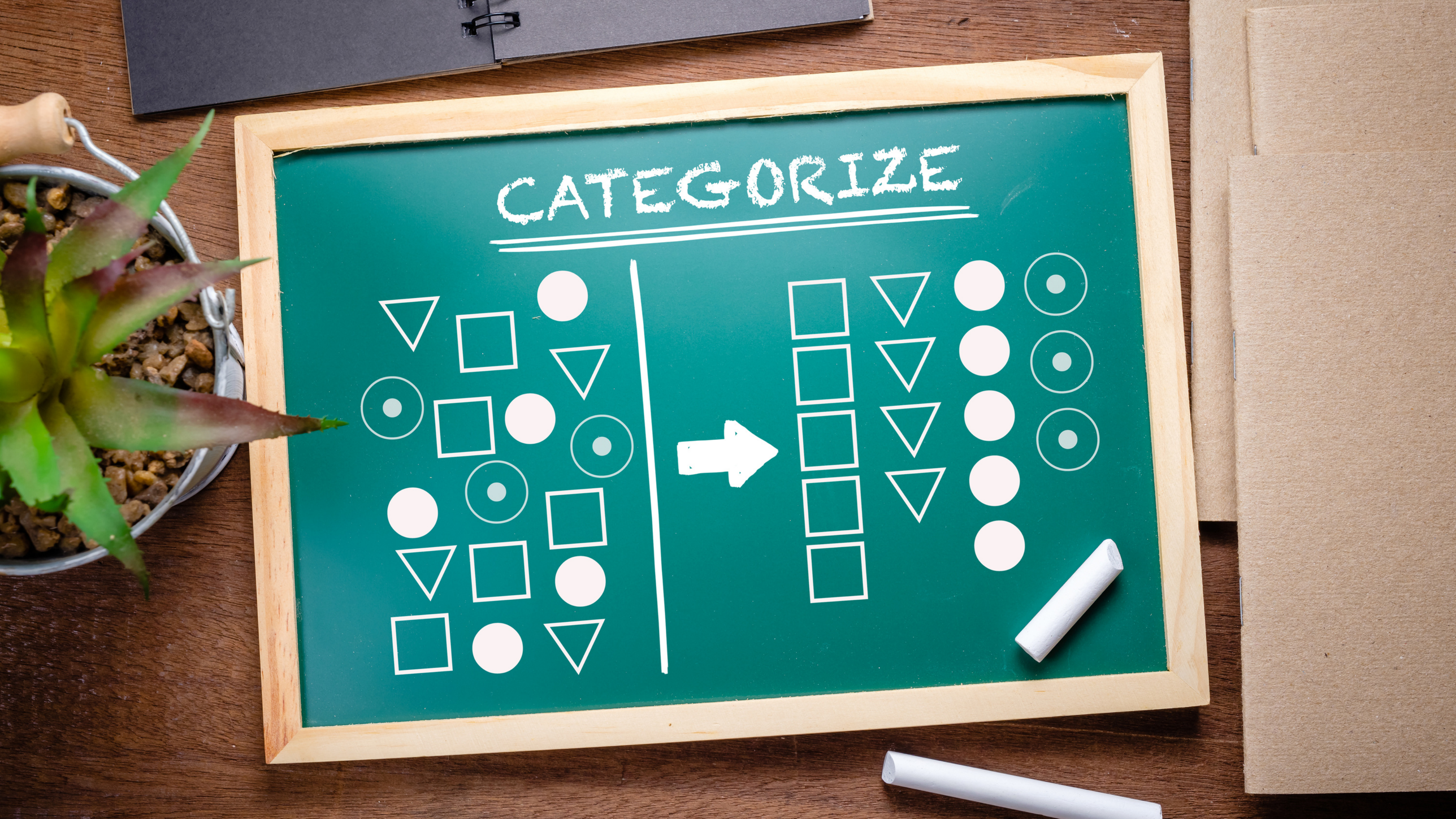
CATEGORIZE

STEP 2: CATEGORIZE

The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

STEP 2: CATEGORIZE

The purpose is to define criticality or sensitivity of information systems according to the worst case scenario and its adverse impact on the business.

STEP 2: CATEGORIZE

The result is used as the basis for developing the security plan, security controls and determining the risk inherent in operating the system.

TABLE 3: CATEGORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK C-1 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]
TASK C-2 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] • Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [*Cybersecurity Framework*: **Profile**] • Security categorization results reflect the organization's risk management strategy.
TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

TASK C-1

Tasks	Outcomes
TASK C-1 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]

Types of descriptive system information include:

- Name
- Version / release number
- Contact information
- Location
- Manufacturer
- Purpose

TASK C-2

TASK C-2 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] • Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [*Cybersecurity Framework*: **Profile**] • Security categorization results reflect the organization's risk management strategy.

TASK C-2

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TASK C-3

TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.