and tolerance (such as outlined in GOVERN), organizations can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures and actions. Organizations may choose to handle risk in different ways — including mitigating, transferring, avoiding, or accepting the risks — depending on the potential impacts. Importantly, organizations can use the Framework both internally and to oversee third parties.

"may choose to handle risk in "one or more ways , not "different ways"

Creating and Using Framework Profiles to Understand, Assess, Prioritize, and Communicate
The Framework’s mechanism for describing an organization’s current or target cybersecurity posture in terms of the Core’s outcomes is called a Framework Profile (Profile). Profiles are used to understand, assess, prioritize, and tailor the sectorand technology-neutral Core outcomes (i.e., Functions, Categories, and Subcategories) based on an organization’s cybersecurity technology-neutral organization’s and leading
Organizations can create and use Profiles to utilize the full capabilities of the Framework (as discussed in Section 1). While organizations can use the Framework without Profiles, they provide the opportunity to develop a prioritized roadmap to achieve the cybersecurity outcomes of the Framework. There are many ways to use Profiles, including to:

- Compare current cybersecurity practices to sector-specific standards and regulatory requirements
- Document the Informative References (e.g., standards, guidelines, and policies) and the practices (e.g., procedures and safeguards) currently in place and planned in the future
- Set cybersecurity goals for the organization, identify gaps between current practices and the goals, and plan how to address the gaps in a cost-effective manner.

“achieve the cybersecurity outcomes of the” Profile, which is very different from “outcomes of the Framework.”

The NIST Cybersecurity Framework and the NIST Privacy Framework can be used together to collectively address cybersecurity and privacy risks, as illustrated by Fig. 8. As the right side of the Venn diagram depicts, organizations using the Cybersecurity Framework to manage cybersecurity risks can leverage the Privacy Framework Identify-P, Govern-P, Control-P, and Communicate-P Functions to identify and manage privacy risks unrelated to cybersecurity incidents, such as those described above. The Cybersecurity Framework DETECT, RESPOND, and Communicate-P Functions to address.

This is really confusing as what I think you are trying to say is that adding privacy means that Cyber-related privacy events have to be not only covered by both (extra work for both) but also should remain consistent for both frameworks.