					Insert Registered Legal Entity Name Here							
Document number: PII15-FS					Document Title: **Financial Sector PII Incident and Breach Management Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS communications and documented incident evidence
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operational control, privacy risk assessment and treatment linkage
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, evaluation, nonconformity, corrective action and improvement
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incident management planning and preparation for PII processing
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Response to information security incidents involving PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Legal, statutory, regulatory, contractual requirements and protection of records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Processor customer agreement and customer obligation support
GDPR	Article 5(2); Article 24	Controller	Supporting	Accountability and controller responsibility
GDPR	Article 26	Joint Controller	Supporting	Joint-controller incident responsibility coordination
GDPR	Article 28	Both	Supporting	Processor assistance and processor contract obligations

GDPR	Article 32	Both	Supporting	Security of processing and breach detection capability
GDPR	Article 33	Both	Primary	Personal data breach notification and breach documentation
GDPR	Article 34	Controller	Primary	Communication of personal data breaches to affected PII principals
GDPR	Article 39	Conditional	Supporting	DPO advice, monitoring, cooperation and contact-point support
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	ICT-related incident management process for in-scope financial entities
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	ICT-related incident and significant cyber threat classification criteria
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Major ICT-related incident reporting and significant cyber threat notification
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Reporting content, time limits, templates and procedures
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Significant incident reporting where applicable
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Information security and privacy compliance principles
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII incident response responsibilities and event reporting

ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incident planning, assessment, response, lessons learned and evidence collection
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Incident management process lifecycle
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incident policy, plan, awareness, testing and lessons learned
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detection, notification, triage, analysis, response and reporting operations
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Public cloud processor notification and breach record expectations

1. Scope

1.1 This policy defines the requirements for identifying, reporting, triaging, classifying, assessing, containing, notifying, documenting, closing and improving from PII incidents and PII breaches in financial-sector PIMS scopes.

1.2 **Implementation notice:** This policy is a financial-sector replacement variant for PII15. It must not be implemented concurrently with PII15 for the same PIMS scope, business unit, product, customer environment, regulated service or evidence boundary. Organizations must select either PII15 or PII15-FS for the same scope to avoid duplicate incident-management obligations, duplicate registers and duplicate audit evidence work.

1.3 This policy applies to:

1.3.1 the organization acting as a PII controller in a financial-sector context;

1.3.2 the organization acting as a joint controller where incident or breach responsibility coordination is required;

1.3.3 the organization acting as a PII processor for financial-sector customers;

1.3.4 the organization acting as a subprocessor for financial-sector customers or upstream processors;

1.3.5 systems, applications, services, processes, suppliers, processors, subprocessors and third parties that process, store, transmit, support, access or otherwise affect PII within the financial-sector PIMS scope.

1.4 This policy uses REG10 - PII Incident and Breach Register as the primary evidence object for financial-sector PII incident and breach management.

1.5 This policy uses supporting evidence objects as follows:

1.5.1 REG01 for PIMS scope, applicable interested-party, sectoral, customer, contractual and reporting context.

1.5.2 REG02 for affected processing activities, PII categories, PII principal categories, purposes, systems and services.

1.5.3 REG03 for Statement of Applicability and control applicability updates, including replacement of PII15 by PII15-FS for the same scope.

1.5.4 REG04 for privacy risk, DPIA, residual risk and risk treatment linkage.

1.5.5 REG08 for processor, subprocessor, customer, supplier and third-party incident interface evidence.

1.5.6 REG09 for international transfer linkage when an incident affects cross-border processing.

1.5.7 REG11 for training, awareness and incident-response competence evidence.

1.5.8 REG12 for audit, nonconformity, corrective action, management review and improvement evidence.

1.6 This policy relies on related PIMS policies for specialist controls:

1.6.1 PII03 governs processing inventory and lawful basis records.

1.6.2 PII04 governs privacy notice and transparency controls outside breach-specific communications.

1.6.3 PII06 governs PII principal rights requests that arise before, during or after an incident.

1.6.4 PII07 governs privacy risk assessment and DPIA methodology.

1.6.5 PII08 governs privacy by design and default controls.

1.6.6 PII10 governs retention, deletion and disposal controls.

1.6.7 PII12 governs processor, subprocessor, supplier and third-party privacy relationship controls.

1.6.8 PII13 governs international PII transfer mechanisms and transfer risk records.

1.6.9 PII14 governs preventive and detective PII security and access controls.

1.6.10 PII16 governs privacy training, awareness and competence.

1.6.11 PII17 governs documented information and evidence management.

1.6.12 PII18 governs monitoring, internal audit, management review, nonconformity, corrective action and continual improvement.

1.6.13 PII23 governs cloud PII processor controls where cloud processor obligations are in scope.

1.7 For this policy:

1.7.1 "PII incident" means a suspected or confirmed event that has affected, may have affected or could reasonably affect the confidentiality, integrity, availability, lawful processing or authorized handling of PII.

1.7.2 "PII breach" means a confirmed PII incident involving unauthorized, unlawful, accidental or unintended destruction, loss, alteration, disclosure of, access to, unavailability of or compromise of PII.

1.7.3 "Financial-sector PII incident" means a PII incident that affects, may affect or is reasonably connected to regulated financial services, financial-sector customers, financial counterparties, financial transactions, financial operations or financial-sector PII processing.

1.7.4 "Major financial-sector incident" means a financial-sector PII incident or related ICT incident that meets documented materiality or reporting criteria in REG10.

1.7.5 "Significant cyber threat" means a cyber threat recorded in REG10 that could materially affect in-scope financial-sector services, PII processing, customers, counterparties or operations.

1.7.6 "Breach assessment" means the documented evaluation of whether a PII incident is a PII breach, what PII and PII principals are affected, what risks may arise, what notifications or communications are required and what remedial action is needed.

1.7.7 "Awareness" means the point at which the organization has a reasonable degree of certainty that a security or privacy incident has occurred and PII has been or may have been compromised.

1.7.8 "High-impact financial-sector PII incident" means a PII incident involving high-risk processing, special category or highly sensitive PII, large-scale PII, vulnerable individuals, regulated customers, material service disruption, financial counterparties, financial transactions, multi-jurisdictional impact, privileged access compromise, public exposure, ransomware, service unavailability or significant operational, customer, financial or reputational impact.

1.7.9 "Material incident change" means new or changed information affecting incident scope, severity, PII categories, PII principal impact, service impact, financial-sector classification, notification decision, customer impact, root cause, containment, recovery, corrective action or external reporting obligations.

2. Purpose

2.1 The purpose of this policy is to ensure that PII incidents and breaches in financial-sector contexts are handled consistently, promptly, lawfully, securely and with audit-ready evidence.

2.2 This policy supports accountability by requiring financial-sector PII incidents and breaches to be recorded in REG10 and linked to affected processing records, privacy risks, processor and subprocessor relationships, transfer records, corrective actions, training records, financial-sector reporting decisions and management review evidence where triggered.

2.3 This policy ensures that controller, joint controller, processor and subprocessor obligations are handled through distinct applicability rules while maintaining one integrated financial-sector incident and breach evidence model.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 ensure suspected financial-sector PII incidents are reported and recorded promptly;

3.1.2 ensure financial-sector PII incidents are triaged and classified using consistent privacy, security, operational and sectoral criteria;

3.1.3 ensure breach assessments consider affected PII, PII principals, systems, services, processing activities, processors, subprocessors, transfers, risks, customers, counterparties and remedial actions;

3.1.4 ensure controller notification and PII principal communication decisions are documented;

3.1.5 ensure processor and subprocessor breach notifications to customers or upstream parties are made without undue delay and in accordance with applicable agreements;

3.1.6 ensure financial-sector reporting triggers are evaluated, documented and tracked where applicable;

3.1.7 ensure evidence is preserved and protected during incident handling;

3.1.8 ensure containment, eradication, recovery and validation are tracked through REG10;

3.1.9 ensure significant cyber threats and major financial-sector incidents are routed to appropriate decision and reporting workflows;

3.1.10 ensure incident lessons learned result in corrective action, training, control improvement and management review;

3.1.11 ensure incident and breach records are available for audit, management review, customer assurance and regulatory review where applicable;

3.1.12 ensure PII15-FS replaces PII15 for the same financial-sector scope and does not duplicate PII15 evidence work.

4. Policy Statements

4.1 Variant activation, readiness and intake

4.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST document activation of PII15-FS in REG01 and REG03 before this policy is used for a financial-sector PIMS scope.

4.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST document in REG03 and REG12 that PII15 is not concurrently implemented for the same financial-sector PIMS scope before PII15-FS is approved.

4.1.3 [All] The Incident Response Coordinator MUST record every reported or detected suspected financial-sector PII incident in REG10 within one business day of receipt, or sooner where an applicable notification, customer or reporting timeline may be triggered.

4.1.4 [Conditional] The Privacy Lead / PIMS Manager MUST maintain financial-sector PII incident and breach handling criteria in REG10 at least annually and after any material change to PIMS scope, legal context, customer obligations, contractual obligations, sectoral reporting context or high-risk processing.

4.1.5 [Both] The Information Security Lead MUST confirm incident evidence preservation requirements in REG10 within 24 hours after a suspected incident affects a system, service or application processing PII.

4.1.6 [Conditional] The Vendor / Procurement Owner MUST maintain financial-sector third-party incident contact and evidence-routing requirements in REG08 before onboarding and at least

annually for in-scope processors, subprocessors, suppliers and outsourced reporting providers.

4.2 Classification and breach assessment

4.2.1 [All] The Incident Response Coordinator MUST classify each REG10 entry within 24 hours of intake as a non-PII event, suspected PII incident, confirmed PII incident, confirmed PII breach, financial-sector PII incident, major financial-sector incident, significant cyber threat or pending-classification entry.

4.2.2 [Conditional] The Information Security Lead MUST assess affected services, clients, counterparties, transactions, service downtime, geographic spread, data loss, service criticality and economic impact in REG10 when a PII incident may affect financial-sector services or operations.

4.2.3 [Both] The Privacy Lead / PIMS Manager MUST identify the affected processing activity, PII categories, PII principal categories, systems, processors, subprocessors, transfer locations and privacy risks in REG02, REG04, REG08, REG09 and REG10 before the breach notification decision is finalized.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor MUST assess the risk to affected PII principals for each confirmed or reasonably suspected PII breach and record the notification recommendation, risk rationale and advice in REG10 before the external notification decision is made.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST record joint-controller incident responsibility allocation in REG08 and REG10 within 24 hours after identifying shared responsibility for a suspected or confirmed PII breach.

4.2.6 [Processor] The Privacy Lead / PIMS Manager MUST assess customer instructions, contractual notification obligations and cooperation obligations in REG08 and REG10 within 24 hours after a suspected or confirmed PII breach affects processing performed as a processor.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST identify the upstream notification chain and required evidence routing in REG08 and REG10 within 24 hours after a suspected or confirmed PII incident affects processing performed as a subprocessor.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Exceptions

9.1.1 [All] The Privacy Lead / PIMS Manager MUST record any exception to this policy in REG12 before implementation, or within 24 hours after emergency action where prior approval was not feasible.

9.1.2 [Conditional] Top Management MUST approve any exception that materially affects breach notification timing, financial-sector reporting timing, public communication, customer commitment, evidence preservation or PII principal risk before the incident is closed, with approval evidence retained in REG10 and REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST document advice for any delayed notification, no-notification decision, reporting exception or exceptional communication approach before incident closure, with advice retained in REG10.

9.1.4 [Both] The Vendor / Procurement Owner MUST record supplier, processor, subprocessor, customer or outsourced provider exceptions affecting financial-sector incident response in REG08 and REG12 within five business days after identifying the exception.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST review open exceptions to this policy at least monthly until closure, with review status retained in REG12.

10. Enforcement

10.1.1 [All] The Process Owner / Business Owner MUST escalate failure to report a suspected financial-sector PII incident, preserve evidence, follow assigned actions or cooperate with breach assessment to the Privacy Lead / PIMS Manager within two business days after discovery, with evidence retained in REG12.

10.1.2 [Both] The Incident Response Coordinator MUST escalate late reporting, missed classification, missing evidence, missed escalation or overdue containment action to the Privacy Lead / PIMS Manager within one business day after identifying the issue, with evidence retained in REG10 and REG12.

10.1.3 [Both] The Privacy Lead / PIMS Manager MUST record a REG12 nonconformity when a breach of this policy affects incident intake, triage, containment, notification, reporting, evidence integrity, communication or corrective action.

10.1.4 [Both] The Vendor / Procurement Owner MUST initiate supplier, processor, subprocessor or outsourced provider remediation through REG08 and REG12 within five business days when a third party fails to meet agreed incident, breach, evidence or reporting obligations.

10.1.5 [Conditional] Top Management MUST review material or recurring PII15-FS nonconformities at the next scheduled management review, with decisions and required actions retained in REG12.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST trigger remedial training in REG11 within 30 calendar days when a policy nonconformity involves role awareness, late reporting, escalation failure, evidence-handling failure or communication failure.

11. Review and Maintenance

11.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST review this policy at least annually and record the review outcome, required changes and approval status in REG12.

11.1.2 [Conditional] The Incident Response Coordinator MUST trigger a post-incident review of this policy within 30 calendar days after closure of any high-impact financial-sector PII incident, confirmed PII breach, major financial-sector incident or significant cyber threat, with review evidence retained in REG10 and REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST review this policy within 30 calendar days after becoming aware of a material change to legal, sectoral, customer, contractual, processor, subprocessor, reporting-template, reporting-timeline or transfer-related incident reporting requirements, with review evidence retained in REG01, REG08, REG09 and REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST review implementation of this policy at least annually through the PIMS internal audit programme, with audit findings and corrective actions retained in REG12.

11.1.5 [Conditional] Top Management MUST review incident trends, significant breaches, reporting performance, overdue corrective actions and policy effectiveness during scheduled management review, with outputs retained in REG12.

11.1.6 [Conditional] The Privacy Lead / PIMS Manager MUST review the replacement relationship between PII15-FS and PII15 at least annually and after any PIMS scoping change to verify that both policies are not implemented for the same financial-sector scope, with review evidence retained in REG03 and REG12.

12. Related Policies

12.1 This policy should be read with:

12.1.1 PII01 - Privacy Information Management System Policy

12.1.2 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.1.3 PII03 - PII Processing Inventory and Lawful Basis Policy

12.1.4 PII04 - Privacy Notice and Transparency Policy

12.1.5 PII06 - PII Principal Rights Management Policy

12.1.6 PII07 - Privacy Risk Assessment and DPIA Policy

12.1.7 PII08 - Privacy by Design and Default Policy

12.1.8 PII10 - PII Retention, Deletion and Disposal Policy

12.1.9 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.1.10 PII13 - International PII Transfer Policy

12.1.11 PII14 - PII Security and Access Control Policy

12.1.12 PII16 - Privacy Training, Awareness and Competence Policy

12.1.13 PII17 - PIMS Documented Information and Evidence Management Policy

12.1.14 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.1.15 PII23 - Cloud PII Processor Policy, where financial-sector cloud processor obligations are in scope

12.2 PII15 - PII Incident and Breach Management Policy is the baseline incident and breach policy. PII15-FS is a financial-sector replacement variant for PII15. PII15 and PII15-FS must not be implemented concurrently for the same PIMS scope, business unit, product, customer environment, regulated service or evidence boundary.

13. Reference Standards and Frameworks

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].