STEP 1: PREPARE

STEP 1: PREPARE

The purpose is to carry out essential activities at the organization, mission and business process and information system levels of the organization to help prepare the organization to manage its security and privacy risks.

STEP 1: PREPARE

The tasks are divided into:

- Organization-level
- System-level

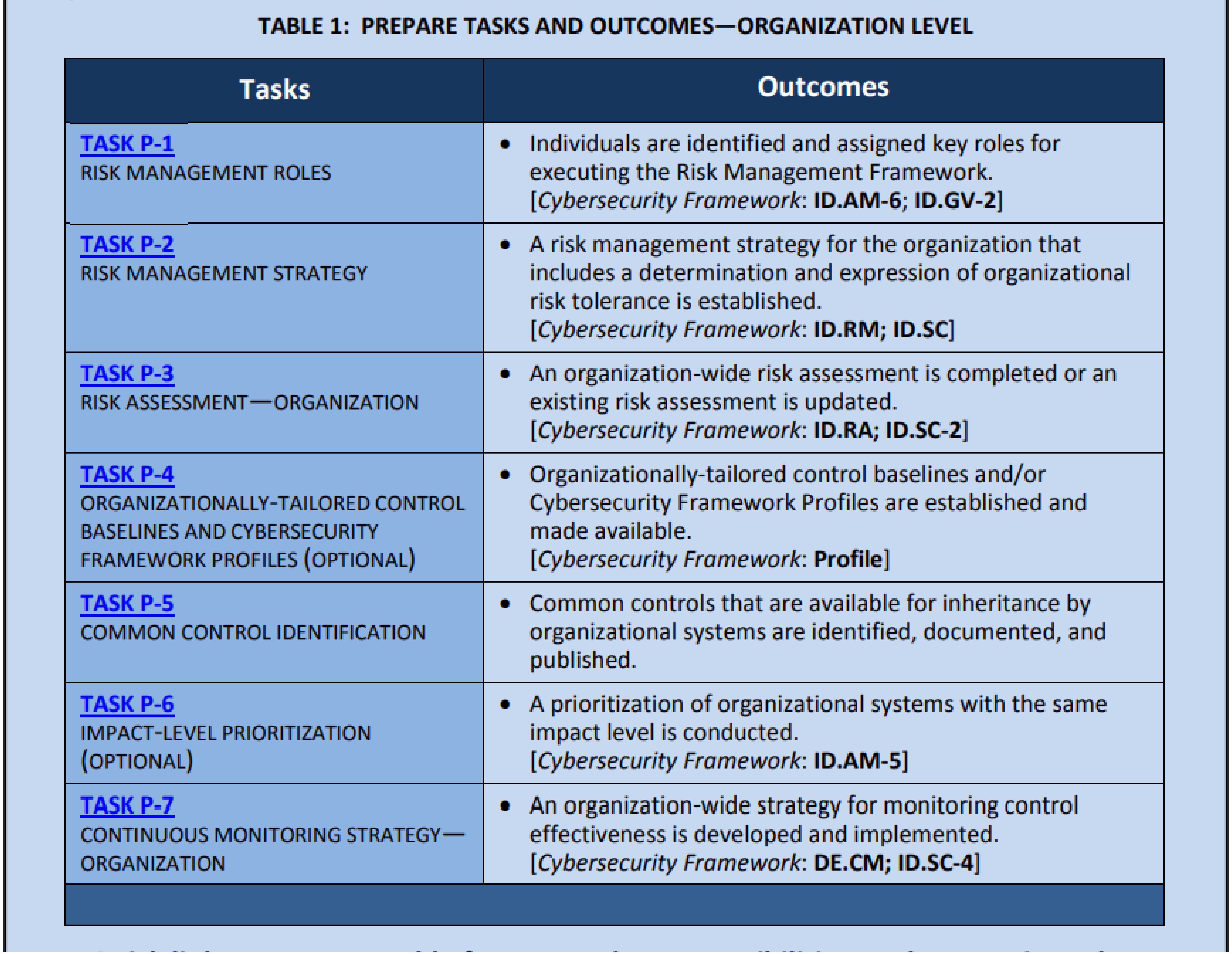
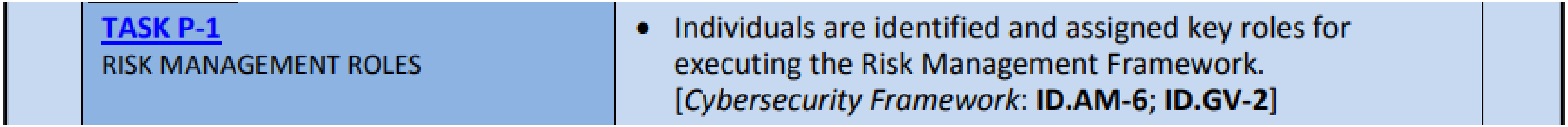


TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: **ID.AM-6**; **ID.GV-2**]
TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: **Profile**]
TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

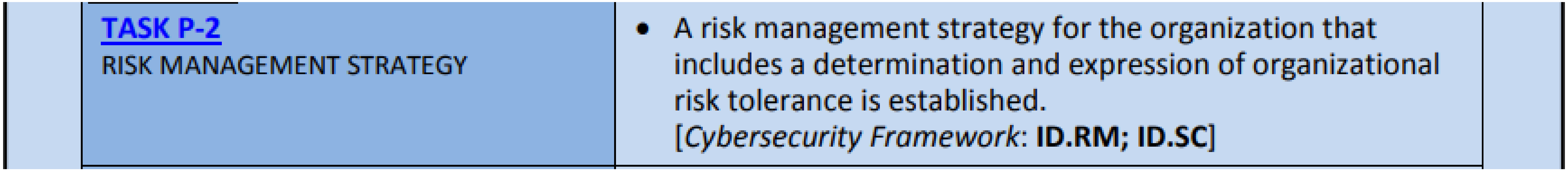
TASK P-1: RMR



	TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: **ID.AM-6; ID.GV-2**]	

Individuals can be assigned multiple roles but there must be no conflict of interest. Individuals can be internal or external to the organization

TASK P-2: RMS



TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**]

Risk tolerance refers to the degree of risk or uncertainty that is acceptable to your organization

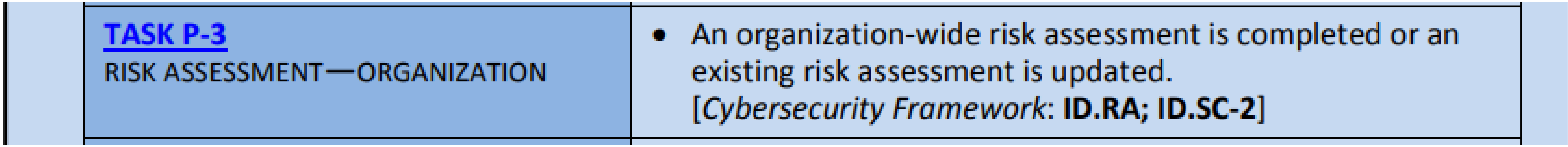
TASK P-2: RMS

Risk management strategy makes explicit the

- threats
- assumptions
- constraints
- priorities
- trade-offs
- risk tolerance

used for making investments and operational decisions.

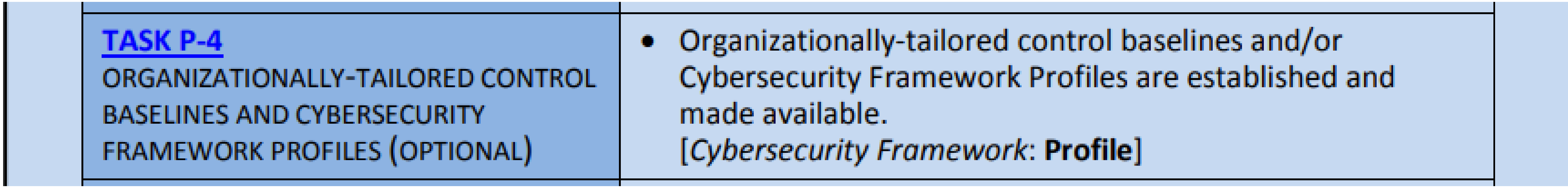
TASK P-3: RA



TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]

New risk assessment is conducted or an existing one is updated to help the organization establish a cybersecurity framework profile.

TASK P-4: TCB & CFP



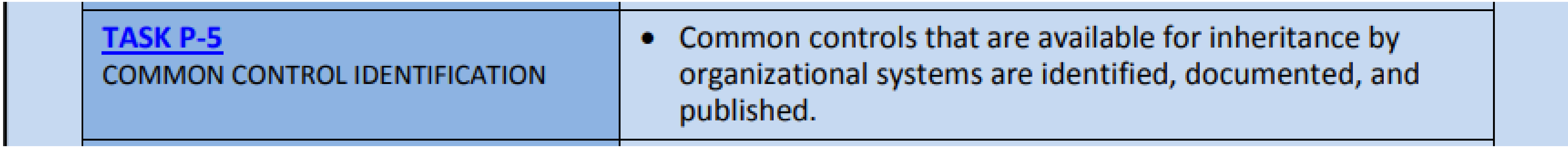
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: **Profile**]

To address the organizational mission or business need for specialized sets of controls to reduce risk, organizationally-tailored control baselines may be developed for organization-wide use

TASK P-4: TCB & CFP

An organizationally–tailored baseline provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established control baselines described in [SP 800–53B].

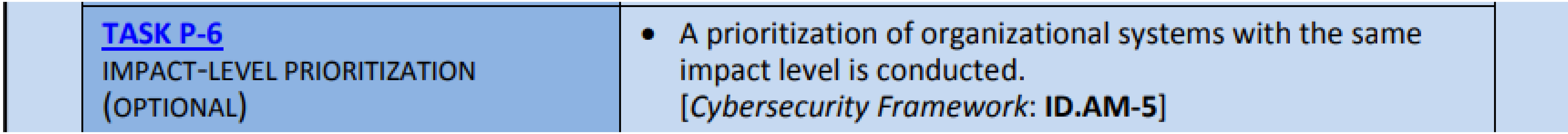
TASK P-5: CCI



TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.

Common controls are those that can be inherited by one or more information systems e.g endpoint security software

TASK P-6: ILP

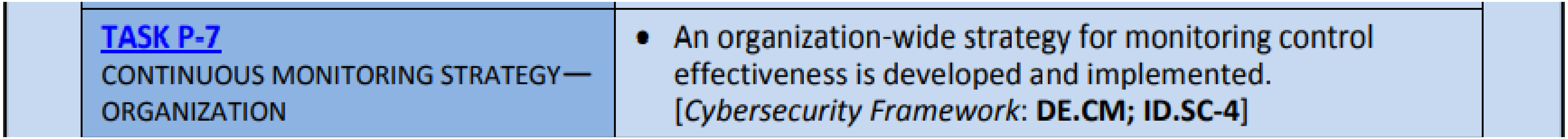


TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	- A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]

This is done only after organizational systems have been categorized (Task C1) based on impact (low, moderate or high).

Systems within the same impact level can be further subcategorized e.g (low-moderate, moderate-moderate, high-moderate)

TASK P-7: CMS



TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	- An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

The organizational continuous monitoring strategy addresses monitoring requirements at the organization, mission/business process, and information system levels.

TASK P-7: CMS

The continuous monitoring strategy identifies the minimum monitoring frequency for implemented controls across the organization; defines the ongoing control assessment approach; and describes how ongoing assessments are to be conducted