

A network diagram with several circular icons containing stylized human figures. These icons are interconnected by a web of thin, light-colored lines. The background is a dark teal color with a subtle pattern of these lines and icons, creating a sense of a digital or social network. The overall aesthetic is modern and tech-oriented.

# PRIVACY AS A STAKEHOLDER

HOW TO GET A SEAT AT THE TABLE

## **PRIVACY AS A STAKEHOLDER (PraaS) SUPPORTS THE OPERATIONALIZATION OF PRIVACY ACROSS THE ENTERPRISE AND ENABLES THE MISSION AND BUSINESS THROUGH A PRIVACY-BY-DESIGN METHOD.**

It helps establish connections and takes a multidisciplinary approach to managing risk across enterprise services (e.g., records management, information technology [IT] system development, big data, public relations [PR], insider threat, physical security).

Booz Allen created the PraaS service offering to help improve situational awareness across organizations, better manage enterprise-wide privacy risks, and strengthen organizations day-to-day business decisions, strategies, and program development based on our knowledge and experience supporting Privacy Offices across the Federal Government and commercial markets.

# DEFINING THE ROLE OF PraaS



***PraaS is operationalizing privacy across an organization by getting privacy a seat at the table to address risks and serve as a business enabler.***

Successfully implementing PraaS includes obtaining buy-in from your organization's senior leaders, building relationships and partnerships across your organization, demonstrating the value of privacy as a differentiator, and finding ways to get to "yes" while still protecting the organization's privacy interests.

The role of a Chief Privacy Officer, Senior Agency Official for Privacy, or Privacy Official—both in name and function—varies from organization to organization. The Privacy Official should be a senior member of the organization's leadership team with representation across the organization to ensure privacy equities are being considered from the beginning when developing business programs or making business decisions. For an organization to implement PraaS,

there needs to be a deliberate cultural shift that moves away from a reactive compliance function to the concept of embedding privacy as a risk-based proactive mission enabler.

Using an awareness campaign, this service can be appropriately socialized within an organization to elevate the concept and embed it into business operations. If organizations consider and acknowledge privacy as a key differentiator instead of an inhibitor, PraaS can become a fundamental part of the organization, serving as a value-add to programs across the enterprise. Ultimately, this will result in increase to the organization's public trust, brand and reputation, help achieve business goals and cost reductions, and reduce overall risk.

---

*If organizations consider and acknowledge privacy as a key differentiator instead of an inhibitor, PraaS can become a fundamental part of the organization, serving as a value-add to programs across the enterprise.*

THE NOTIONS OF “BAKING IN PRIVACY” OR  
“GIVING PRIVACY A SEAT AT THE TABLE”  
HAVE BEEN USED IN THEORY, BUT PraaS  
FORMALIZES THE PROCESSES BY WHICH  
A PRIVACY OFFICIAL WOULD ENGAGE IN  
MISSION AREAS AND BUSINESS SERVICES  
ACROSS AN ORGANIZATION WHERE PRIVACY  
NEEDS TO BE CONSIDERED.

# PraaS IN PRACTICE

## SCENARIO 1

***The IT Department recently procured a new IT system without consulting a Privacy Official.***

The system is associated with a public-facing web app, which collects large amounts of personally identifiable information (PII), some of which is totally unnecessary and collected without the user knowing. The system was just breached, and the users are outraged that their PII has been compromised.

### ***How PraaS would have helped:***

The Privacy Official should be engaged in every aspect and major decision point during the planning, development, and “go-live” for new IT systems. Some instances in which the Privacy Official could have helped to reduce the business impact of this scenario include:

- Proactively determining the authority and business need to collect the information
- Ensuring data minimization to only that which is relevant and necessary
- Increasing transparency around what information is collected and how

## SCENARIO 2

***An employee with your organization was arrested for armed robbery.***

Given this person’s role in your organization, the local newspaper wanted a comment about his employment status and the disciplinary actions taken. The Communications Department and Human Resources complied and issued a statement indicating that the employee has been fired and included some additional facts about his employment. A few days later, turns out the police had the wrong guy! In addition, some of the information provided by your organization was also incorrect; now your organization’s and the employee’s reputation are both damaged.

### ***How PraaS would have helped:***

During PR cleanup, engaging the Privacy Official may not seem like the first call an organization would make, but it should be one of them. In this instance, the Privacy Official would have engaged with the PR and HR teams to:

- Determine what, if any, information can be disclosed, and obtain consent and individual participation where necessary
- Ensure the quality and integrity of PII maintained by the organization
- Provide appropriate training so employees are aware of responsibilities for accessing PII and can be held accountable

## SCENARIO 3

***Your organization recently developed an Insider Threat Program; however, one of the most sensitive systems containing large volumes of client PII wasn’t included.***

Consequently, the information contained within this system has been misused by an employee who was looking to steal the information and sell to a competitor. On top of that, you’ve discovered the Insider Threat Program is misusing employee information for purposes beyond investigations. There are now various employee complaints and even a few threatening to sue!

### ***How PraaS would have helped:***

The Privacy Official is essential to engagement in any organizational Insider Threat Program. In this capacity, the Privacy Official could have helped to:

- Ensure transparency around insider threat policies and processes
- Provide appropriate notice to employees regarding the Insider Threat Program and the use of their PII, and put policies in place to ensure the use of that PII is limited to investigations
- Deliver training to ensure employees are accountable for the proper use, handling, and protection of PII

# ABOUT BOOZ ALLEN'S PaaS SOLUTION

***Booz Allen understands the importance of embedding privacy across an organization.***

We help a wide variety of organizations prepare for what's next and advise both federal and commercial organizations on how to modernize traditional privacy programs to more effectively manage and mitigate privacy risk across the enterprise. As thought leaders in next-generation privacy considerations, Booz Allen understands the complexities of the changing privacy landscape and the impact on how organizations handle PII when building new programs and services.

Our experience and expertise can help organizations develop and implement a comprehensive privacy management approach that minimizes risks while satisfying your business needs. Organizations need a strategy and

implementation plan to formalize the concept of PaaS within an organization. Implementation would have to be risk based and dependent upon resources, with fully resourced privacy programs being able to integrate more quickly across an organization and less-resourced offices would have to prioritize based on the organization's risk tolerance.

***Key components of this strategy include the following steps:***

1. **Obtain buy-in and support from senior leadership and key stakeholders** across your organization's business units with whom you would have to engage.
2. **Get to know your organization—** identify the major offices that touch/intersect with PII; what are their major projects, priorities, and key initiatives; and how can the Privacy Official support them.

3. **Determine where the biggest risks are, and start there.** This involves surveying the organization to identify high value assets and major initiatives and beginning to prioritize with counterparts within the relevant business units.
4. **Figure out where your "quick wins" lie and use them as a case study** to show value.

***Like any successful initiative, this is not a "one-and-done" thing; it's a process that requires ongoing effort.***

Maintaining continuous awareness of your organization by promoting open dialogue with key stakeholders, keeping a pulse on changes across your organization, and ensuring awareness of the PaaS role and benefits are keys to making PaaS successful at your organization.

## HOW BOOZ ALLEN CAN HELP

***Our Privacy Consulting Team comprises industry experts with experience in both the commercial sector and the Federal Government, who have built full-scale enterprise privacy programs.***

Our depth of experience allows us to bring best practices from one organization to another, while customizing the need to fit that environment. We have assisted clients with developing

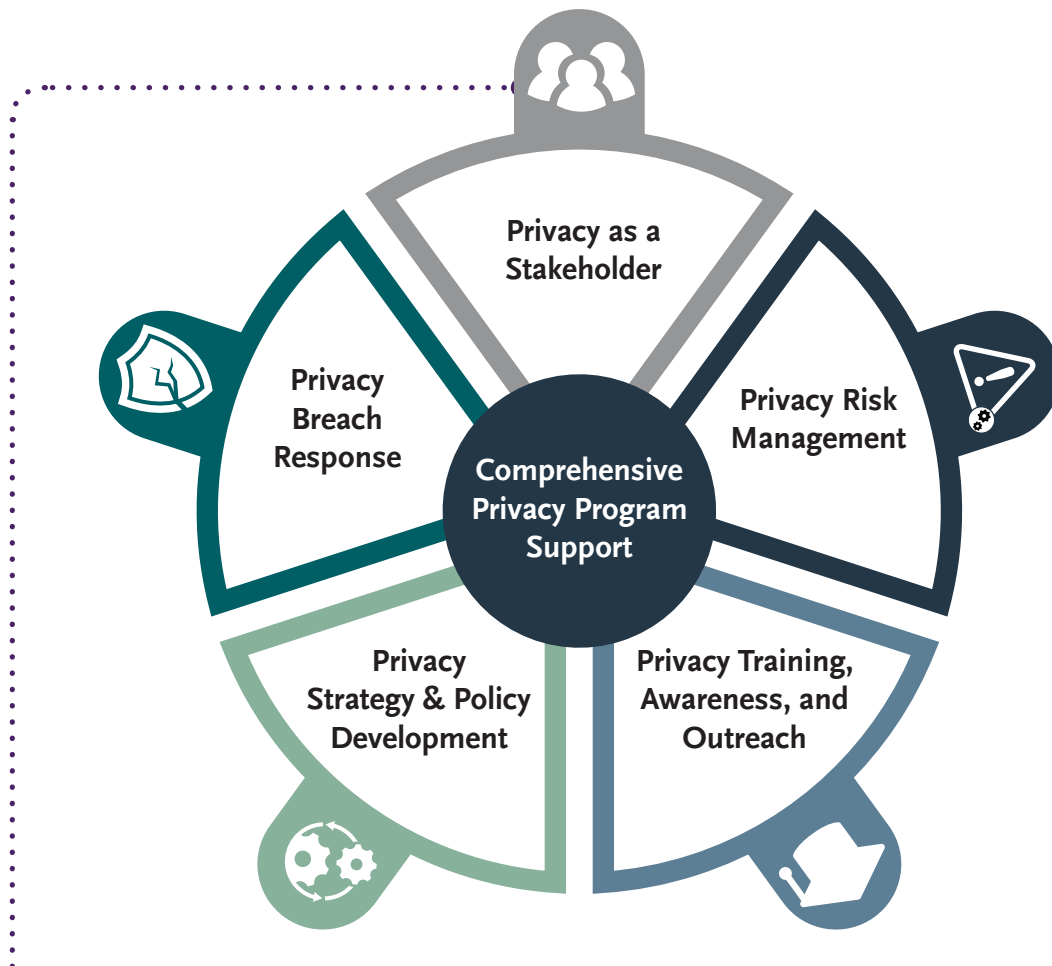
and maturing their privacy programs and worked to operationalize privacy across organizations to areas such as insider threat, records management, and IT system development.

We understand that building relationships is key and have worked with clients to demonstrate the value of considering privacy at the ground level of new projects and programs.

**We have a team of privacy experts equipped and ready to help you:**

- Develop and implement a PaaS strategy
- Create and execute an awareness campaign
- Work side-by-side with you to identify privacy risks and embed privacy across your organization

# BOOZ ALLEN'S PRIVACY SERVICE OFFERINGS



## PRIVACY AS A STAKEHOLDER OFFERINGS

- Work with Records Management to ensure records schedules exist for PII
- Assess Paperwork Reduction Act information collections for privacy risk, and develop necessary privacy notices
- Assess Big Data initiatives for privacy risks, and develop privacy guidelines
- Support the development of Insider Threat Programs to ensure privacy equities are addressed
- Integrate Privacy Continuous Monitoring processes into existing Security Continuous Monitoring programs
- Advise on Freedom of Information Act (FOIA) and Privacy Act requests to ensure proper protection of PII
- Ensure Security Operations Centers have processes and policies in place to appropriately handle PII
- Assess Physical Security processes to ensure privacy protections are in place
- Support the development of Controlled Unclassified Information (CUI) policies and programs



## About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit [BoozAllen.com](http://BoozAllen.com).

---

*For more information, please contact:*

### **LIZ TRIBELLI**

[tribelli\\_elizabeth@bah.com](mailto:tribelli_elizabeth@bah.com)

### **DIANNA CARR**

[carr\\_dianna@bah.com](mailto:carr_dianna@bah.com)