

# NICE Webinar Series

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



The Intersection of the Privacy and Cybersecurity Workforce  
February 19, 2020

# NICE Framework Knowledge Descriptions

K0004: Knowledge of cybersecurity and privacy principles.

# Privacy Principles

- Organization for Economic Cooperation and Development (OECD)  
<http://www.oecd.org/corporate/mne/1922428.pdf>
- Office of Management and Budget Circular A-130 (2016)  
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>

# Privacy Engineering Objectives

## **Predictability**

Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service

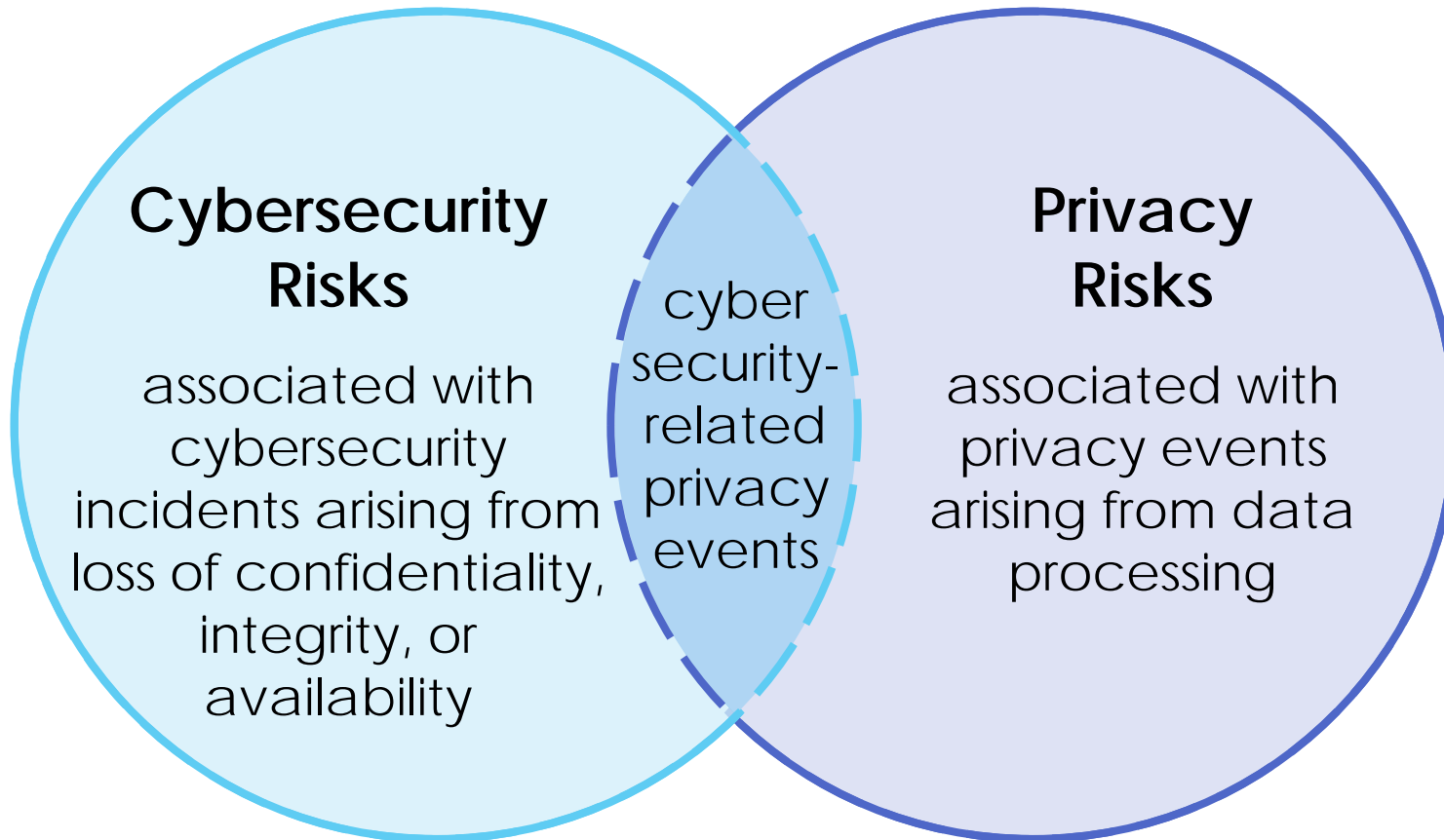
## **Manageability**

Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure

## **Disassociability**

Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

# Relationship Between Cybersecurity and Privacy Risk



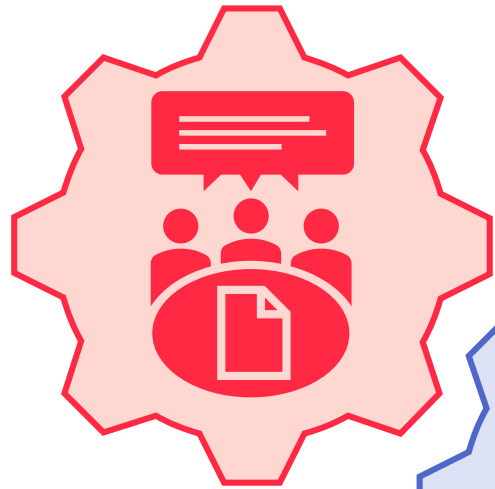
**Data:** A representation of information, including digital and non-digital formats

**Privacy Event:** The occurrence or potential occurrence of problematic data actions

**Data Processing:** The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

**Privacy Risk:** The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

# Privacy Framework Structure



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

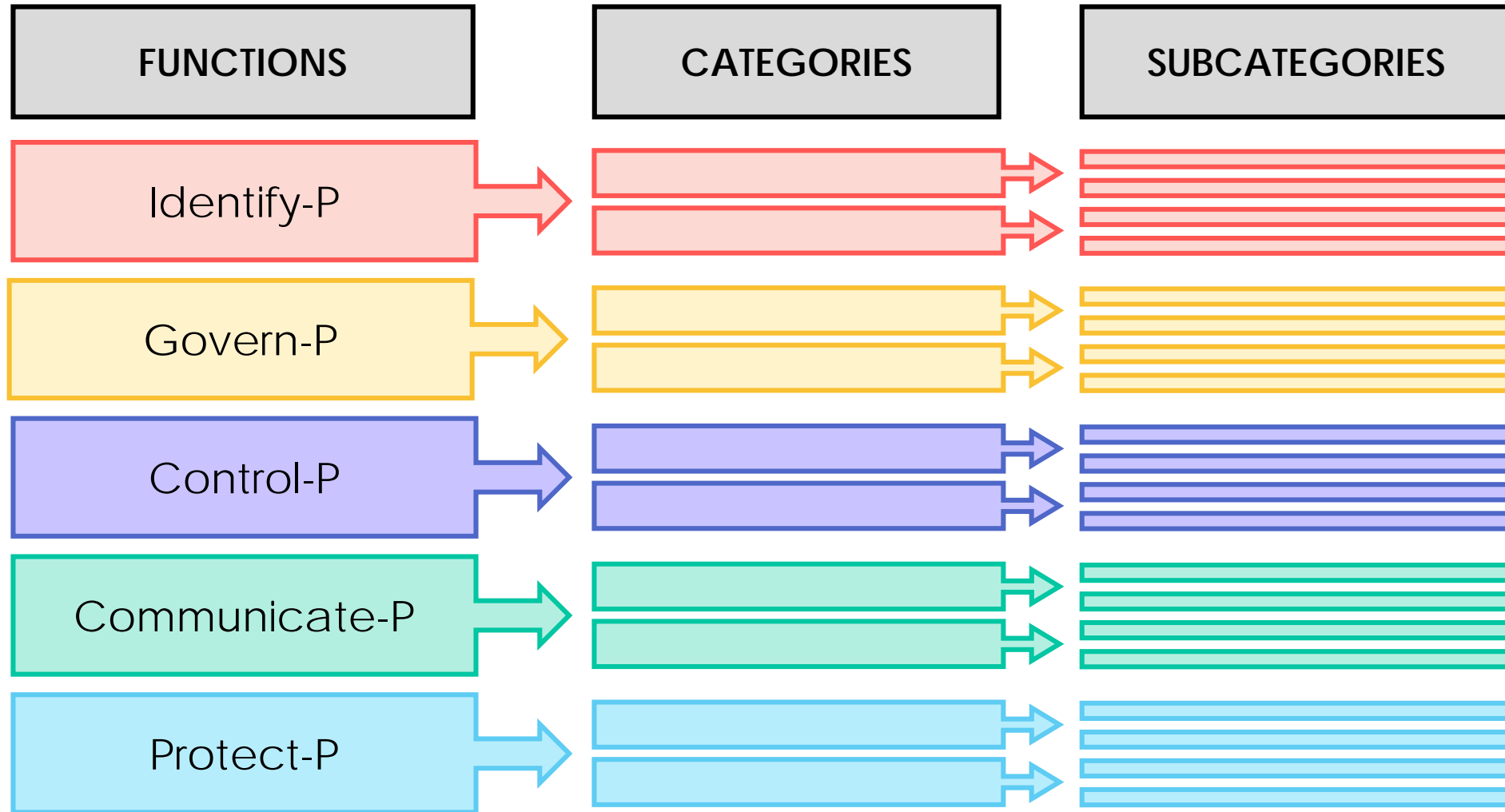


**Profiles** are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk



**Implementation Tiers** help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

# Privacy Framework Core



# Control-P Example

## FUNCTIONS

## CATEGORIES

## SUBCATEGORIES

**Control-P**

**Data Processing Management (CT.DM-P):** Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).

**CT.DM-P1:** Data elements can be accessed for review.

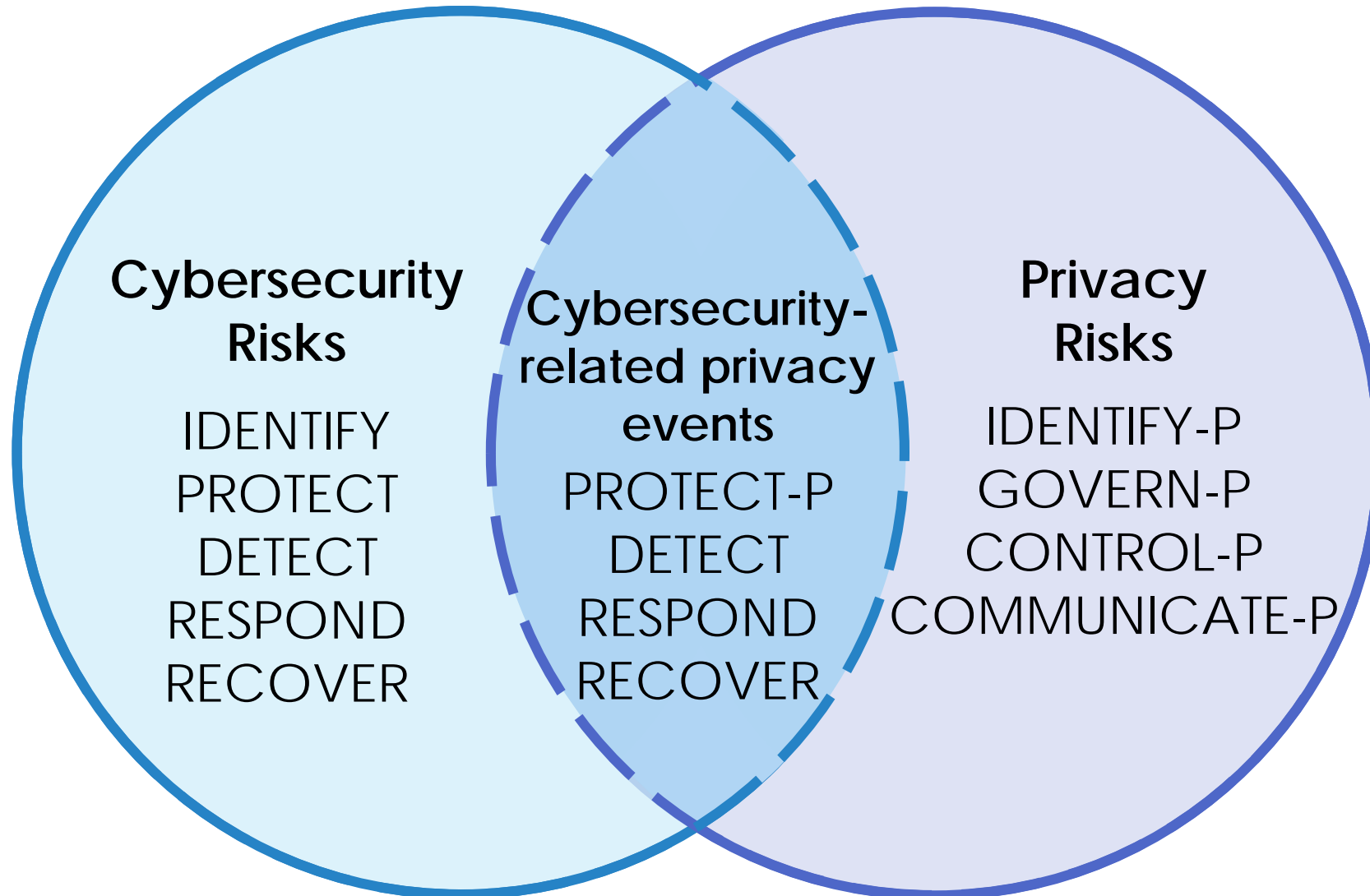
**CT.DM-P2:** Data elements can be accessed for transmission or disclosure.

**CT.DM-P3:** Data elements can be accessed for alteration.

**CT.DM-P4:** Data elements can be accessed for deletion.



# Cybersecurity Framework Alignment



# Roadmap

- Privacy Risk Assessment
- Mechanisms to Provide Confidence
- Emerging Technologies
- De-Identification Techniques and Re-identification Risks
- Inventory and Mapping
- Technical Standards
- **Privacy Workforce**
- International and Regulatory Aspects, Impacts and Alignment

# Privacy Framework Resources



## Website

<https://www.nist.gov/privacyframework>



## Mailing List

<List.nist.gov/privacyframework>



## Contact Us

PrivacyFramework@nist.gov

@NISTcyber #PrivacyFramework

# Q & A

The Mission of the  
IAPP is to Define,  
Promote and  
Improve the Privacy  
Profession Globally.

---

iapp

international association  
of privacy professionals



# Globally, the laws are becoming more stringent and enforcement is ramping up.



Increasing Cost of Breaches

- Juniper research, 8/19



# Privacy by Design

Laws *require* compliance with the principles of **Privacy by Design**.

- changes the way to plan, design, build, test and maintain applications
- Affects the way we vet and integrate Third Party Software

## 7 PRINCIPLES OF PRIVACY BY DESIGN



### PROACTIVE, NOT REACTIVE, PREVENTATIVE, NOT REMEDIAL

The Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.



### FULL FUNCTIONALITY – POSITIVE-SUM, NOT ZERO-SUM

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.



### PRIVACY AS THE DEFAULT SETTING

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.



### END-TO-END SECURITY

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.



### PRIVACY EMBEDDED INTO THE DESIGN

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.



### VISIBILITY AND TRANSPARENCY

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.



### RESPECT FOR USER PRIVACY

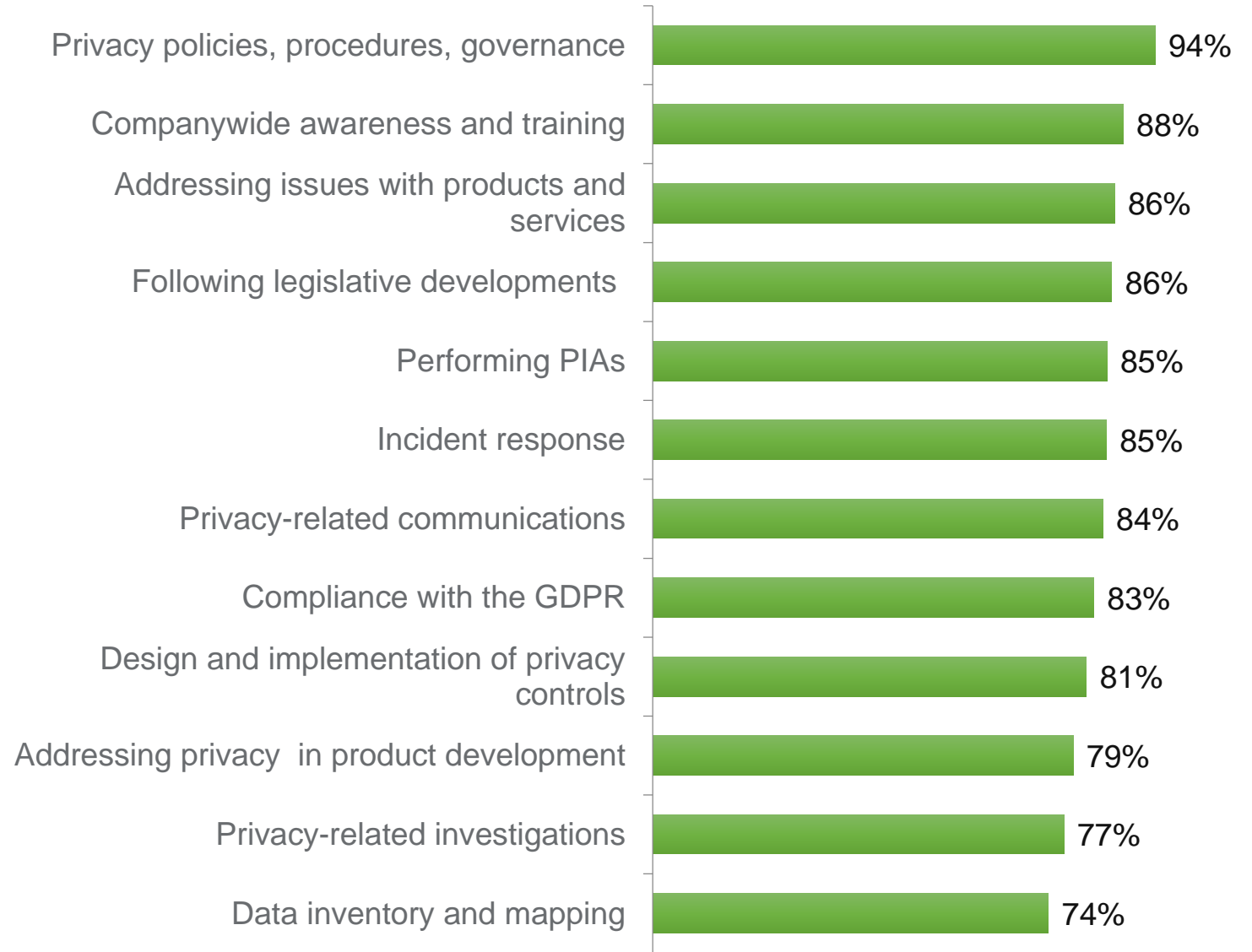
Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Helping small businesses work towards Data Protection Compliance and deliver on their Web Application Goals

[www.ServeIT.com](http://www.ServeIT.com)

# What are the overall responsibilities of privacy teams?

---





# What are the overall responsibilities of privacy teams?

---





Security is about protection and availability. It requires rules & restrictions.

Privacy is about content, context and usage. It requires **ethics** and **trust**.

**Protect-P (PR-P):**  
Develop and implement appropriate data processing safeguards.

**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.

**Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.

- Domain II. A. a. vi. & D. b. i. & ii.2-4  
Incident response  
Privacy incidents
- Legal compliance
    - Preventing harm
    - Collection limitations
    - Accountability
    - Monitoring and enforcement
  - Develop a privacy incident response plan
  - Identify elements of the privacy incident response plan
  - Integrate privacy incident response into business continuity planning
- Domain II. C. e. ii. & iv.  
Monitor
- Monitor compliance with established privacy policies
  - Compliance monitoring (e.g. collection, use and retention)
    - Internal audit
    - Self-regulation
    - Retention strategy
    - Exit strategy

- Domain II. B. b. i.  
Access controls for physical and virtual systems
- Access control on need to know
  - Account management (e.g., provision process)
  - Privilege management

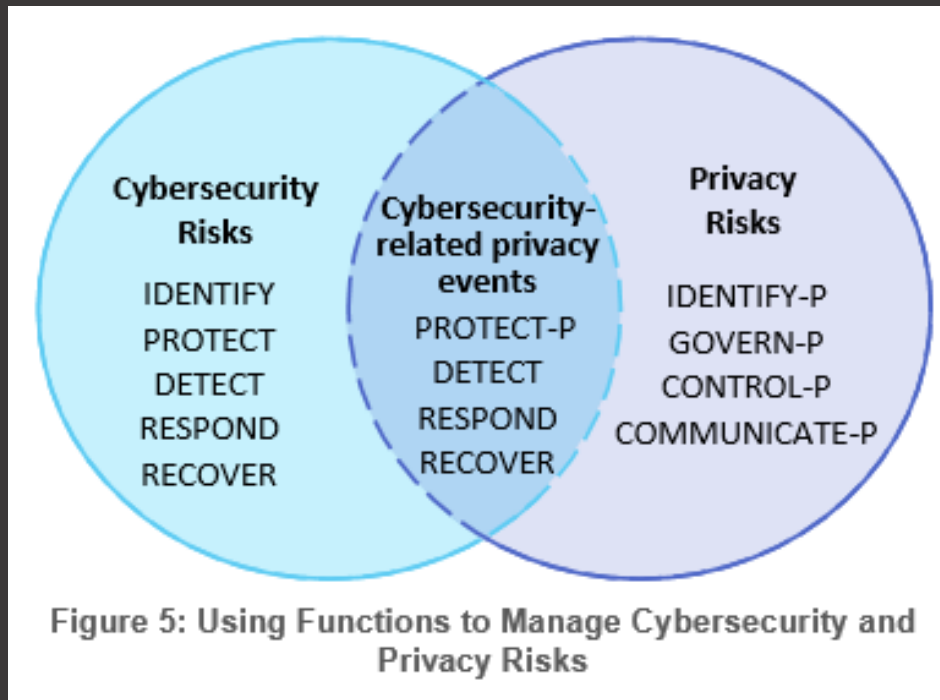


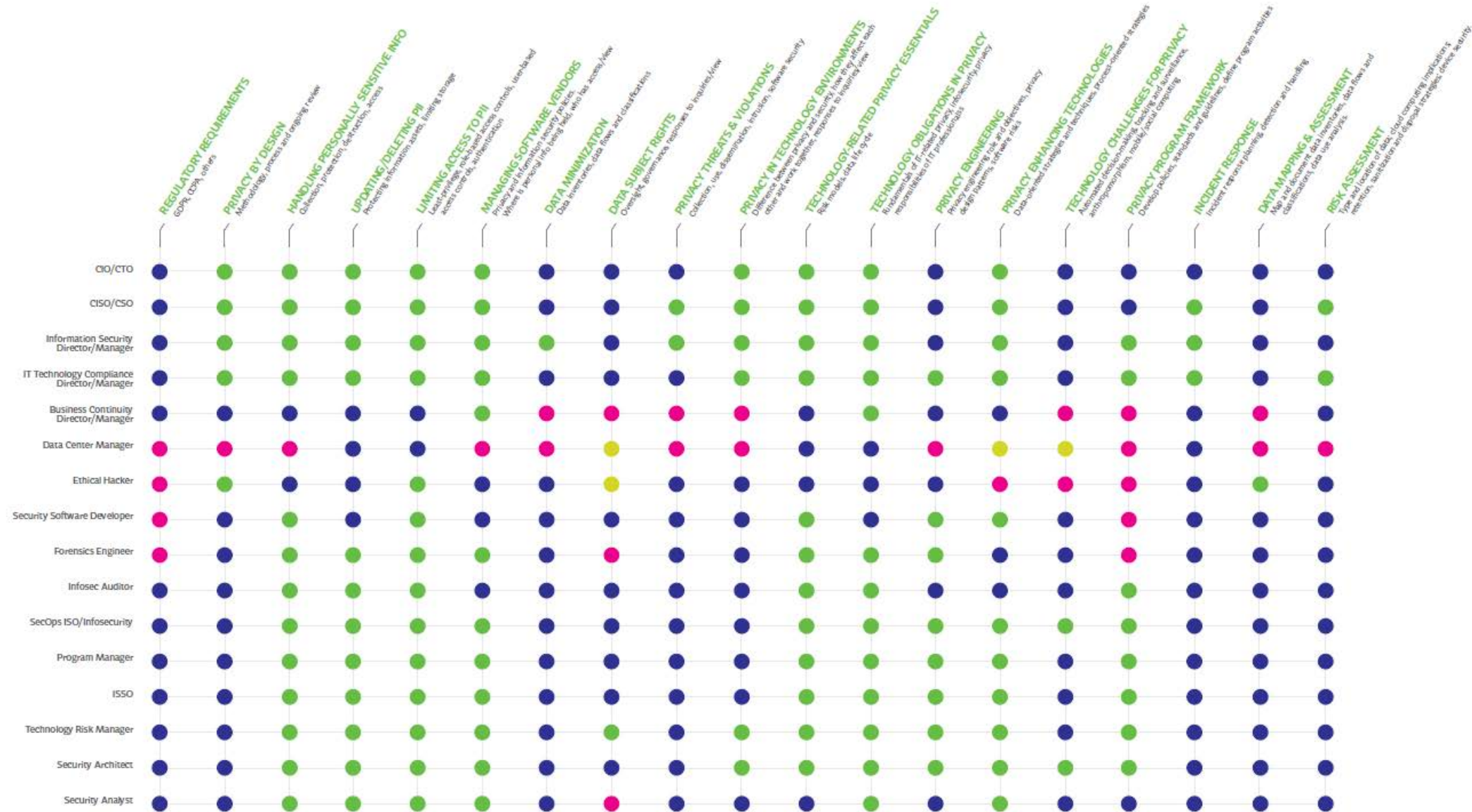
Figure 5: Using Functions to Manage Cybersecurity and Privacy Risks



# INFOSEC PROS: BUILD YOUR PRIVACY MUSCLE

<https://iapp.org/l/infosec-privacy-knowledge/>

Use this grid to assess individual and team privacy skill sets and develop a roadmap for professional development.



# INFOSEC PROFESSIONALS NEED FOR PRIVACY KNOWLEDGE

“From a business perspective, the reality is that data about us is going to drive everything we do and the way we interact with each other,” said Mark Thompson, Global Privacy Advisory Lead at KPMG | United Kingdom. “This creates a whole new kind of security landscape, which is increasingly centered around PII data risk.”

“The goal is protection,” said Pa. “Only if security and privacy functions head in the same direction, can we achieve that goal.”

“The whole idea of ‘reasonable security’ as part of a privacy program means it is now the responsibility of security teams to understand privacy. And that has been a big shift,” said Dana Simberko, Chief Risk, Privacy, and Information Security Officer at AvePoint Inc. “Privacy laws have significant consequences such as regulatory fines and breach requirements that fall squarely on the shoulders of security. So, there is really no way you can separate the two domains in theory or in practice.”



Partnership of  
Legal and Tech  
is critical!



# IAPP Privacy. Security. Risk. 2020

Training September 29-30

Workshops September 30

**Conference October 1-2**

**AUSTIN, TX**



## IAPP PRIVACY ENGINEERING SECTION

This is where privacy professionals working in the IT and privacy engineering fields come together and connect. The Privacy Engineering Section offers a range of programs, events, content and networking opportunities through which privacy pros working in IT and related fields can connect and advance.



## CALLING ALL PRIVACY ENGINEERS!

Experts in the privacy engineering field are being asked to step up and share their expertise. We're looking for speakers to address topics such as user interface design, data ethics in artificial intelligence, privacy by design, de-identification, implementation of privacy technologies and much more.

# Q & A





# The Intersection of the Privacy and Cybersecurity Workforce

NICE Webinar

Jonathan Fox

Director, Privacy Engineering

February 19 2020

*“No matter what market you’re in, no matter what service you provide or product you sell... from right now until the end of time, you’re in the privacy game. Welcome.”*

**WIRED**

**THE PRIVACY REVOLT: THE GROWING DEMAND FOR PRIVACY-AS-A-SERVICE**



Today's overlap will deepen and grow

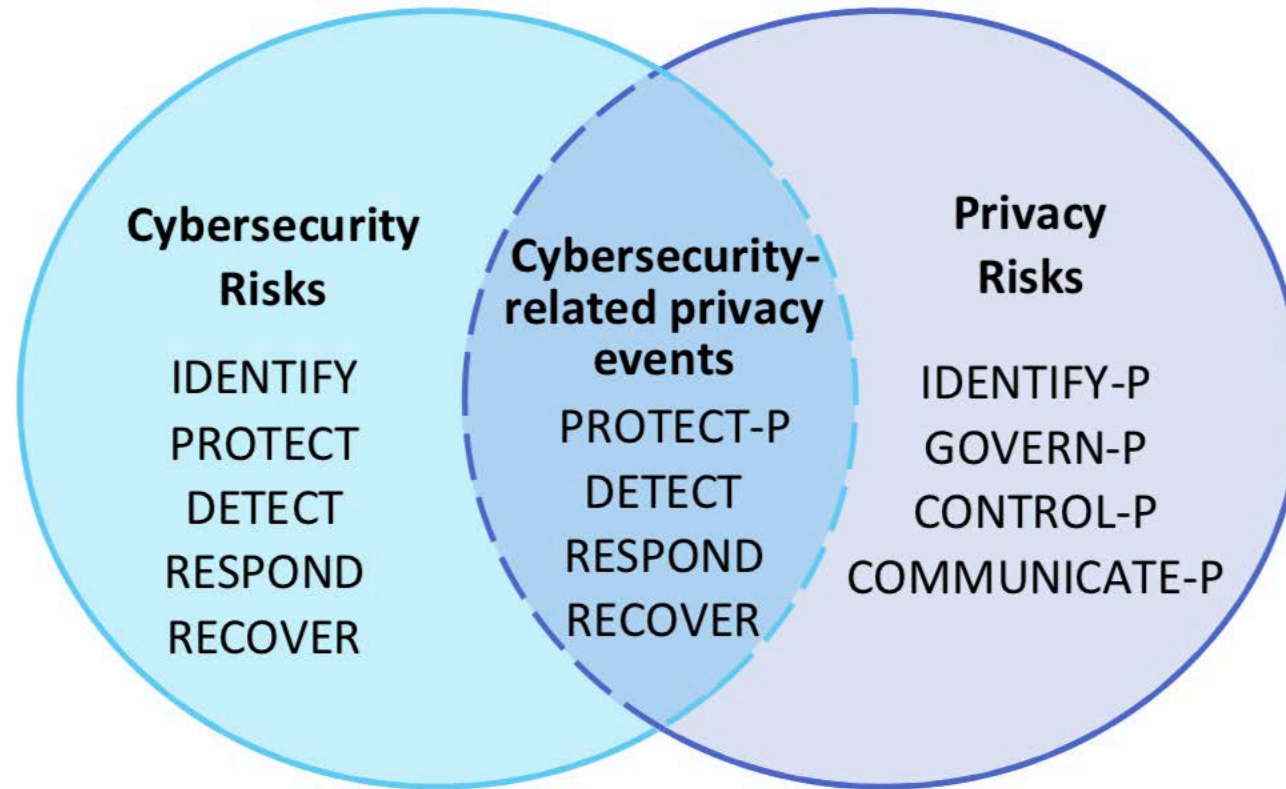
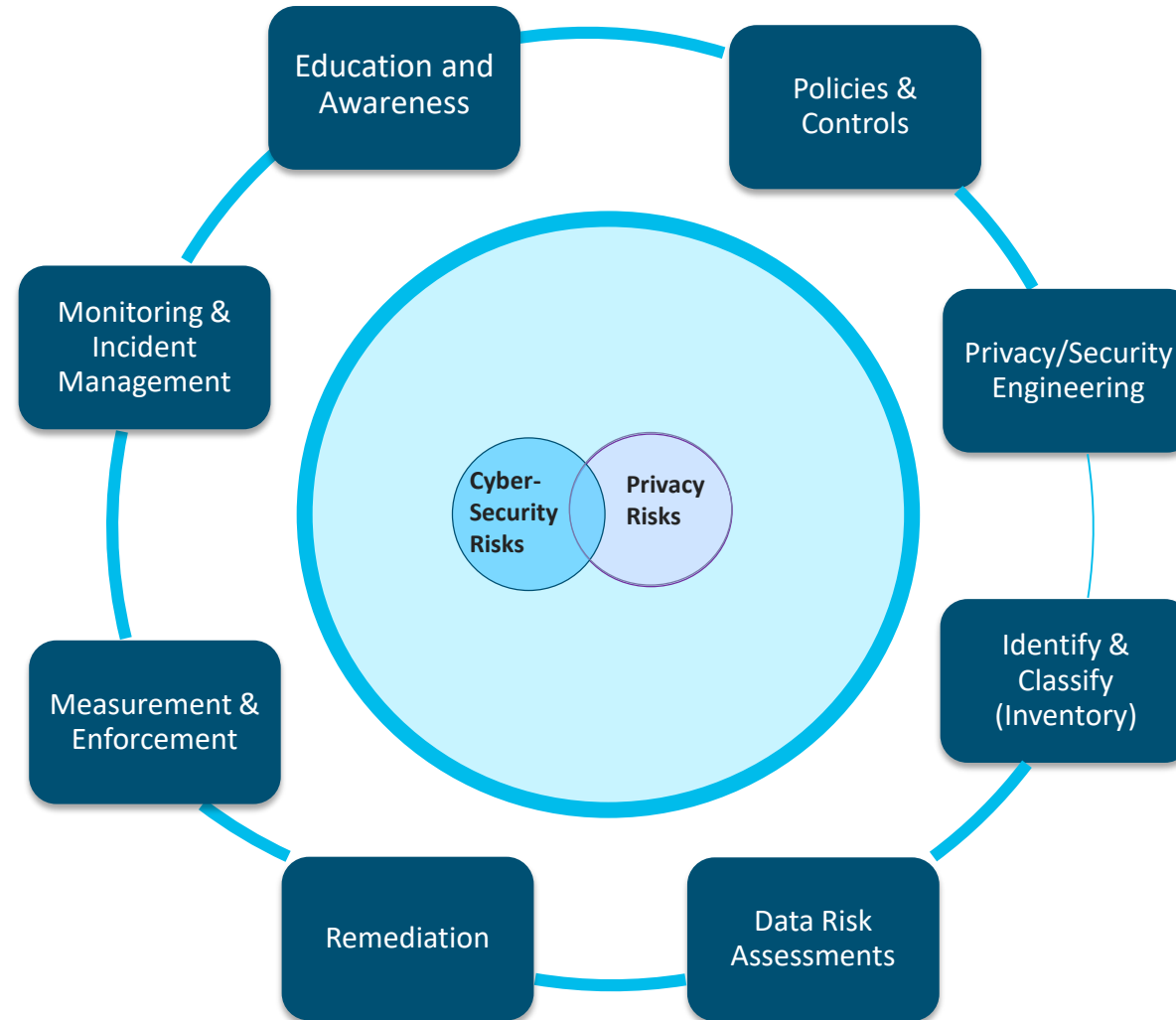


Figure 5: Using Functions to Manage Cybersecurity and Privacy Risks

# Functions in the data protection ecosystem will grow



# Increased domain expertise will be required



Marketing

Engineering

HR

M&A

IT Ops

**Privacy is contextual**

**In addition to increased standardization of privacy roles and responsibilities, we will see the continued rise of Privacy SMEs in the different business functions**

# The only constant will be change

- Data will flow
- New purposes will be imagined
- Risk will continue to need to be managed
- New roles and responsibilities will emerge



# Q & A



# Thank You for Joining Us!

**Upcoming Webinar: “NICE Framework Uses and Success Stories”**

**When: Wednesday, March 18, 2020 at 2:00pm EDT**

**Register: <https://nistnice.adobeconnect.com/webinarmar2020/event/registration.html>**

[nist.gov/nice/webinars](https://nist.gov/nice/webinars)