
# STEP 3: SELECT CONTROLS

# STEP 3: SELECT CONTROLS

The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

# STEP 3: SELECT CONTROLS

Controls are the tools the business uses to satisfy the cyber security supply chain and privacy requirements.

# STEP 3: SELECT CONTROLS

Controls can be classified as

- Technical - Anti-malware
- Administrative - Security Policies
- Physical - Security door

- Preventative - Anti-malware
- Detective - Logs/Auditing
- Corrective - Disaster Recovery Policy

## TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

| ID | FAMILY | ID | FAMILY |
|---|---|---|---|
| AC | Access Control | PE | Physical and Environmental Protection |
| AT | Awareness and Training | PL | Planning |
| AU | Audit and Accountability | PM | Program Management |
| CA | Assessment, Authorization, and Monitoring | PS | Personnel Security |
| CM | Configuration Management | PT | PII Processing and Transparency |
| CP | Contingency Planning | RA | Risk Assessment |
| IA | Identification and Authentication | SA | System and Services Acquisition |
| IR | Incident Response | SC | System and Communications Protection |
| MA | Maintenance | SI | System and Information Integrity |
| MP | Media Protection | SR | Supply Chain Risk Management |

# NIST SP 800-53 Rev.5

**TABLE 4: SELECT TASKS AND OUTCOMES**

| Tasks | Outcomes |
|---|---|
| **TASK S-1**<br>CONTROL SELECTION | • Control baselines necessary to protect the system commensurate with risk are selected.<br>[*Cybersecurity Framework*: **Profile**] |
| **TASK S-2**<br>CONTROL TAILORING | • Controls are tailored producing tailored control baselines.<br>[*Cybersecurity Framework*: **Profile**] |
| **TASK S-3**<br>CONTROL ALLOCATION | • Controls are designated as system-specific, hybrid, or common controls.<br>• Controls are allocated to the specific system elements (i.e., machine, physical, or human elements).<br>[*Cybersecurity Framework*: **Profile**; **PR.IP**] |
| **TASK S-4**<br>DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS | • Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.<br>[*Cybersecurity Framework*: **Profile**] |
| **TASK S-5**<br>CONTINUOUS MONITORING STRATEGY—SYSTEM | • A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.<br>[*Cybersecurity Framework*: **ID.GV**; **DE.CM**] |
| **TASK S-6**<br>PLAN REVIEW AND APPROVAL | • Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official. |
| | |

# TASK S-1

| | |
|---|---|
| **TASK S-1**<br>CONTROL SELECTION | • Control baselines necessary to protect the system commensurate with risk are selected.<br>[*Cybersecurity Framework*: **Profile**] |

Controls can be chosen by:

- Baseline control selection
- Organizational generated control selection

# Base Line Control Selection

A pre-written set of controls that were published to help the business with their security and privacy needs.

# Organization Generated Selection


DIY approach and could be more cost-effective

# TASK S-2

| | |
|---|---|
| **TASK S-2**<br>CONTROL TAILORING | • Controls are tailored producing tailored control baselines.<br>[*Cybersecurity Framework*: **Profile**] |

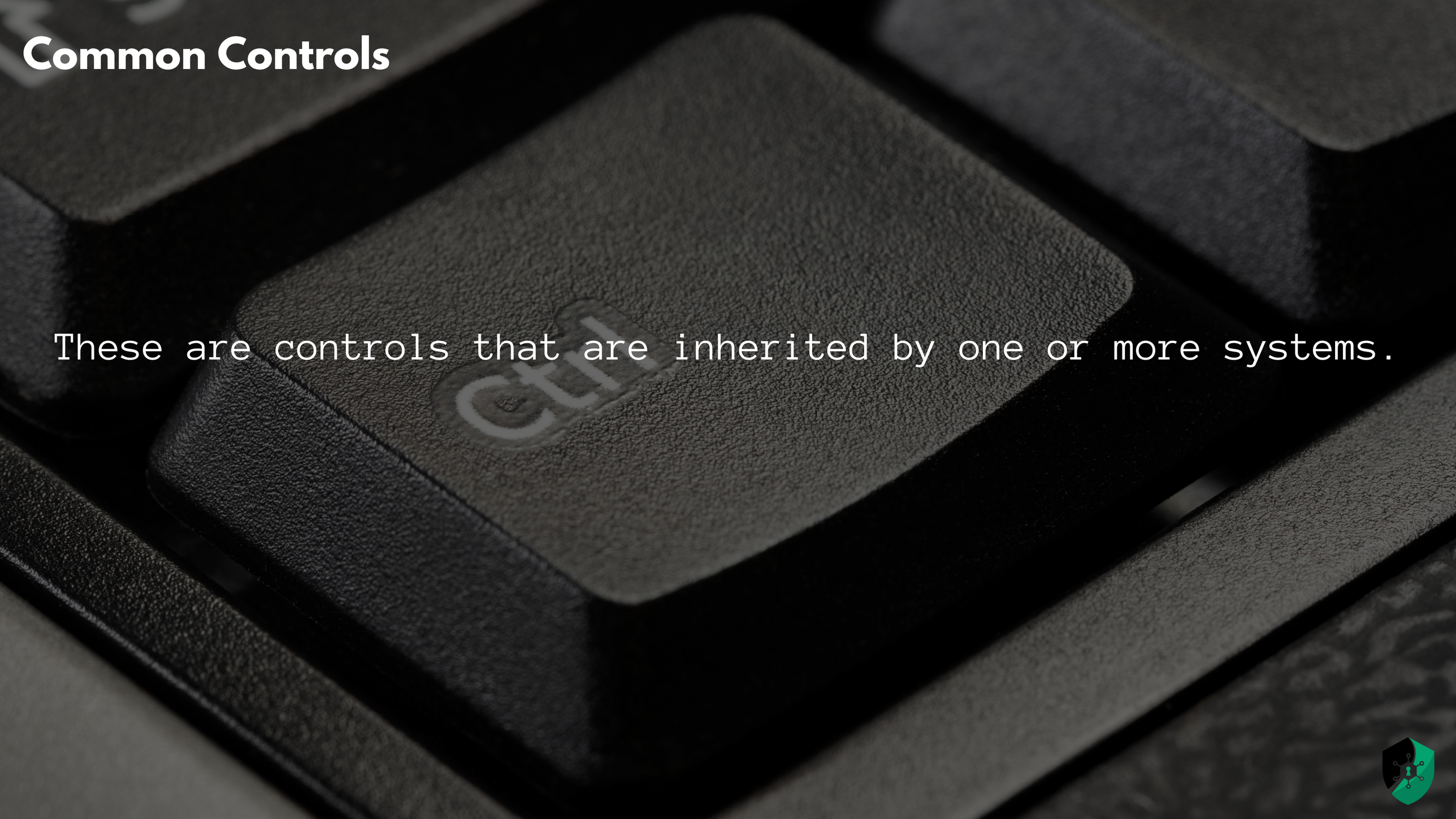
Controls are tailored based on various factors

- Threats
- Security & Privacy risks
- Mission & Business functions

# TASK S-3

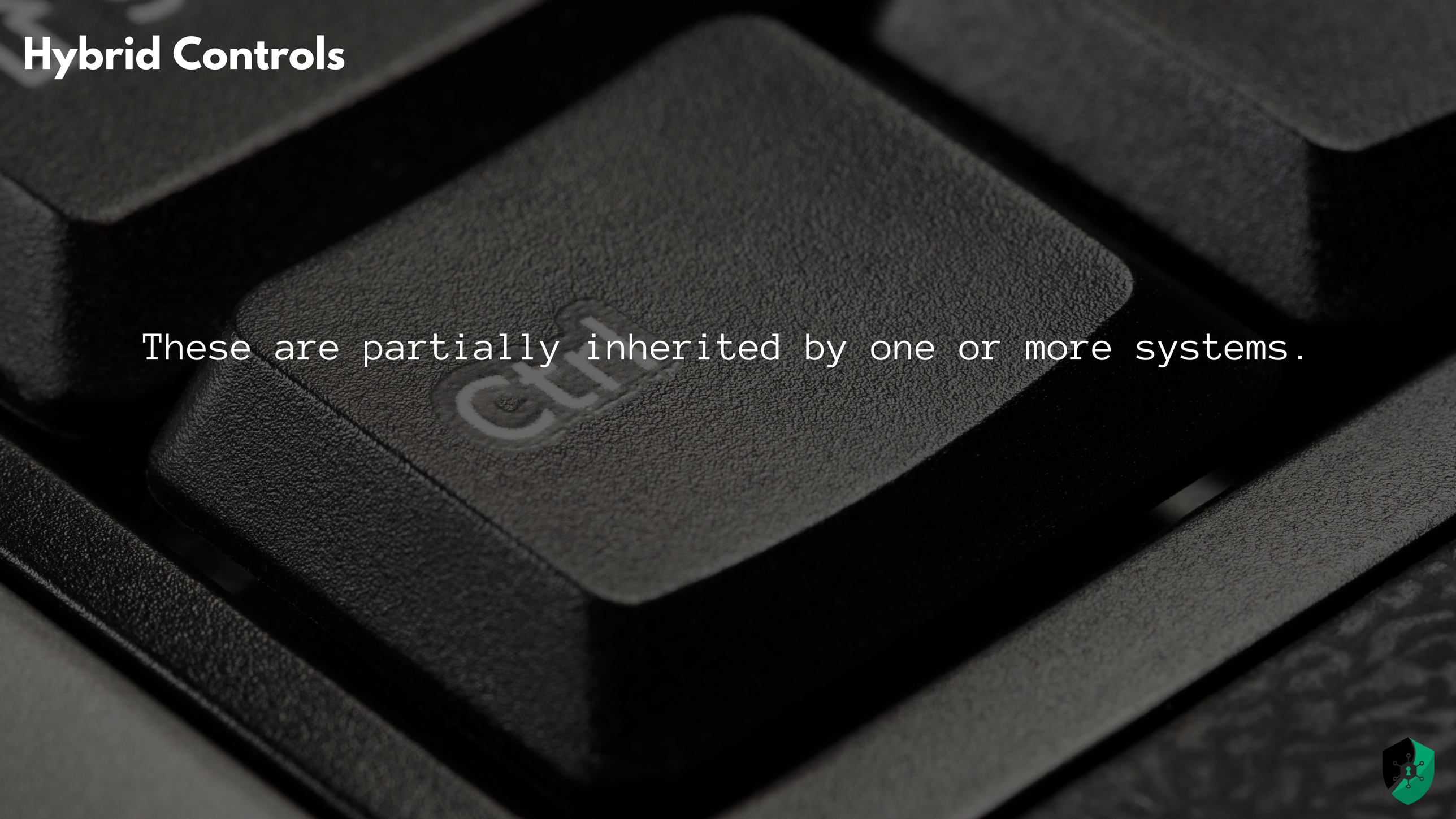
| | |
|---|---|
| **TASK S-3**<br>CONTROL ALLOCATION | • Controls are designated as system-specific, hybrid, or common controls.<br>• Controls are allocated to the specific system elements (i.e., machine, physical, or human elements).<br>[*Cybersecurity Framework*: **Profile**; **PR.IP**] |

# Common Controls



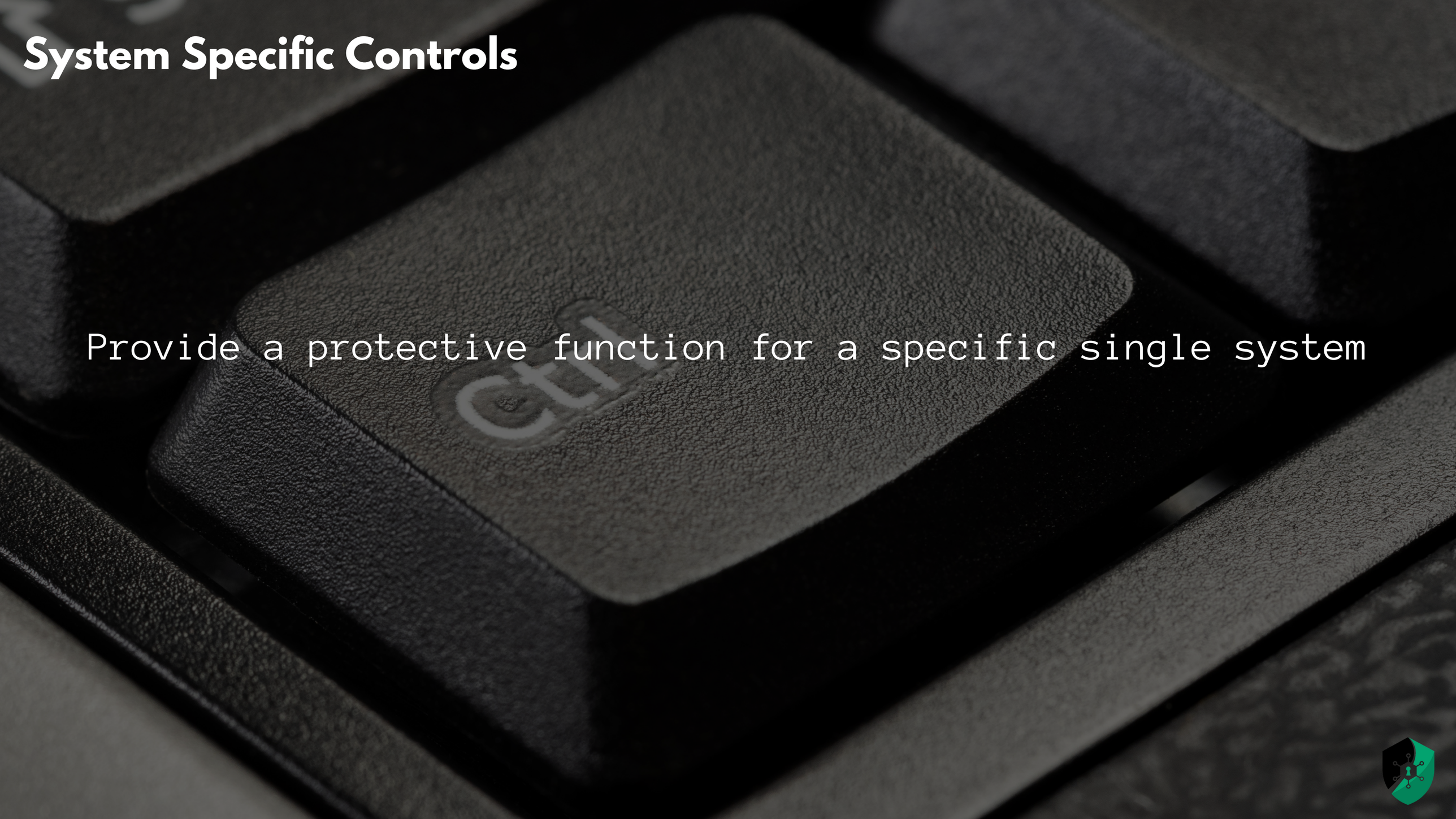

These are controls that are inherited by one or more systems.

# Hybrid Controls




These are partially inherited by one or more systems.

# System Specific Controls




Provide a protective function for a specific single system

# TASK S-4, S-5 & S-6

| | |
|---|---|
| **TASK S-4**<br>DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS | • Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**] |
| **TASK S-5**<br>CONTINUOUS MONITORING STRATEGY—SYSTEM | • A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV**; **DE.CM**] |
| **TASK S-6**<br>PLAN REVIEW AND APPROVAL | • Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official. |