I understand you’d like to update the Statement of Applicability (SoA) table to ISO 27001:2022, covering all 93 controls, while maintaining the format from the image. Additionally, you want to include two new columns:

1. **“New/Old (New Control)”** to indicate whether each control is new or old compared to ISO 27001:2013, and specify new controls.
2. **“Implemented in Old Standard (Yes/No)”** to indicate whether each control was implemented under the ISO 27001:2013 standard.

### **Step 1: Recap of the Existing Table Format**

The SoA table in the image has the following columns:

* **Domain/Sub-Domain/Control**
* **Control Description**
* **Applicability**
* **Legal Requirement**
* **Regulatory Requirement**
* **Contractual Requirement**
* **Risk Assessment**
* **Description/Commentary**
* **Control Origin**
* **ITRMS Reference**
* **Rationale for Exclusion**

The image shows that all visible controls (A.5 and A.6 from 2013) are marked “Yes” for applicability, legal, regulatory, contractual, and risk assessment requirements, with “Internal” as the control origin and “ISO27001 standard annexure” as the ITRMS reference. I’ll assume this pattern holds for all controls unless specified otherwise.

### **Step 2: ISO 27001:2013 vs. ISO 27001:2022 Overview**

* **ISO 27001:2013**: 114 controls across 14 domains (A.5 to A.18).
* **ISO 27001:2022**: 93 controls across 4 domains:  
  + Organizational (A.5, 37 controls)
  + People (A.6, 8 controls)
  + Physical (A.7, 14 controls)
  + Technological (A.8, 34 controls)

The 2022 standard introduced 11 new controls:

* A.5.7: Threat intelligence
* A.5.23: Information security for use of cloud services
* A.5.30: ICT readiness for business continuity
* A.7.4: Physical security monitoring
* A.8.9: Configuration management
* A.8.10: Information deletion
* A.8.11: Data masking
* A.8.12: Data leakage prevention
* A.8.16: Monitoring activities
* A.8.23: Web filtering
* A.8.28: Secure coding

### **Step 3: Assumptions for the “Implemented in Old Standard (Yes/No)” Column**

Since the image shows that all visible controls (A.5 and A.6) were applicable and likely implemented (given the “Yes” for all requirement fields), I’ll assume that controls existing in the 2013 standard were implemented (“Yes”). For new controls introduced in 2022, this column will be “No,” as they were not part of the 2013 standard and thus not implemented under it. However, this is an assumption based on the image; you should verify the actual implementation status in your organization.

### **Step 4: Build the Complete SoA Table with New Columns**

Below is the entire SoA table for ISO 27001:2022, covering all 93 controls, with the two new columns: **“New/Old (New Control)”** and **“Implemented in Old Standard (Yes/No)”**. The table follows the format from the image.

| **Domain/Sub-Domain/Control** | **Control Description** | **Applicability** | **Legal Requirement** | **Regulatory Requirement** | **Contractual Requirement** | **Risk Assessment** | **Description/Commentary** | **Control Origin** | **ITRMS Reference** | **Rationale for Exclusion** | **New/Old (New Control)** | **Implemented in Old Standard (Yes/No)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ORGANIZATIONAL CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |  |
| A.5.1 | Information security policies | Yes | Yes | Yes | Yes | Yes | Policies defined and reviewed annually. | Internal | ISO27001 standard annexure | N/A | Old (Merged A teniendo.5.1.1 and A.5.1.2) | Yes |
| A.5.2 | Information security roles and responsibilities | Yes | Yes | Yes | Yes | Yes | Roles assigned to security team. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.1) | Yes |
| A.5.3 | Segregation of duties | Yes | Yes | Yes | Yes | Yes | Duties segregated to prevent fraud. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.2) | Yes |
| A.5.4 | Management responsibilities | Yes | Yes | Yes | Yes | Yes | Management ensures policy adherence. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.1) | Yes |
| A.5.5 | Contact with authorities | Yes | Yes | Yes | Yes | Yes | Contacts with law enforcement established. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.3) | Yes |
| A.5.6 | Contact with special interest groups | Yes | Yes | Yes | Yes | Yes | Membership in security forums. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.4) | Yes |
| A.5.7 | Threat intelligence | Yes | Yes | Yes | Yes | Yes | Threat intelligence collection process in place. | Internal | ISO27001 standard annexure | N/A | New (A.5.7) | No |
| A.5.8 | Information security in project management | Yes | Yes | Yes | Yes | Yes | Security integrated into projects. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.5) | Yes |
| A.5.9 | Inventory of information and other associated assets | Yes | Yes | Yes | Yes | Yes | Asset inventory maintained. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.1.1) | Yes |
| A.5.10 | Acceptable use of information and other associated assets | Yes | Yes | Yes | Yes | Yes | Acceptable use policies defined. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.1.3) | Yes |
| A.5.11 | Return of assets | Yes | Yes | Yes | Yes | Yes | Process for returning assets on termination. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.1.4) | Yes |
| A.5.12 | Classification of information | Yes | Yes | Yes | Yes | Yes | Information classified by sensitivity. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.2.1) | Yes |
| A.5.13 | Labelling of information | Yes | Yes | Yes | Yes | Yes | Information labeled per classification. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.2.2) | Yes |
| A.5.14 | Information transfer | Yes | Yes | Yes | Yes | Yes | Secure information transfer processes. | Internal | ISO27001 standard annexure | N/A | Old (From A.13.2.1) | Yes |
| A.5.15 | Access control | Yes | Yes | Yes | Yes | Yes | Access control policy implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.1.1) | Yes |
| A.5.16 | Identity management | Yes | Yes | Yes | Yes | Yes | Identity management processes in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.2.1) | Yes |
| A.5.17 | Authentication information | Yes | Yes | Yes | Yes | Yes | Secure management of authentication info. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.2.4) | Yes |
| A.5.18 | Access rights | Yes | Yes | Yes | Yes | Yes | Access rights reviewed regularly. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.2.5) | Yes |
| A.5.19 | Information security in supplier relationships | Yes | Yes | Yes | Yes | Yes | Security requirements in supplier agreements. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.1.1) | Yes |
| A.5.20 | Addressing information security within supplier agreements | Yes | Yes | Yes | Yes | Yes | Security clauses in supplier contracts. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.1.2) | Yes |
| A.5.21 | Managing information security in the ICT supply chain | Yes | Yes | Yes | Yes | Yes | Security managed across ICT supply chain. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.1.3) | Yes |
| A.5.22 | Monitoring, review, and change management of supplier services | Yes | Yes | Yes | Yes | Yes | Supplier services monitored and reviewed. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.2.1) | Yes |
| A.5.23 | Information security for use of cloud services | Yes | Yes | Yes | Yes | Yes | Policies for secure cloud service use. | Internal | ISO27001 standard annexure | N/A | New (A.5.23) | No |
| A.5.24 | Information security incident management planning and preparation | Yes | Yes | Yes | Yes | Yes | Incident management plan established. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.1) | Yes |
| A.5.25 | Assessment and decision on information security events | Yes | Yes | Yes | Yes | Yes | Process to assess security events. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.4) | Yes |
| A.5.26 | Response to information security incidents | Yes | Yes | Yes | Yes | Yes | Incident response procedures defined. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.5) | Yes |
| A.5.27 | Learning from information security incidents | Yes | Yes | Yes | Yes | Yes | Lessons learned from incidents documented. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.6) | Yes |
| A.5.28 | Collection of evidence | Yes | Yes | Yes | Yes | Yes | Evidence collection procedures in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.7) | Yes |
| A.5.29 | Information security during disruption | Yes | Yes | Yes | Yes | Yes | Security maintained during disruptions. | Internal | ISO27001 standard annexure | N/A | Old (From A.17.1.1) | Yes |
| A.5.30 | ICT readiness for business continuity | Yes | Yes | Yes | Yes | Yes | ICT readiness plan for continuity. | Internal | ISO27001 standard annexure | N/A | New (A.5.30) | No |
| A.5.31 | Legal, statutory, regulatory, and contractual requirements | Yes | Yes | Yes | Yes | Yes | Compliance with legal requirements. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.1.1) | Yes |
| A.5.32 | Intellectual property rights | Yes | Yes | Yes | Yes | Yes | Processes to protect intellectual property. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.1.2) | Yes |
| A.5.33 | Protection of records | Yes | Yes | Yes | Yes | Yes | Records protected from unauthorized access. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.1.3) | Yes |
| A.5.34 | Privacy and protection of PII | Yes | Yes | Yes | Yes | Yes | PII protected per regulations. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.1.4) | Yes |
| A.5.35 | Independent review of information security | Yes | Yes | Yes | Yes | Yes | Independent reviews conducted periodically. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.2.1) | Yes |
| A.5.36 | Compliance with security policies and standards | Yes | Yes | Yes | Yes | Yes | Compliance with policies monitored. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.2.2) | Yes |
| A.5.37 | Documented operating procedures | Yes | Yes | Yes | Yes | Yes | Operating procedures documented. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.1.1) | Yes |
| **PEOPLE CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |  |
| A.6.1 | Screening | Yes | Yes | Yes | Yes | Yes | Background checks for employees. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.1.1) | Yes |
| A.6.2 | Terms and conditions of employment | Yes | Yes | Yes | Yes | Yes | Security responsibilities in contracts. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.1.2) | Yes |
| A.6.3 | Information security awareness, education, and training | Yes | Yes | Yes | Yes | Yes | Security awareness training provided. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.2.2) | Yes |
| A.6.4 | Disciplinary process | Yes | Yes | Yes | Yes | Yes | Disciplinary process for breaches. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.2.3) | Yes |
| A.6.5 | Responsibilities after termination or change of employment | Yes | Yes | Yes | Yes | Yes | Responsibilities defined for termination. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.3.1) | Yes |
| A.6.6 | Confidentiality or non-disclosure agreements | Yes | Yes | Yes | Yes | Yes | NDAs signed by employees and third parties. | Internal | ISO27001 standard annexure | N/A | Old (From A.13.2.4) | Yes |
| A.6.7 | Remote working | Yes | Yes | Yes | Yes | Yes | Policy for securing remote work. | Internal | ISO27001 standard annexure | N/A | Old (Renamed from A.6.2.2 Teleworking) | Yes |
| A.6.8 | Information security event reporting | Yes | Yes | Yes | Yes | Yes | Process for reporting security events. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.2) | Yes |
| **PHYSICAL CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |  |
| A.7.1 | Physical security perimeters | Yes | Yes | Yes | Yes | Yes | Perimeters secured with controls. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.1) | Yes |
| A.7.2 | Physical entry controls | Yes | Yes | Yes | Yes | Yes | Entry controls to secure areas. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.2) | Yes |
| A.7.3 | Securing offices, rooms, and facilities | Yes | Yes | Yes | Yes | Yes | Offices secured against threats. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.3) | Yes |
| A.7.4 | Physical security monitoring | Yes | Yes | Yes | Yes | Yes | Physical security monitored with CCTV. | Internal | ISO27001 standard annexure | N/A | New (A.7.4) | No |
| A.7.5 | Protecting against physical and environmental threats | Yes | Yes | Yes | Yes | Yes | Protections against fire, flood, etc. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.4) | Yes |
| A.7.6 | Working in secure areas | Yes | Yes | Yes | Yes | Yes | Procedures for secure areas. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.5) | Yes |
| A.7.7 | Clear desk and clear screen | Yes | Yes | Yes | Yes | Yes | Clear desk and screen policies enforced. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.9) | Yes |
| A.7.8 | Equipment siting and protection | Yes | Yes | Yes | Yes | Yes | Equipment protected from threats. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.1) | Yes |
| A.7.9 | Security of assets off-premises | Yes | Yes | Yes | Yes | Yes | Security for assets off-premises. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.6) | Yes |
| A.7.10 | Storage media | Yes | Yes | Yes | Yes | Yes | Storage media securely managed. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.3.1) | Yes |
| A.7.11 | Supporting utilities | Yes | Yes | Yes | Yes | Yes | Utilities like power secured. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.2) | Yes |
| A.7.12 | Cabling security | Yes | Yes | Yes | Yes | Yes | Cabling protected from tampering. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.3) | Yes |
| A.7.13 | Equipment maintenance | Yes | Yes | Yes | Yes | Yes | Equipment maintenance scheduled. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.4) | Yes |
| A.7.14 | Secure disposal or reuse of equipment | Yes | Yes | Yes | Yes | Yes | Secure disposal processes in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.7) | Yes |
| **TECHNOLOGICAL CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |  |
| A.8.1 | User endpoint devices | Yes | Yes | Yes | Yes | Yes | Policy for securing endpoint devices. | Internal | ISO27001 standard annexure | N/A | Old (Expanded from A.6.2.1) | Yes |
| A.8.2 | Privileged access rights | Yes | Yes | Yes | Yes | Yes | Privileged access rights controlled. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.2.3) | Yes |
| A.8.3 | Information access restriction | Yes | Yes | Yes | Yes | Yes | Access restricted based on need-to-know. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.4.1) | Yes |
| A.8.4 | Access to source code | Yes | Yes | Yes | Yes | Yes | Access to source code restricted. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.4.5) | Yes |
| A.8.5 | Secure authentication | Yes | Yes | Yes | Yes | Yes | Secure authentication mechanisms in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.4.2) | Yes |
| A.8.6 | Capacity management | Yes | Yes | Yes | Yes | Yes | Capacity monitored and managed. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.1.3) | Yes |
| A.8.7 | Protection against malware | Yes | Yes | Yes | Yes | Yes | Anti-malware controls implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.2.1) | Yes |
| A.8.8 | Management of technical vulnerabilities | Yes | Yes | Yes | Yes | Yes | Vulnerabilities identified and mitigated. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.6.1) | Yes |
| A.8.9 | Configuration management | Yes | Yes | Yes | Yes | Yes | Configuration management processes defined. | Internal | ISO27001 standard annexure | N/A | New (A.8.9) | No |
| A.8.10 | Information deletion | Yes | Yes | Yes | Yes | Yes | Processes for secure information deletion. | Internal | ISO27001 standard annexure | N/A | New (A.8.10) | No |
| A.8.11 | Data masking | Yes | Yes | Yes | Yes | Yes | Data masking for sensitive data. | Internal | ISO27001 standard annexure | N/A | New (A.8.11) | No |
| A.8.12 | Data leakage prevention | Yes | Yes | Yes | Yes | Yes | DLP measures implemented. | Internal | ISO27001 standard annexure | N/A | New (A.8.12) | No |
| A.8.13 | Information backup | Yes | Yes | Yes | Yes | Yes | Backup processes in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.3.1) | Yes |
| A.8.14 | Redundancy of information processing facilities | Yes | Yes | Yes | Yes | Yes | Redundancy for critical systems. | Internal | ISO27001 standard annexure | N/A | Old (From A.17.2.1) | Yes |
| A.8.15 | Logging | Yes | Yes | Yes | Yes | Yes | Logging of system activities implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.4.1) | Yes |
| A.8.16 | Monitoring activities | Yes | Yes | Yes | Yes | Yes | Monitoring for system anomalies. | Internal | ISO27001 standard annexure | N/A | New (A.8.16) | No |
| A.8.17 | Clock synchronization | Yes | Yes | Yes | Yes | Yes | Clocks synchronized for logging. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.4.4) | Yes |
| A.8.18 | Use of privileged utility programs | Yes | Yes | Yes | Yes | Yes | Use of privileged utilities controlled. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.4.4) | Yes |
| A.8.19 | Installation of software on operational systems | Yes | Yes | Yes | Yes | Yes | Software installation controlled. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.5.1) | Yes |
| A.8.20 | Networks security | Yes | Yes | Yes | Yes | Yes | Network security controls implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.13.1.1) | Yes |
| A.8.21 | Security of network services | Yes | Yes | Yes | Yes | Yes | Network services secured. | Internal | ISO27001 standard annexure | N/A | Old (From A.13.1.2) | Yes |
| A.8.22 | Segregation of networks | Yes | Yes | Yes | Yes | Yes | Networks segregated based on risk. | Internal | ISO27001 standard annexure | N/A | Old (From A.13.1.3) | Yes |
| A.8.23 | Web filtering | Yes | Yes | Yes | Yes | Yes | Web filtering to block malicious sites. | Internal | ISO27001 standard annexure | N/A | New (A.8.23) | No |
| A.8.24 | Use of cryptography | Yes | Yes | Yes | Yes | Yes | Cryptographic controls implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.10.1.1) | Yes |
| A.8.25 | Secure development life cycle | Yes | Yes | Yes | Yes | Yes | Secure development processes defined. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.2.1) | Yes |
| A.8.26 | Application security requirements | Yes | Yes | Yes | Yes | Yes | Security requirements in development. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.1.2) | Yes |
| A.8.27 | Secure system architecture and engineering principles | Yes | Yes | Yes | Yes | Yes | Secure architecture principles applied. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.2.5) | Yes |
| A.8.28 | Secure coding | Yes | Yes | Yes | Yes | Yes | Secure coding practices implemented. | Internal | ISO27001 standard annexure | N/A | New (A.8.28) | No |
| A.8.29 | Security testing in development and acceptance | Yes | Yes | Yes | Yes | Yes | Security testing during development. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.2.8) | Yes |
| A.8.30 | Outsourced development | Yes | Yes | Yes | Yes | Yes | Security for outsourced development. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.2.7) | Yes |
| A.8.31 | Separation of development, test, and production environments | Yes | Yes | Yes | Yes | Yes | Environments separated to reduce risk. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.1.4) | Yes |
| A.8.32 | Change management | Yes | Yes | Yes | Yes | Yes | Change management processes in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.1.2) | Yes |
| A.8.33 | Test information | Yes | Yes | Yes | Yes | Yes | Test data protected and controlled. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.3.1) | Yes |
| A.8.34 | Protection of information systems during audit testing | Yes | Yes | Yes | Yes | Yes | Systems protected during audits. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.7.1) | Yes |

### **Step 5: Explanation of New Columns**

* **New/Old (New Control)**: Indicates if the control is “New” (introduced in 2022) or “Old” (carried over from 2013). For new controls, the control number is specified (e.g., New (A.5.7)).
* **Implemented in Old Standard (Yes/No)**: Indicates whether the control was implemented under ISO 27001:2013. For controls marked “Old,” this is “Yes” (based on the image’s pattern of applicability). For new controls, this is “No,” as they were not part of the 2013 standard.

### **Step 6: Key Observations**

* **Merged Controls**: A.5.1 in 2022 merges A.5.1.1 and A.5.1.2 from 2013, combining policy definition and review.
* **Renamed Controls**: A.6.2.2 (Teleworking) is renamed to A.6.7 (Remote working).
* **Expanded Controls**: A.6.2.1 (Mobile device policy) is now A.8.1 (User endpoint devices), covering all endpoint devices.
* **New Controls**: The 11 new controls (e.g., A.5.7, A.5.23, A.8.28) address modern needs like threat intelligence, cloud security, and secure coding, and were not implemented in the 2013 standard.

### **Step 7: Recommendations**

* **Verify Implementation**: The “Implemented in Old Standard” column assumes “Yes” for old controls based on the image. Confirm the actual implementation status in your organization.
* **Review Applicability**: All controls are marked “Yes” for applicability and requirements, following the image’s pattern. Reassess each control for your context.
* **Customize Descriptions**: The “Description/Commentary” column uses placeholders. Tailor these to reflect your organization’s implementation.
* **Risk Assessment**: Reassess risks for new controls like A.5.7 (Threat intelligence) and A.5.23 (Cloud services).
* **Update Documentation**: Align policies and ITRMS references with the 2022 standard.

This table provides a complete SoA for ISO 27001:2022, formatted like the one in the image, with the requested columns for comparison and implementation status. If you need further adjustments or specific details, let me know!