

# INFORMATION



# PRIVACY



## OMB CIRCULAR A-130: INTEGRATION OF INFORMATION SECURITY AND PRIVACY

In 2016, OMB revised Circular A-130, the circular establishing general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, information technology resources, and supporting infrastructure and services. The circular addresses responsibilities for protecting federal information resources and managing personally identifiable information (PII). In establishing requirements for information security programs and privacy programs, the circular emphasizes the need for both programs to collaborate on shared objectives:

*While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements.*

[[OMB A-130](#)] requires organizations to implement the RMF that is described in this guideline. With the 2016 revision to the circular, OMB also requires organizations to integrate privacy into the RMF process:

*The RMF provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the SDLC. This Circular requires organizations to use the RMF to manage privacy risks beyond those that are typically included under the “confidentiality” objective of the term “information security.” While many privacy risks relate to the unauthorized access or disclosure of PII, privacy risks may also result from other activities, including the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation.*

This section of the guideline describes the *relationship* between information security programs and privacy programs under the RMF. However, subject to OMB policy, organizations retain the flexibility to undertake the integration of privacy into the RMF in the most effective manner, considering the organization’s mission and circumstances.



The background of the slide features a dark, monochromatic aesthetic. A hand is shown holding a tablet, which displays a large, semi-transparent word 'SECURITY' in the center. The word is rendered in a bold, sans-serif font. Surrounding the word and the hand are various digital and technical motifs: faint binary code (0s and 1s) is scattered across the background; thin, glowing blue lines suggest circuitry or data flow; and several gear icons are visible, particularly around the tablet and the word 'SECURITY'. The overall composition conveys a sense of digital security and technology.

OMB – United States Office of Management & Budget

Circulars are memos that tell other federal agencies what they need to do



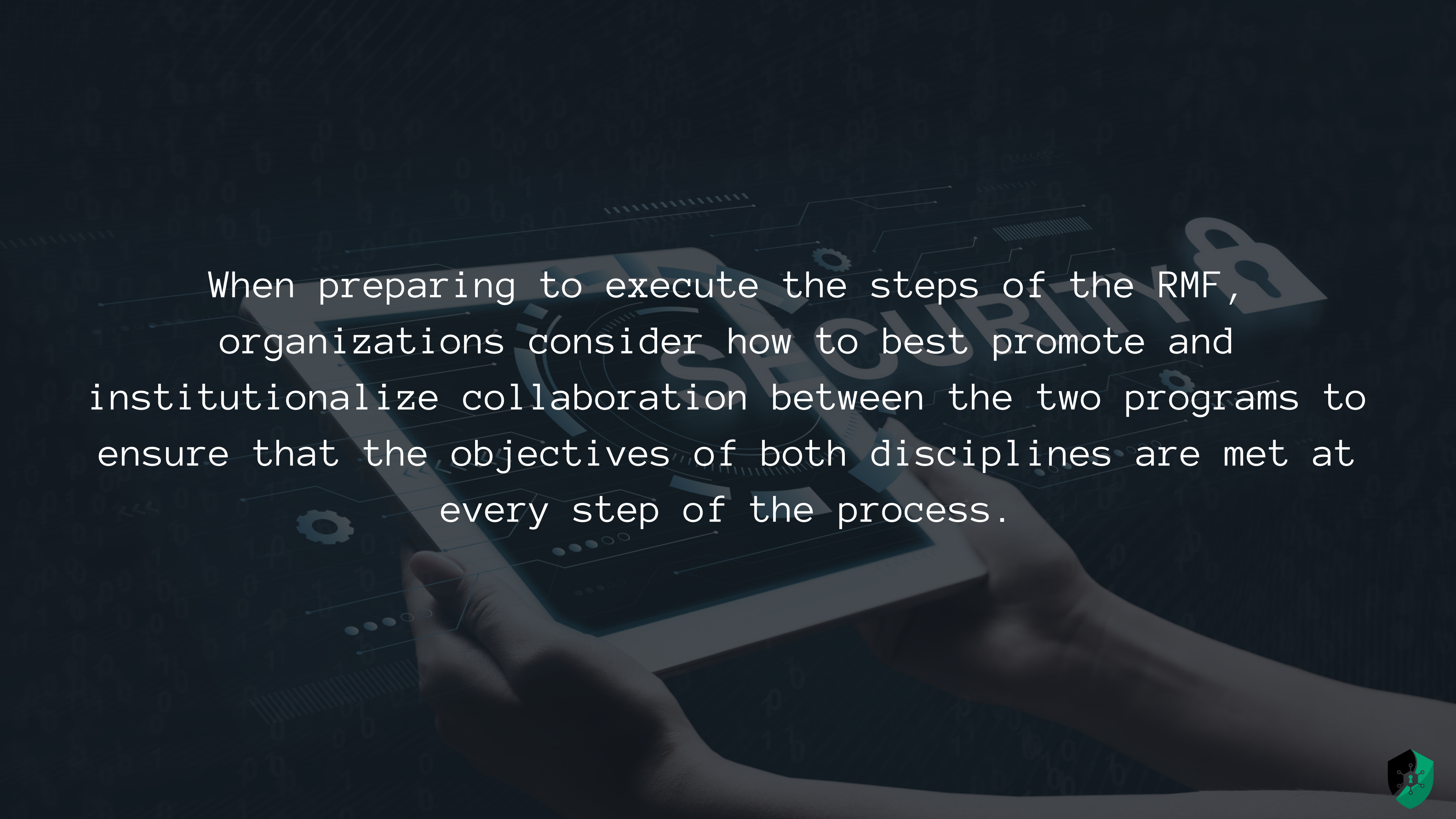


The background of the slide features a dark, moody aesthetic. A hand is visible at the bottom, holding a tablet. The tablet screen and the background are overlaid with various digital security-themed elements: a large, semi-transparent word 'SECURITY' in a bold, sans-serif font; a padlock icon; several interlocking gears; and a network of glowing blue lines and dots. Faint binary code (0s and 1s) is scattered throughout the background, creating a high-tech, digital environment.

With the latest version of RMF, Information security & privacy are now integrated together because even though they have different objectives, those objectives are overlapping and complimentary.








When preparing to execute the steps of the RMF, organizations consider how to best promote and institutionalize collaboration between the two programs to ensure that the objectives of both disciplines are met at every step of the process.







Information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction





Privacy programs are responsible for ensuring compliance with applicable privacy requirements and for managing the risks to individuals associated with the creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as “processing”) of PII





Information Security – CIA

Privacy – PII



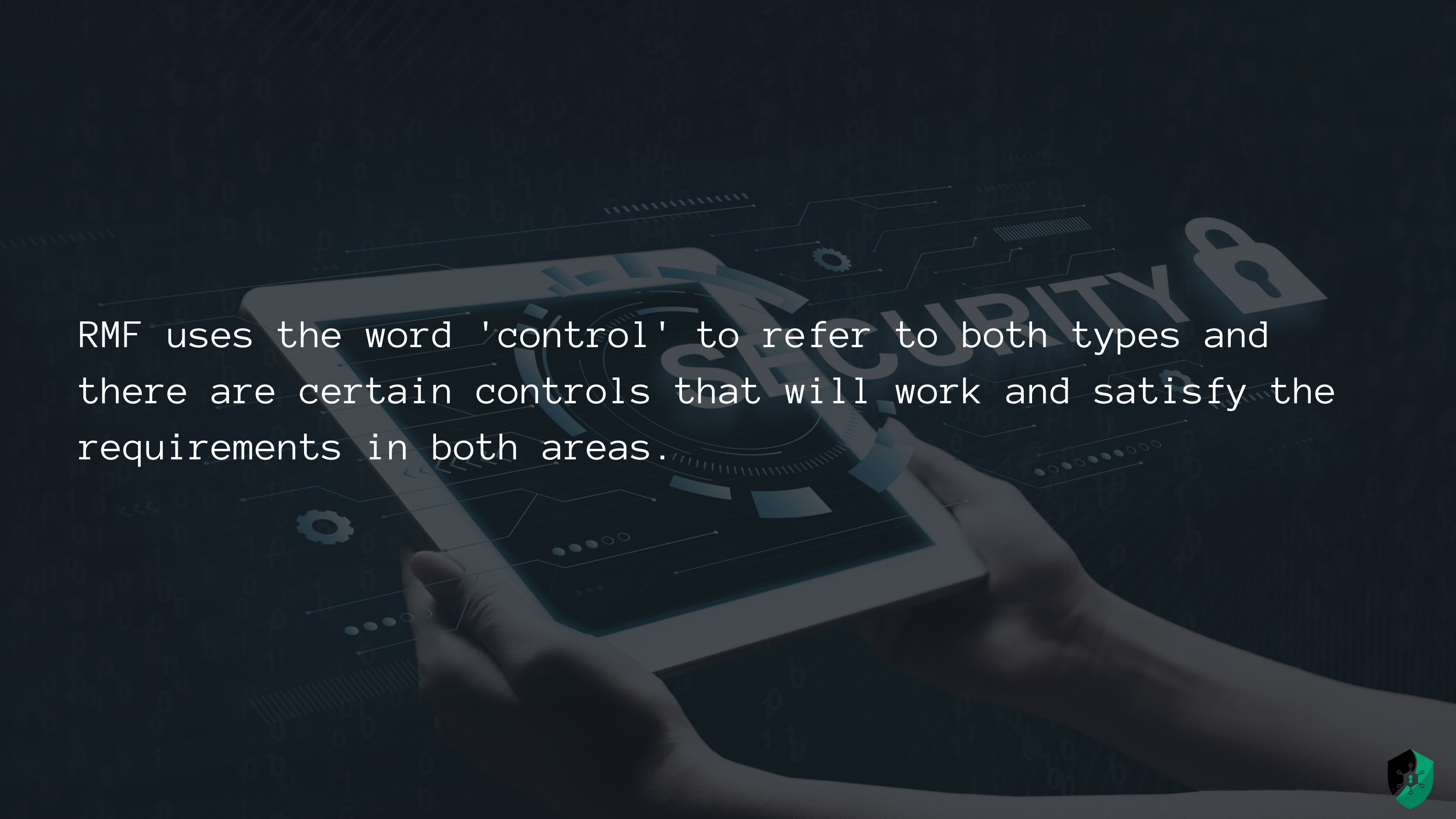


Security Control – safeguards or countermeasures prescribed for an information system to protect the CIA of the system and its information.

Privacy Control – Administrative, technical or physical safeguard that is going to be used within an organization to ensure compliance with the applicable privacy requirements and to manage privacy risks.







RMF uses the word 'control' to refer to both types and there are certain controls that will work and satisfy the requirements in both areas.

