without a corresponding complete training record.
- Security requires that training records themselves be held at appropriate sensitivity and protected against unauthorised amendment.
- Accessibility requires that authorised auditors and security officers can retrieve individual or aggregate records promptly.

The Training Management System (TMS) must provide automated alerts when refresher training is due or overdue, a dashboard showing training currency across the workforce by tier and access level, integration with the access control system to enforce the competency gate, role-based access controls so that only authorised HR and security personnel can amend records, and an immutable audit log of every record creation, amendment and access event. Where a commercial TMS is not available, a controlled spreadsheet equivalent may be used provided it is stored on a classified network share with restricted write access and automated version control.

Retention periods for the principal record types should follow the deeper of two standards: the statutory minimum applicable under Portuguese law, and the duration required to support subsequent enforcement defence.

SMOP Completion Certificates should be retained for the duration of employment plus seven years; signed Security Commitments for employment plus ten years; module attendance registers and refresher training records for five years; assessment results sheets for employment plus seven years; provisional access risk acceptances for employment plus five years; and departure security briefing records for ten years from the date of departure. Annual compliance audit reports should be retained for at least five years.

4.6. The Portuguese Enforcement Context

An important contextual consideration for Portuguese organisations is the current enforcement environment. The CNPD itself reported in 2025 that staff shortages have constrained its capacity to process contraordenação cases, with only two coimas applied during the year, totalling EUR 47,000, despite 472 data-breach processes opened [18].

The mismatch between case volume and enforcement throughput signals that current administrative enforcement risk is comparatively low and that organisational complacency is easy. The SMOP framework should therefore be understood not as a response to immediate enforcement pressure but as a structural control against the much larger underlying risk of operational incidents — and against the higher penalty exposure that will likely follow once CNPD enforcement capacity is restored. The combined sanction regime under NIS2 (administrative fines up to EUR 10 million or 2% of global turnover for essential entities), the GDPR (up to EUR 20 million or 4% of global turnover), the Cybercrime Law (criminal liability up to three years' imprisonment in aggravated cases) and the Law no. 58/2019 (national contraordenação framework with minimum amounts specifically defined for SMEs) defines a substantial latent liability that an undertrained workforce continuously generates.

A second contextual factor is the introduction of personal management liability under NIS2. Decreto-Lei no. 125/2025 places direct responsibility on the management bodies of essential and important entities for compliance with cybersecurity risk-management measures, including training. The clear policy direction is towards an enforcement model in which senior managers cannot delegate compliance away from themselves; the existence of a documented, auditable and effectively delivered onboarding programme is, in this model, a direct element of the management body's own due diligence.

4.7. Limitations and Further Research

There are two principal limitations for this analysis.

 doi:10.20944/preprints202606.0125.v1

First, the case material is drawn from publicly available decisions and a small set of anonymised internal incidents; broader empirical validation across Portuguese sectors — particularly the financial, healthcare and defence sectors — would strengthen the temporal-risk findings and refine the role-tier calibration of the refresher schedule.

Second, the programme architecture is presented in a generic form and would require role-specific tailoring before deployment, particularly for environments handling MUITO SECRETO material or material subject to specific EU-classified handling caveats.

Further research should focus on three areas: empirical evaluation of the temporal-risk profile in Portuguese organisational settings; standardised assessment instruments shared across entities to reduce duplication of effort and support cross-organisational mobility of cleared personnel; and the integration of the SMOP with sector-specific obligations, notably the supervisory expectations of the Banco de Portugal and the European Central Bank for credit institutions, and of the Direção-Geral da Saúde for healthcare entities.

5. Conclusions

Placing new staff in classified or sensitive environments before mandatory training has been completed is a structural rather than incidental source of security risk.

The risk peaks in the first thirty days of employment, is dominated by knowledge-based mistakes, and is directly addressable through a competency-gated onboarding programme delivered before unsupervised access begins. The two Portuguese CNPD enforcement cases examined in this article — the 2021 Câmara Municipal de Lisboa decision and the 2022 Instituto Nacional de Estatística decision — illustrate how the consequences of inadequate onboarding cascade from individual procedural acts into organisational liability of substantial financial and reputational weight.

The Structured Mandatory Onboarding Programme proposed in this article — eight modules, formal written and practical assessment with an 80% threshold, signed Security Commitment, role-tiered refresher schedule and an auditable training records architecture — provides a proportionate and directly transposable framework for Portuguese public and private entities operating under SEGNAC, the GDPR and NIS2. The programme is built around three structural principles: front-loading, so that core training is completed within the first ten working days; competency-gating, so that progression depends on demonstrated knowledge rather than mere attendance; and auditability, so that the organisation can demonstrate compliance to CNPD, CNCS and internal audit on demand. The eight modules cover classification, physical handling and custody, incident reporting, chain-of-custody systems, secure IT use, physical security, insider threat awareness and security culture, and together address the four core competency domains in which untrained new staff have been shown to underperform.

Although the framework proposed in this study is applicable across multiple sectors, its relevance is particularly evident in critical information systems where personnel represent a primary security dependency. In such environments, onboarding processes should be regarded not merely as human-resources activities but as integral components of organisational resilience, operational continuity and security governance.

Future work should focus on the empirical evaluation of the temporal-risk profile in Portuguese settings; on the integration of the SMOP with sector-specific obligations, particularly in the financial and healthcare sectors; and on the development of standardised assessment instruments shared across entities to reduce duplication of effort and to support cross-organisational mobility of cleared personnel. The introduction of personal management liability under Decreto-Lei no. 125/2025 makes the personnel-security dimension of compliance directly material to the management body's own due diligence, and is likely to drive renewed attention to onboarding architecture across Portuguese essential and important entities in the next reporting cycle.

Author Contributions: Ana C. G. R. Almeida was responsible for the conceptualisation of the study, literature review, regulatory analysis, methodological development, design of the Structured Mandatory Onboarding

 doi:10.20944/preprints202606.0125.v1

Programme (SMOP), drafting of the manuscript, and overall revision of the paper. Antonio Goncalves contributed to the review of the methodological framework, validation of the proposed onboarding architecture, and critical revision of the manuscript. Mario Monteiro Marques contributed to the review of the manuscript and provided subject-matter expertise regarding security governance, personnel security, and classified information environments. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analysed in this study. All regulatory and case sources cited are publicly available.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Cabinet Office. HMG Government Security Classifications Policy, Version 3.1; His Majesty's Stationery Office: London, UK, 2023.
2. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5; U.S. Department of Commerce: Washington, DC, USA, 2020. https://doi.org/10.6028/NIST.SP.800-53r5.
3. European Parliament and Council. Regulation (EU) 2016/679 (General Data Protection Regulation). Off. J. Eur. Union 2016, L 119, 1–88.
4. European Parliament and Council. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Off. J. Eur. Union 2022, L 333, 80–152.
5. ISO/IEC. Information security, cybersecurity and privacy protection — Information security management systems — Requirements; ISO/IEC 27001:2022; ISO: Geneva, Switzerland, 2022.
6. Council of the European Union. Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information. Off. J. Eur. Union 2013, L 274, 1–50.
7. Assembleia da República. Lei n.º 58/2019, de 8 de agosto. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679. Diário da República, 1.ª série, n.º 151, 8 August 2019.
8. Governo de Portugal. Decreto-Lei n.º 125/2025, de 4 de dezembro. Aprova o Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555. Diário da República, 1.ª série, 4 December 2025.
9. Assembleia da República. Lei n.º 109/2009, de 15 de setembro. Lei do Cibercrime. Diário da República, 1.ª série, n.º 179, 15 September 2009.
10. Centro Nacional de Cibersegurança (CNCS). Quadro Nacional de Referência para a Cibersegurança (QNRCS); CNCS: Lisbon, Portugal, 2024. Available online: https://www.cncs.gov.pt (accessed on 26 May 2026).
11. Cappelli, D.; Moore, A.; Trzeciak, R. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes; Addison-Wesley / Carnegie Mellon SEI: Boston, MA, USA, 2012.
12. National Archives and Records Administration (NARA). Annual Report to the President: Status of Declassification Activities; NARA ISOO: Washington, DC, USA, 2022. Available online: https://www.archives.gov/isoo/reports (accessed on 26 May 2026).
13. Centre for the Protection of National Infrastructure (CPNI/NPSA). Personnel Security: Effective Practice Guide; CPNI / NPSA: London, UK, 2021. Available online: https://www.npsa.gov.uk/personnel-security (accessed on 26 May 2026).
14. Wiegmann, D.A.; Shappell, S.A. A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System; Ashgate Publishing: Aldershot, UK, 2003.
15. Reason, J. Human Error; Cambridge University Press: Cambridge, UK, 1990.

 doi:10.20944/preprints202606.0125.v1

16. Comissão Nacional de Proteção de Dados (CNPD). Deliberação relativa à Câmara Municipal de Lisboa — transferência de dados de organizadores de manifestação; CNPD: Lisbon, Portugal, 2021.
17. Comissão Nacional de Proteção de Dados (CNPD). Deliberação relativa ao Instituto Nacional de Estatística (INE) — Censos 2021; CNPD: Lisbon, Portugal, 2022.
18. Comissão Nacional de Proteção de Dados (CNPD). Relatório de Atividades 2025; CNPD: Lisbon, Portugal, 2026.
19. Knowles, M.S.; Holton, E.F.; Swanson, R.A. The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development, 8th ed.; Routledge: London, UK, 2015.
20. Lund, A.; Jensen, B.; Morrison, D. Security Awareness Training Effectiveness: A Longitudinal Study of Knowledge Retention in Classified Environments. J. Inf. Secur. Appl. 2018, 43, 78–89. https://doi.org/10.1016/j.jisa.2018.10.005.