I understand you’d like the entire Statement of Applicability (SoA) table updated to ISO 27001:2022, covering all controls (not just those visible in the image), with a new column indicating whether each control is “New” or “Old” compared to ISO 27001:2013, and specifying new controls where applicable. The table should match the format of the existing SoA shown in the image, which includes 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**

We’ll add a new column: **“New/Old (New Control)”** to indicate whether the control is new or old and highlight new controls introduced in 2022.

### **Step 1: Overview of ISO 27001:2013 vs. ISO 27001:2022**

* **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 version introduced 11 new controls, merged some existing ones, and reorganized others. The image shows controls from A.5 and A.6, but you’ve requested the entire table, so I’ll cover all 93 controls in the 2022 standard, map them to their 2013 equivalents where applicable, and include the new/old comparison.

### **Step 2: Mapping and New Controls**

I’ll map all 2013 controls to their 2022 equivalents and identify the 11 new controls introduced in 2022:

* **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: Build the Entire SoA Table**

Since the image shows a pattern (all controls 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 otherwise specified. The “Description/Commentary” and “Rationale for Exclusion” columns will be filled with placeholder text where necessary, as these are organization-specific.

Below is the complete SoA table for ISO 27001:2022, with all 93 controls, formatted like the table in the image, and including the new column for comparison.

| **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)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ORGANIZATIONAL CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |
| A.5.1 | Information security policies | Yes | Yes | Yes | Yes | Yes | Policies defined and documented; reviewed annually. | Internal | ISO27001 standard annexure | N/A | Old (Merged A.5.1.1 and A.5.1.2) |
| A.5.2 | Information security roles and responsibilities | Yes | Yes | Yes | Yes | Yes | Roles and responsibilities assigned to security team. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.1) |
| A.5.3 | Segregation of duties | Yes | Yes | Yes | Yes | Yes | Duties segregated to prevent fraud and errors. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.2) |
| A.5.4 | Management responsibilities | Yes | Yes | Yes | Yes | Yes | Management ensures security policies are followed. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.1) |
| A.5.5 | Contact with authorities | Yes | Yes | Yes | Yes | Yes | Contacts established with law enforcement. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.3) |
| A.5.6 | Contact with special interest groups | Yes | Yes | Yes | Yes | Yes | Membership in security forums for knowledge sharing. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.4) |
| A.5.7 | Threat intelligence | Yes | Yes | Yes | Yes | Yes | Process to collect and analyze threat intelligence. | Internal | ISO27001 standard annexure | N/A | New (A.5.7) |
| A.5.8 | Information security in project management | Yes | Yes | Yes | Yes | Yes | Security integrated into project management. | Internal | ISO27001 standard annexure | N/A | Old (From A.6.1.5) |
| A.5.9 | Inventory of information and other associated assets | Yes | Yes | Yes | Yes | Yes | Asset inventory maintained and updated. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.1.1) |
| A.5.10 | Acceptable use of information and other associated assets | Yes | Yes | Yes | Yes | Yes | Acceptable use policies defined and communicated. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.1.3) |
| A.5.11 | Return of assets | Yes | Yes | Yes | Yes | Yes | Process for returning assets upon termination. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.1.4) |
| A.5.12 | Classification of information | Yes | Yes | Yes | Yes | Yes | Information classified based on sensitivity. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.2.1) |
| A.5.13 | Labelling of information | Yes | Yes | Yes | Yes | Yes | Information labeled according to classification. | Internal | ISO27001 standard annexure | N/A | Old (From A.8.2.2) |
| A.5.14 | Information transfer | Yes | Yes | Yes | Yes | Yes | Secure processes for information transfer. | Internal | ISO27001 standard annexure | N/A | Old (From A.13.2.1) |
| A.5.15 | Access control | Yes | Yes | Yes | Yes | Yes | Access control policy defined and implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.1.1) |
| 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) |
| A.5.17 | Authentication information | Yes | Yes | Yes | Yes | Yes | Secure management of authentication information. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.2.4) |
| A.5.18 | Access rights | Yes | Yes | Yes | Yes | Yes | Access rights reviewed and updated regularly. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.2.5) |
| A.5.19 | Information security in supplier relationships | Yes | Yes | Yes | Yes | Yes | Security requirements included in supplier agreements. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.1.1) |
| A.5.20 | Addressing information security within supplier agreements | Yes | Yes | Yes | Yes | Yes | Security clauses included in supplier contracts. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.1.2) |
| A.5.21 | Managing information security in the ICT supply chain | Yes | Yes | Yes | Yes | Yes | Security managed across the ICT supply chain. | Internal | ISO27001 standard annexure | N/A | Old (From A.15.1.3) |
| 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) |
| A.5.23 | Information security for use of cloud services | Yes | Yes | Yes | Yes | Yes | Policies for secure use of cloud services. | Internal | ISO27001 standard annexure | N/A | New (A.5.23) |
| A.5.24 | Information security incident management planning and preparation | Yes | Yes | Yes | Yes | Yes | Incident management plan in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.1) |
| A.5.25 | Assessment and decision on information security events | Yes | Yes | Yes | Yes | Yes | Process to assess and decide on security events. | Internal | ISO27001 standard annexure | N/A | Old (From A.16.1.4) |
| 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) |
| 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) |
| 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) |
| 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) |
| A.5.30 | ICT readiness for business continuity | Yes | Yes | Yes | Yes | Yes | ICT readiness plan for business continuity. | Internal | ISO27001 standard annexure | N/A | New (A.5.30) |
| A.5.31 | Legal, statutory, regulatory, and contractual requirements | Yes | Yes | Yes | Yes | Yes | Compliance with legal and regulatory requirements. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.1.1) |
| 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) |
| 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) |
| A.5.34 | Privacy and protection of PII | Yes | Yes | Yes | Yes | Yes | PII protected in compliance with regulations. | Internal | ISO27001 standard annexure | N/A | Old (From A.18.1.4) |
| 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) |
| 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) |
| A.5.37 | Documented operating procedures | Yes | Yes | Yes | Yes | Yes | Operating procedures documented and maintained. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.1.1) |
| **PEOPLE CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |
| A.6.1 | Screening | Yes | Yes | Yes | Yes | Yes | Background checks conducted for employees. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.1.1) |
| A.6.2 | Terms and conditions of employment | Yes | Yes | Yes | Yes | Yes | Security responsibilities in employment contracts. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.1.2) |
| 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) |
| A.6.4 | Disciplinary process | Yes | Yes | Yes | Yes | Yes | Disciplinary process for security breaches. | Internal | ISO27001 standard annexure | N/A | Old (From A.7.2.3) |
| 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) |
| 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) |
| A.6.7 | Remote working | Yes | Yes | Yes | Yes | Yes | Policy for securing remote work environments. | Internal | ISO27001 standard annexure | N/A | Old (Renamed from A.6.2.2 Teleworking) |
| 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) |
| **PHYSICAL CONTROLS** |  |  |  |  |  |  |  |  |  |  |  |
| A.7.1 | Physical security perimeters | Yes | Yes | Yes | Yes | Yes | Physical perimeters secured with controls. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.1) |
| A.7.2 | Physical entry controls | Yes | Yes | Yes | Yes | Yes | Entry controls to secure areas implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.2) |
| A.7.3 | Securing offices, rooms, and facilities | Yes | Yes | Yes | Yes | Yes | Offices and facilities secured against threats. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.3) |
| 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) |
| 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) |
| A.7.6 | Working in secure areas | Yes | Yes | Yes | Yes | Yes | Procedures for working in secure areas. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.1.5) |
| 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) |
| A.7.8 | Equipment siting and protection | Yes | Yes | Yes | Yes | Yes | Equipment protected from physical threats. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.1) |
| A.7.9 | Security of assets off-premises | Yes | Yes | Yes | Yes | Yes | Security for assets off-premises ensured. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.6) |
| 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) |
| A.7.11 | Supporting utilities | Yes | Yes | Yes | Yes | Yes | Utilities like power and cooling secured. | Internal | ISO27001 standard annexure | N/A | Old (From A.11.2.2) |
| 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) |
| 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) |
| 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) |
| **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) |
| 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) |
| 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) |
| 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) |
| A.8.5 | Secure authentication | Yes | Yes | Yes | Yes | Yes | Secure authentication mechanisms implemented. | Internal | ISO27001 standard annexure | N/A | Old (From A.9.4.2) |
| 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) |
| A.8.7 | Protection against malware | Yes | Yes | Yes | Yes | Yes | Anti-malware controls in place. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.2.1) |
| 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) |
| A.8.9 | Configuration management | Yes | Yes | Yes | Yes | Yes | Configuration management processes defined. | Internal | ISO27001 standard annexure | N/A | New (A.8.9) |
| 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) |
| A.8.11 | Data masking | Yes | Yes | Yes | Yes | Yes | Data masking applied to sensitive data. | Internal | ISO27001 standard annexure | N/A | New (A.8.11) |
| A.8.12 | Data leakage prevention | Yes | Yes | Yes | Yes | Yes | DLP measures implemented. | Internal | ISO27001 standard annexure | N/A | New (A.8.12) |
| 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) |
| A.8.14 | Redundancy of information processing facilities | Yes | Yes | Yes | Yes | Yes | Redundancy for critical systems ensured. | Internal | ISO27001 standard annexure | N/A | Old (From A.17.2.1) |
| 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) |
| A.8.16 | Monitoring activities | Yes | Yes | Yes | Yes | Yes | Monitoring of systems for anomalies. | Internal | ISO27001 standard annexure | N/A | New (A.8.16) |
| A.8.17 | Clock synchronization | Yes | Yes | Yes | Yes | Yes | Clocks synchronized for accurate logging. | Internal | ISO27001 standard annexure | N/A | Old (From A.12.4.4) |
| 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) |
| 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) |
| 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) |
| 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) |
| 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) |
| 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) |
| 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) |
| 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) |
| A.8.26 | Application security requirements | Yes | Yes | Yes | Yes | Yes | Security requirements in application development. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.1.2) |
| 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) |
| A.8.28 | Secure coding | Yes | Yes | Yes | Yes | Yes | Secure coding practices implemented. | Internal | ISO27001 standard annexure | N/A | New (A.8.28) |
| 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) |
| A.8.30 | Outsourced development | Yes | Yes | Yes | Yes | Yes | Security requirements for outsourced development. | Internal | ISO27001 standard annexure | N/A | Old (From A.14.2.7) |
| 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) |
| 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) |
| 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) |
| 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) |

### **Step 4: Explanation of the New Column**

* **New/Old (New Control)**: Indicates whether 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)). For old controls, I note significant changes like merging, renaming, or expansion.

### **Step 5: Key Observations**

* **Merged Controls**: Some 2013 controls were merged in 2022 (e.g., A.5.1.1 and A.5.1.2 into A.5.1).
* **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.5.30) address modern security needs like threat intelligence, cloud services, and secure coding.

### **Step 6: Recommendations**

* **Review Applicability**: The table assumes all controls are applicable with “Yes” for all requirements, as seen in the image. You should review each control’s applicability to your organization.
* **Update Descriptions**: The “Description/Commentary” column uses placeholders. You should customize these based on your organization’s implementation.
* **Risk Assessment**: Reassess risks, especially for new controls like A.5.7 (Threat intelligence) and A.5.23 (Cloud services).
* **Document Updates**: Update your policies and ITRMS references to align with the 2022 standard.

This table provides a complete SoA for ISO 27001:2022, formatted like the one in the image, with the requested comparison column. If you need further customization or assistance with specific controls, let me know!