NIS2 Stakeholder Engagement Plan - World Bank

Document Version: 1.2

Publication Date: June 3, 2025

Author: [Your Name/CISO Office]

Approver(s): CISO, Head of Compliance

Status: Draft

1. Introduction and Purpose

Use Case: This Stakeholder Engagement Plan outlines the comprehensive and strategically vital strategy for identifying, communicating, and collaborating effectively with all key internal and external stakeholders involved in, or significantly affected by, "World Bank's" NIS2 compliance project. Effective stakeholder engagement is far more than a procedural step; it is a foundational pillar and a critical success factor for the entire initiative. It is absolutely crucial for ensuring broad organizational buy-in and commitment, proactively identifying and addressing potential roadblocks or points of resistance, facilitating the smooth and efficient implementation of often complex operational and technical changes, skillfully managing diverse (and sometimes conflicting) expectations, and ultimately achieving a state of successful, deeply embedded, and sustainable NIS2 compliance. Overlooking or underestimating the importance of thorough stakeholder engagement can lead to profound misunderstandings of requirements and objectives, active or passive resistance to necessary changes, significant project delays and budget overruns, and ultimately, a compliance program that, while perhaps technically complete, is far less effective in practice and fails to achieve the desired level of organizational resilience.

The purpose of this plan is to:

- Systematically identify all relevant internal and external stakeholders, moving beyond simple titles to thoroughly understand their specific interests, motivations, level of influence within the organization or externally, potential concerns or anxieties regarding the NIS2 changes, and their tailored communication needs and preferences related to the Directive.
- Define and establish clear, consistent, reliable, and appropriate communication channels, craft carefully considered key messages for different audiences, and determine optimal frequencies for engagement with each distinct stakeholder group to ensure information is timely, relevant, and actionable.
- Outline a detailed program of specific and varied engagement activities, such as workshops, briefings, and feedback sessions, designed to foster active collaboration, promote transparent and two-way information sharing, and build strong, trust-based

working relationships that can weather the challenges of a complex compliance project.

- Establish robust, clearly defined, and easily accessible mechanisms for collecting stakeholder feedback, addressing queries and concerns promptly and thoroughly, and resolving any emerging issues or conflicts in a timely, fair, and constructive manner, thereby maintaining project momentum and positive stakeholder sentiment.

2. Project Goals and Objectives (NIS2 Compliance)

The primary, overarching goal of the NIS2 Compliance Project is to ensure "World Bank" meticulously and demonstrably meets all its legal and regulatory obligations under the NIS2 Directive by the nationally stipulated deadlines. Achieving this goal is paramount to safeguarding the bank's operational integrity, protecting its valuable reputation, and maintaining the trust of its customers and regulatory bodies. Key objectives underpinning this central goal include:

- **Achieving full and demonstrable compliance with all applicable NIS2 articles:** This extends beyond a superficial checklist approach. It means deeply embedding the spirit and letter of the NIS2 requirements into the bank's daily operational fabric, ensuring that all mandated technical, operational, and organizational measures are not only implemented but are also demonstrably effective, regularly reviewed, and consistently applied across all in-scope services and systems.
- **Enhancing the cybersecurity resilience of critical banking services:** This involves a significant and measurable strengthening of our defenses against a constantly evolving landscape of sophisticated cyber threats. It includes improving our preventative controls, our ability to detect intrusions rapidly, our capacity to respond effectively to incidents, and ensuring the swift and orderly recovery of essential banking services to minimize disruption to our customers, the bank's operations, and the wider financial ecosystem.
- **Establishing robust, integrated risk management and incident reporting capabilities:** This requires the implementation and maturation of a comprehensive cybersecurity risk management framework that is fully aligned with NIS2's "all-hazards" approach (considering physical, environmental, and human factors alongside technical ones). It also necessitates the development of highly efficient, well-rehearsed processes for detecting, analyzing, classifying, and reporting significant cybersecurity incidents to the designated competent authorities and, where necessary, to affected service recipients, all within the strict and demanding timelines set forth by NIS2.
- **Fostering a strong, pervasive cybersecurity culture across the organization:** This critical objective aims to move "World Bank" beyond a mere compliance-driven mindset. It involves cultivating a shared understanding of cyber risks and individual

responsibilities at every level of the organization, from the Boardroom to the frontline. It means encouraging proactive security-conscious behaviors, empowering employees to challenge insecure practices, and making cybersecurity an integral, non-negotiable part of "World Bank's" operational DNA and core values.

- **Minimizing the risk of severe penalties and lasting reputational damage associated with non-compliance:** This involves proactively identifying and addressing potential compliance gaps and control weaknesses to avoid the substantial financial fines (which can be a significant percentage of global turnover), potential legal liabilities for management, and the often more damaging long-term consequences of reputational harm, including the loss of customer trust, diminished market confidence, and increased regulatory scrutiny.

3. Stakeholder Identification and Analysis

Stakeholder Group	Key Contact(s) / Representative(s)	Role/Interest in NIS2 Project	Influence	Impact	Communication Needs
Internal Stakeholders					
1. Board of Directors	Chairperson, Audit Committee Chair	Ultimate oversight body, responsible for approving strategic direction & significant budget allocations, bears ultimate accountability for the bank's compliance. Their primary expectation is assurance that cybersecurity risks, particularly those highlighted by NIS2, are being effectively managed and that the bank is meeting its legal obligations.	High	High	Concise, high-level executive summaries focusing on strategic implications, clear articulation of risk exposure (current vs. target state) and mitigation strategies, unambiguous compliance status dashboards (e.g., RAG status), clear outlines of strategic decisions required from them, and robust justifications for investment.
2. CEO & Senior Executive Management	CEO, COO, CFO, CRO	Responsible for driving the bank's strategic direction, actively championing the NIS2 compliance effort across the organization, allocating necessary resources (financial and human), understanding and managing the operational impact of changes. Deeply concerned with overall business risk, financial performance, and maintaining the bank's market standing.	High	High	Regular, clear, and action-oriented progress updates against the project plan, timely identification of key decisions needed from them to maintain momentum, detailed risk reports explaining the business implications of identified gaps or threats, transparent budget status reports and accurate forecasts for future expenditure.
3. IT Department (incl. Security)	CIO, Heads of Infra/Apps/Security	Primary responsibility for leading the technical implementation of NIS2 requirements, managing complex system changes and integrations, enforcing detailed security policies and standards, and serving as the primary team for incident response and the ongoing operation of technical controls. Requires clear,	High	High	Highly detailed technical requirements and functional specifications for new or modified systems and controls, clear and realistic project plans with defined tasks and timelines, comprehensive information on operational changes affecting IT infrastructure and processes, specific training on new security

		unambiguous guidance and adequate resources to execute effectively.			tools, technologies, and procedures.
4. Legal & Compliance Department	Chief Legal Officer, Head of Compliance	Tasked with interpreting the complex legal text of the NIS2 Directive and its national transpositions, meticulously reviewing and drafting compliant policies and procedures, acting as the primary liaison with regulatory bodies and external counsel, and ensuring overall legal and regulatory adherence across all NIS2-related activities.	High	High	Detailed and nuanced legal interpretations of specific NIS2 articles and their implications for the bank, drafts of policies and procedures for thorough legal review and input, precise understanding of incident reporting requirements (what, when, how, to whom), and timely updates on audit findings and any interactions with regulatory authorities.
5. Risk Management Department	Chief Risk Officer	Responsible for integrating NIS2-specific cybersecurity risks into the bank's overarching Enterprise Risk Management (ERM) framework, validating the methodologies used for cybersecurity risk assessments, ensuring consistency in risk treatment decisions, and aligning cyber risk reporting with broader enterprise risk reporting.	High	Medium	Detailed cybersecurity risk assessment results and methodologies, comprehensive information on the effectiveness of implemented controls, clear articulation of how NIS2 risks align with and impact the broader ERM framework, and the specific methodologies and criteria used for risk evaluation.
6. Operations Departments (Business Units)	Heads of Retail, Corporate, Payments etc.	Need to understand and manage the direct impact of NIS2 requirements on their daily business processes, service delivery mechanisms, and customer interactions. They will provide critical resources for Business Continuity Planning (BCP) and Disaster Recovery (DR) efforts and are responsible for ensuring their staff are aware of and adhere to new procedures.	Medium	High	Clear, practical communication on specific process changes and their rationale, detailed requirements for their involvement in BCP/DR planning and testing exercises, tailored training materials for their teams focusing on operational impacts, and timely information on any potential service impacts or disruptions during the implementation of new controls.
7. Human Resources Department	Head of HR	Responsible for developing and delivering cybersecurity training programs for all employees (including NIS2-specific content), updating HR security policies (e.g., for onboarding new staff, managing leavers, acceptable use of IT assets), and potentially managing enhanced background checks for personnel in sensitive roles.	Medium	Medium	Approved and finalized training content and materials, clear guidance on updates to HR policies affecting personnel (e.g., disciplinary procedures for security breaches), and defined requirements for security screening or background checks if applicable.
8. Internal Audit Department	Head of Internal Audit	Tasked with providing independent and objective assurance of "World Bank's" NIS2 compliance status, reviewing the design adequacy and operational effectiveness of implemented cybersecurity controls, and	Medium	Medium	Unfettered access to all relevant documentation, systems, and personnel for audit purposes, clear audit plans outlining scope and objectives, and access to findings from the gap analysis and ongoing risk assessments to

		identifying areas for improvement or potential non-compliance.			inform their audit scope and focus areas.
9. Project Management Office (PMO)	Head of PMO	Responsible for ensuring adherence to the bank's established project governance standards, meticulously tracking progress against agreed milestones and deliverables, managing consolidated project reporting, and facilitating effective resource coordination and allocation across different project streams.	Medium	Medium	Regular and accurate project status updates from the NIS2 project team, detailed resource utilization reports, access to project risk and issue logs, and assurance that the project is adhering to agreed project management methodologies and reporting cycles.
10. All Employees	N/A	Collectively responsible for understanding and adhering to new or updated cybersecurity policies and procedures, consistently practicing good cyber hygiene (e.g., vigilance against phishing, strong password practices, secure data handling), and promptly reporting any suspicious activities or potential security incidents. Their collective action and vigilance are critical to the overall security posture.	Low (individually in terms of project direction)	High (collectively in terms of impact on security and compliance)	Clear, concise, and engaging awareness campaigns explaining the importance of their role, practical and easy-to-understand training on cyber hygiene principles and incident reporting procedures, and readily accessible policy updates and user-friendly guidelines.
External Stakeholders					
11. National Competent Authorities (NCAs)	Designated contacts per country	Official governmental or regulatory bodies responsible for the supervision and enforcement of the NIS2 Directive within their national jurisdiction. They will receive mandatory incident reports, have the power to conduct audits and inspections, and can impose sanctions for non-compliance. They expect timely, accurate, and comprehensive information.	High	High	Formal, structured incident reports that meticulously meet all NIS2 criteria (content, format, timelines), comprehensive and well-organized evidence of compliance measures upon request (e.g., during an audit), and prompt, transparent, and cooperative responses to any official queries or information requests.
12. National CSIRTs	Designated contacts per country	National Computer Security Incident Response Teams responsible for technical coordination during significant cybersecurity incidents, sharing threat intelligence across sectors, and providing technical assistance and guidance to affected entities.	High	High	Timely and technically detailed incident reports, especially focusing on Indicators of Compromise (IoCs), attack vectors, and mitigation actions. Proactive sharing of relevant threat information observed by "World Bank" that could benefit other entities.
13. Key Third-Party Suppliers/Vendors	Account Managers, Security Contacts	Entities providing critical services or products to "World Bank" whose security posture can directly impact the bank. They need to ensure their own operations meet "World Bank's" enhanced security requirements	Medium	High	Clear and unambiguous articulation of "World Bank's" NIS2-driven cybersecurity requirements and expectations, formal requests for security assessments or evidence of their own compliance (e.g.,

		under NIS2 and adhere to contractual obligations regarding security measures and incident reporting *to the bank*.			certifications, audit reports), and well-defined protocols for incident coordination and timely reporting of breaches affecting the bank's data or services.
14. External Auditors	Audit Partner	Independent firms conducting statutory audits of "World Bank's" financial statements. Their scope may increasingly include an assessment of IT general controls and overall cybersecurity resilience due to the significant operational and financial risks posed by cyber threats.	Medium	Medium	Access to relevant information concerning the bank's IT control environment, the status of its NIS2 compliance efforts, and management's formal assessment and treatment of cybersecurity risks, as these factors can impact financial reporting and internal controls over financial reporting (ICFR).
15. Customers (General Communication)	N/A	The end-users of "World Bank's" services who have a fundamental expectation of secure and reliable banking operations and the robust protection of their personal and financial data. Their trust is a cornerstone of the bank's business.	Low (direct influence on the NIS2 project execution)	Medium (significantly impacted by the outcomes of compliance and security posture)	General public statements, if deemed appropriate and necessary by executive management (especially in response to major industry incidents or to proactively manage reputation), reinforcing "World Bank's" unwavering commitment to data security, customer privacy, and service resilience. Specific incident communications would follow separate, dedicated plans.

4. Communication Strategy

Stakeholder Group	**Key Messages**	**Communication Channels**	**Frequency**	**Responsible**
Board of Directors	Overall NIS2 compliance status (progress, risks, budget), strategic cybersecurity risks and their potential business impact (financial, reputational, operational), required investment levels and ROI justification, key strategic decisions needed for alignment with bank's objectives. Emphasis on demonstrating due diligence, accountability, and providing assurance.	Formal Board Meetings, Dedicated Audit/Risk Committee sessions with detailed presentations, Concise Formal Reports (e.g., quarterly compliance dashboards), CISO Briefings on specific threats or incidents, Secure Board Portal for document distribution.	Quarterly (formal reporting cycle), Ad-hoc for critical emerging issues or urgent decisions.	CISO, CEO
CEO & Senior Executive Management	Detailed project progress against established milestones and budget, immediate resource needs or critical constraints affecting timelines, emerging key risks/issues requiring executive intervention or decision-making, specific strategic or operational decisions required for project momentum. Focus on clear articulation of operational and financial implications, and ensuring project alignment with overall business strategy.	NIS2 Steering Committee Meetings (with pre-reads and defined agendas), Weekly/Bi-weekly Progress Summaries & Executive Dashboards highlighting key metrics, Direct one-on-one Briefings for critical updates or sensitive discussions.	Weekly/Bi-weekly for regular updates, or more frequently if critical decisions are pending or significant issues arise.	CISO, Project Lead

IT Department	Specific technical specifications for new controls and system modifications, detailed project tasks, roles, and assignments with clear dependencies, updated and realistic timelines for deliverables, impact of new/updated security policies on IT operations, system configurations, and support processes. Emphasis on the need for close collaboration, technical feasibility feedback, and proactive problem-solving.	Regular Project Team Meetings (daily stand-ups for core team, weekly for broader team), Specialized Technical Workshops for deep dives on specific technologies or implementations, Internal IT Intranet/Wiki for documentation and knowledge sharing, Targeted Email Updates for specific groups, Change Management System for formal tracking of system changes.	Daily/Weekly for active project team members, As needed for wider IT staff based on specific changes or information dissemination needs.	Project Lead, IT Leads
Legal & Compliance	Nuanced interpretations of NIS2 legal articles, national transpositions, and relevant case law; drafts of policies, standards, and procedures requiring thorough legal and compliance review; detailed understanding and clarification of incident reporting obligations (thresholds, timelines, content); implications of audit findings and any regulatory feedback received.	Regular Working Meetings with dedicated agendas, Collaborative Document Review Platforms (e.g., SharePoint with version control and commenting), Secure Email for sensitive communications and document exchange.	Weekly for ongoing collaboration and review cycles, or as needed when urgent legal interpretation or policy review is critical to project progress.	CISO, Legal Lead
Risk Management	Detailed findings from cybersecurity risk assessments (including likelihood and impact analysis), identified control gaps and their associated risk ratings, proposed methods for integrating NIS2-specific risks into the existing Enterprise Risk Management (ERM) framework, evidence of the effectiveness (or ineffectiveness) of implemented controls, and alignment of cyber risk terminology.	Joint Risk Committee Meetings, Shared Risk Registers and Governance, Risk & Compliance (GRC) tools for centralized tracking, Collaborative Workshops for methodology development and risk calibration.	Monthly for formal risk reporting and review, or as needed when significant new risks are identified or risk assessment results become available.	CISO, CRO
Operations Departments	Specific impacts of proposed NIS2 measures on their daily business processes, workflows, and customer service protocols; clear requirements for their active involvement in Business Continuity Planning (BCP) and Disaster Recovery (DR) strategy development, documentation, and testing; tailored training needs for their staff to ensure understanding and adherence to new procedures; transparent communication regarding potential temporary service impacts or disruptions during the implementation of new controls.	Dedicated Workshops for process mapping, impact assessment, and BCP/DR development; Regular Department Meetings to provide updates and gather feedback; Intranet Updates with FAQs and guidance documents; Direct communication through designated Business Liaison roles within the project team.	Monthly for general updates and progress, Ad-hoc for significant changes, planned system downtimes, or BCP/DR testing events.	Project Lead, Business Liaisons
All Employees	The critical importance of NIS2 compliance for the bank's overall security, regulatory standing, and customer trust; clear articulation of individual responsibilities regarding cyber hygiene practices (e.g., recognizing and reporting phishing attempts, creating strong and unique passwords, secure handling of sensitive data); easily understandable explanations of changes to key security policies; clear and simple instructions on how to report suspicious activities or potential security incidents promptly.	Bank-wide Intranet News articles and dedicated NIS2 project pages, Targeted Email Campaigns with specific calls to action or information, All-Hands Meetings or Town Halls for broader announcements and Q&A, Interactive e-learning Training Modules delivered via the Learning Management System (LMS), visually engaging Posters and Digital Signage in common areas.	Ongoing awareness efforts (e.g., monthly tips, simulated phishing campaigns), Quarterly formal updates on overall project progress and significant policy changes.	CISO Office, HR, Corporate Communications

NCAs / CSIRTs	Formal incident reports adhering strictly to the templates, content requirements, and timelines stipulated by NIS2 and national law; comprehensive and well-organized evidence of implemented compliance measures (particularly during audits or official inspections); transparent, accurate, and prompt responses to official inquiries, requests for information, or directives from the authorities.	Official, secure communication channels as designated and mandated by each National Competent Authority (NCA) or CSIRT (e.g., specific government portals, encrypted email systems, dedicated phone lines for urgent matters).	As per NIS2 reporting requirements (e.g., 24-hour early warning, 72-hour notification), and As needed for any other official interactions, audits, or information requests.	CISO, Legal Department
Key Third-Party Suppliers	Clearly documented updated cybersecurity requirements stemming from "World Bank's" NIS2 obligations; formal requests for evidence of their security controls and posture (e.g., through security questionnaires, third-party audit reports, relevant certifications); well-defined protocols for coordinating on security incidents that may impact the bank; communication regarding any necessary contractual amendments to reflect new security obligations.	Formal Supplier Review Meetings (e.g., quarterly or annually for strategic vendors), Dedicated Secure Supplier Portals for document exchange and communication, formal Contractual Communication channels (e.g., notices as per contract terms), standardized Security Questionnaires and assessment processes.	Annually for standard due diligence and contract reviews, As needed for specific incidents, audits, urgent security bulletins, or contractual changes.	Vendor Management, CISO Office

5. Engagement Activities

1. **Project Kick-off Meeting:** A formal, high-profile launch event for all key internal stakeholders. The primary purpose is to clearly articulate the NIS2 project's strategic vision, overarching goals, defined scope, high-level timeline, and the critical roles and responsibilities each department and key individual will play. This event is crucial for setting a positive and collaborative tone, generating initial momentum, and ensuring everyone starts with a shared understanding of the project's importance and objectives.
2. **NIS2 Steering Committee:** Establishment of and regular, structured meetings with a dedicated committee comprising senior executive management. This committee will provide ongoing high-level oversight, make key strategic decisions, resolve escalated high-level issues and roadblocks, approve significant changes to scope or budget, and ensure the project remains consistently aligned with the bank's broader business objectives and risk appetite.
3. **Working Groups:** Establishment of specialized, cross-functional working groups, each focused on specific, manageable domains of the NIS2 Directive (e.g., a group for Risk Management & Policy development, another for Incident Reporting & Business Continuity planning, a third for Technical Controls & Architecture design, and a fourth for Supply Chain Security). These groups will involve Subject Matter Experts (SMEs) from relevant departments to perform detailed analytical tasks, develop practical solutions, draft specific procedures, and drive implementation within their area of expertise.

4. **Awareness and Training Workshops:** A comprehensive and multi-layered program of workshops and training sessions, carefully tailored for different employee groups. This will include dedicated, in-depth sessions for members of management bodies on their specific governance responsibilities and potential liabilities under NIS2; role-based technical training for IT and security staff on new tools, technologies, and operational procedures; and engaging general awareness sessions for all employees focusing on cyber hygiene best practices and clear incident reporting protocols.
5. **Supplier Engagement Forums/Webinars:** Proactive and structured engagement with critical third-party suppliers, potentially through dedicated forums, webinars, or one-on-one meetings. The aim is to clearly communicate "World Bank's" NIS2-driven cybersecurity expectations and requirements, discuss any new contractual security obligations, and establish clear protocols for ongoing security assessments, due diligence, and coordinated incident response.
6. **Regular Progress Reports and Dashboards:** Development and consistent dissemination of progress reports and visual dashboards, tailored to the needs of different stakeholder audiences. Examples include concise executive summaries and RAG (Red-Amber-Green) status reports for the Board and Steering Committee, more detailed status updates for project working groups, and technical implementation progress reports for IT management. These will track Key Performance Indicators (KPIs), milestones, risks, and issues.
7. **Gap Analysis Review Sessions:** Interactive and collaborative sessions with relevant stakeholders (including business unit representatives, IT, Legal, and Risk) to present the detailed findings of the NIS2 gap analysis. These sessions will facilitate a shared understanding of identified discrepancies, allow for discussion on the potential impact of these gaps, and enable collaborative prioritization of remediation efforts based on risk and business impact.
8. **Policy Review Workshops:** A series of collaborative workshops involving representatives from Legal, Compliance, IT, Information Security, Risk Management, and relevant business units. The purpose is to jointly draft, review, and refine new or significantly updated cybersecurity policies, standards, and procedures to ensure they are not only compliant with NIS2 requirements but are also practical, understandable, and effectively implementable within "World Bank's" operational environment.
9. **Tabletop Exercises and Simulations:** Conducting realistic tabletop exercises and, where feasible and appropriate, more immersive technical simulations focused on various cybersecurity incident response and business continuity scenarios. These exercises will specifically incorporate NIS2 reporting obligations (timelines, content) and will involve key stakeholders from IT, Security, Legal, Communications, and relevant business units to test existing plans, identify weaknesses, and improve cross-departmental coordination and decision-making under pressure.

10. **Targeted Feedback Sessions and Surveys:** Proactively seeking structured input and feedback from various stakeholder groups at key junctures in the project (e.g., after major milestones, training rollouts, or significant policy changes). This will be achieved through targeted feedback sessions (e.g., focus groups) and the use of anonymous surveys to gauge employee understanding of NIS2 requirements, gather concerns or suggestions, and identify areas for improvement in the ongoing stakeholder engagement strategy itself.

6. Feedback Mechanisms

- **Dedicated NIS2 Project Email Address:** A clearly communicated and easily accessible email address (e.g., NIS2Program@worldbank.com) will be established for stakeholders to submit questions, raise concerns, provide suggestions, or request clarifications related to any aspect of the NIS2 compliance project. This inbox will be monitored regularly by designated members of the project team, with a commitment to timely responses.
- **Feedback Forms (Digital and Paper-based):** Standardized feedback forms will be distributed (digitally via links or QR codes, and in paper format where appropriate) during or immediately after training sessions, workshops, and major project meetings. These forms will be designed to capture immediate reactions, assess the clarity and usefulness of information presented, gauge understanding of key concepts, and identify specific areas for improvement in content, delivery, or facilitation.
- **Suggestion Box (Virtual on Intranet):** An anonymous virtual suggestion box will be made accessible via the "World Bank" intranet. This will provide a channel for all employees to provide candid, constructive feedback, share innovative ideas, or raise concerns regarding cybersecurity practices and the NIS2 compliance efforts without any fear of attribution, fostering a more open feedback culture.
- **Regular "Open Door" Sessions / Q&A Forums with CISO Office/Project Team:** Scheduled opportunities (e.g., monthly or bi-monthly "NIS2 Clinics") for employees at all levels to interact directly and informally with members of the CISO office or the core NIS2 project team. These sessions will allow for open dialogue, clarification of doubts, and discussion of concerns in a less formal setting than official meetings.
- **Post-Engagement Surveys (Targeted and Pulse):** Periodic, targeted surveys will be sent to specific stakeholder groups (e.g., IT staff after a technical workshop, business managers after a process change briefing) to assess the effectiveness of particular communication efforts, gauge their level of understanding and buy-in for specific initiatives, and identify any unaddressed needs or persistent concerns. "Pulse" surveys may also be used to quickly gauge sentiment on specific topics. All feedback received through these mechanisms will be systematically logged, categorized, and analyzed by the project team to identify recurring themes, address actionable items promptly, and inform refinements to future engagement activities and communication strategies.

7. Escalation Path for Issues

A clear, well-understood, and consistently applied escalation path is absolutely essential for the timely and effective resolution of issues, and to prevent unaddressed roadblocks from impeding project progress or causing stakeholder frustration. The defined escalation path is as follows:

1. **Level 1: Working Group / Team Level:** Issues identified within specific working groups or by individual project team members should first be attempted to be resolved collaboratively by the respective working group lead or the individual's direct manager, leveraging their immediate expertise and resources.
2. **Level 2: NIS2 Project Lead:** If an issue cannot be satisfactorily resolved at the working group or team level, or if it requires cross-functional input beyond the group's immediate scope (e.g., a conflict between two working groups), it is formally escalated to the NIS2 Project Lead. The Project Lead will assess the issue's complexity and impact, facilitate discussions between relevant parties, and actively work to find a mutually acceptable resolution.
3. **Level 3: NIS2 Steering Committee:** Should the Project Lead be unable to resolve the issue, or if the issue involves significant proposed changes to established policy, conflicts over critical resource allocation, or decisions that could impact the strategic direction of the project, it is then formally escalated to the NIS2 Steering Committee for deliberation, guidance, and authoritative decision-making.
4. **Level 4: CEO / Board of Directors:** In rare instances, critical issues that pose a significant and imminent threat to the overall success of the NIS2 project, have major strategic, financial, or reputational implications for "World Bank," or involve unresolved conflicts or disagreements at the Steering Committee level, are escalated directly to the CEO and, if necessary and appropriate, to the Board of Directors (or a designated Board committee) for final review and resolution. All escalations, regardless of level, will be formally documented (including the nature of the issue, attempts at resolution, and the final decision), tracked through an issue log, and their resolutions will be communicated back to the relevant stakeholders to ensure transparency and closure.

8. Plan Review and Update Schedule

This Stakeholder Engagement Plan is explicitly designed as a living document, recognizing that the project environment, stakeholder needs, and regulatory interpretations may evolve over time. Therefore, it will be formally reviewed on a **quarterly basis** by the CISO office and the NIS2 Project Lead to assess its ongoing effectiveness and relevance. Additionally, the plan will be subject to ad-hoc reviews and potential updates in response to specific triggers, including but not limited to:

- Significant approved changes in the NIS2 project scope, overall timeline, or allocated budget.

- Substantive feedback received from stakeholders indicating that current engagement strategies or communication channels are insufficient, ineffective, or misaligned with their needs.
- Major shifts in the organizational structure of "World Bank" that could impact stakeholder roles, responsibilities, or influence.
- The release of new official guidance, interpretations, or implementing acts related to the NIS2 Directive from EU bodies or national regulatory authorities.
- Important lessons learned from completed engagement activities, project milestones, or any significant project-related incidents or challenges. All updates to this Stakeholder Engagement Plan will be subject to version control, with changes clearly documented. Approved updates will be promptly communicated to all relevant stakeholders to ensure continued alignment, shared understanding, and the ongoing effectiveness of our engagement efforts throughout the lifecycle of the NIS2 compliance project.