opentext™

SERVICE OVERVIEW

Privacy Capabilities Assessment Service

The Privacy Capabilities Assessment Service provides benchmarking against best practices and actionable recommendations to enable organizations to improve their privacy controls and processes that address privacy regulations.

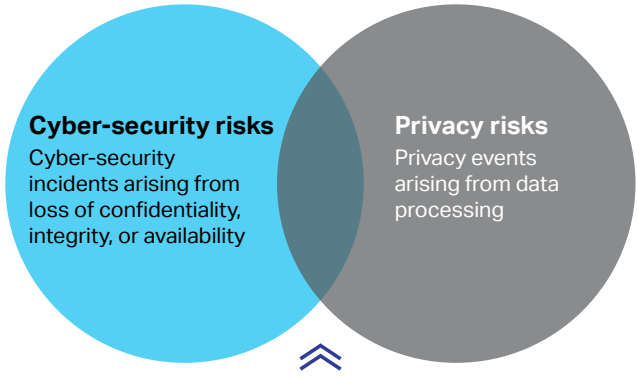
Enable Compliance Capabilities with better visibility into current controls capabilities

Maturity Benchmarking against NIST Privacy Framework Tiers

Deliver Actionable Recommendations to improve current privacy controls and reduce risk

Build Customer Trust by improving transparency and protection of individual's privacy

Evolving privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) require a transparent, risk-based approach to managing personal data. Cyber-security and privacy risks overlap, so understanding the likelihood of potential problems and impacts are key to mitigating both risk areas. Maintaining a complete picture of foundational security controls and core privacy capabilities is critical to maintaining an effective privacy program.



Cyber-security related privacy events

opentext™

The Privacy Capabilities Assessment Service benchmarks an organization's controls against the National Institute of Standards and Technology's (NIST) Privacy best practices. Through a consultative approach, the OpenText team provides an assessment of the organization's current privacy program maturity and a roadmap to improving privacy capabilities within a short time frame. The service uses a best practice methodology that utilizes a five-step approach to the privacy assessment:

Step	Approach
Initiate	Confirm expectations, and create customized approach based on environment, privacy requirements and challenges
Discover	Develop a clear understanding of the current state of processes, technology and people that support the privacy program
Analyze	Evaluate the current state privacy program control activities, identify gaps and benchmark the maturity to NIST Privacy Framework
Recommend	Communicate initial recommendations and gather business or technical requirements required to mitigate identified risks
Mitigate	Provide final report with a roadmap of recommended action plans mitigate risks

Enable Compliance Capabilities

Using the NIST Privacy Framework enhances an enterprise's overall strategy for data protection and enables organizations to adapt to an ever-changing regulatory environment. Recent compliance regulations require a risk-based approach to managing privacy risk. Having a solid understanding of capabilities and gaps from a controls and process perspective, demonstrates that the enterprise is making good-faith efforts toward compliance.

Use of the NIST Framework complements existing business and cyber-security operations to:

- Establish/improve a privacy program
- Communicate privacy requirements with stakeholders
- Assist in prioritizing improvement activities
- Enable investment decisions to address gaps
- Reduce regulatory risks
- Increase audit preparedness
- Increase customer transparency and trust

NIST Cybersecurity Framework: **Tiers**

Maturity Benchmarking

OpenText uses NIST Implementation Tiers to benchmark an organization's current privacy control profile. Experts will leverage questionnaires, interviews, workshops, and document reviews to benchmark current capabilities against up to 100 NIST best practice privacy control activities. The NIST framework leverages a common language for understanding, managing and expressing privacy risk, both internally and externally.

Actionable Recommendations

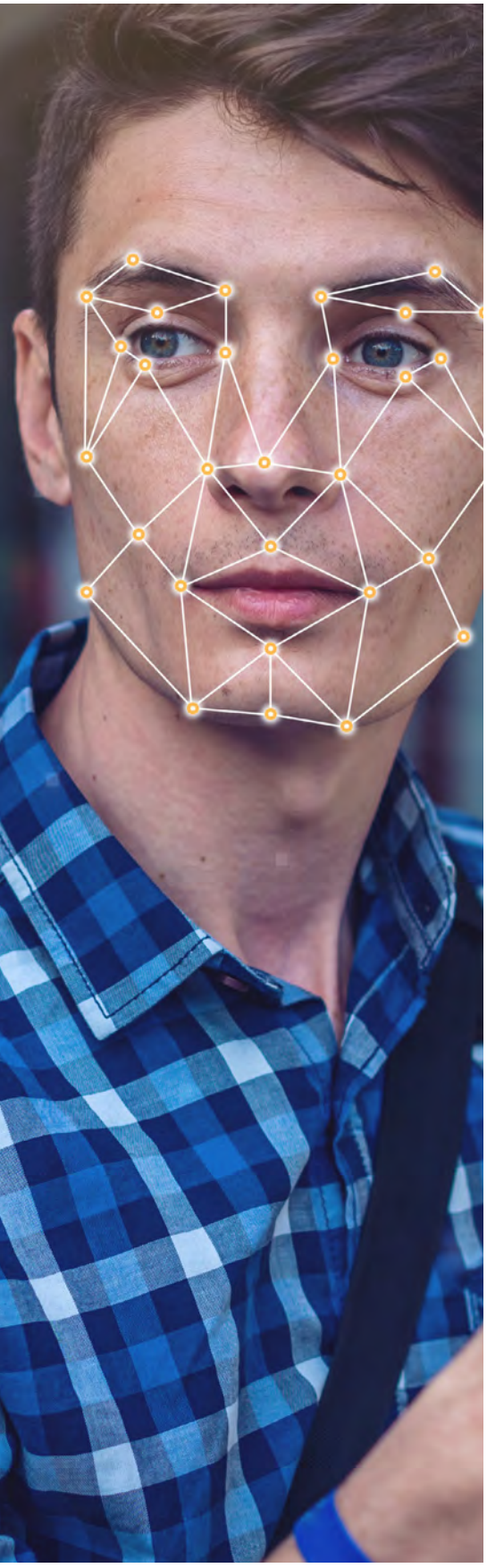
The Privacy Assessment Service's key deliverable is a security assessment report featuring an executive summary, current privacy security control maturity benchmarks and recommendations for improvement. Understanding security status is often a key input toward investment decisions to address any identified gaps. OpenText identifies and assesses the maturity of control actions and procedures.

Risk #	GAP Description	Potential Problem for Individuals	Potential Problem for Organization	Category
1	An inventory of the purposes of data actions occuring in systems in support of XXX products and services is not maintained.	Economic Loss due to identity theft	Breach	ID.IM-P4
2	Audit logs standards for systems in support of XXX products and services are not documented or implemented.	Loss of Trust	Reduced Incident Response Capabilities	CT.DM-P8
3	Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks have not been established.	Loss of Trust	Regulatory Risks	CM.PO-P1
4	Backups of data that includes personal information are not performed on a consistent basis.	Loss of Autonomy	Direct Business Costs	PR.PO-P3

Build Customer Trust

Identifying if data processing could create problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with ethical decision-making in system, product, and service design or deployment. This facilitates optimizing beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole. It also helps avoid a loss of trust that can damage an organization's reputation, result in slow adoption, or cause abandonment of products and services.

opentext™



OpenText's highly skilled team of experts uses industry best practice methodologies to bring unique value to the assessment of an organization's security and privacy posture. OpenText security consultants hold one or more industry standard certifications, including CISSP, CISA, CISM (Certified Information Systems Security Professional, Auditor or Manager, respectively) and have more than 20 years of Risk and Security consulting experience. OpenText's experts collect information from interviews and workshops, using a standard methodology, and can also validate many information points using OpenText-provided analysis tools.

OpenText also offers additional services to address Cyber-Security and Privacy objectives:

- **Data Classification Services**—Leveraging OpenText's AI/ML capabilities to ensure personal data risks are managed effectively.
- **Security and Incident Response Training**—Curated table-top exercises and Security Awareness Workshops to reinforce cyber security best practices.
- **Incident Response Documentation Review**—Analysis of the adequacy and completeness of incident response policy or procedure documentation against best practice (NIST 800-61 rev.2)
- **Threat Hunting Services**—Integrates the best in breed technologies with custom workflows, leveraging machine learning and the MITRE ATT&CK framework to quickly find patterns, relationships and indicators of compromise.

To talk to a Security Services expert, about the Privacy Capabilities Assessment Service or our additional services, please contact **securityservices@opentext.com**

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: **opentext.com**.

Connect with us:

- **OpenText CEO Mark Barrenechea's blog**
- **Twitter** | **LinkedIn**

opentext.com/contact

Copyright © 2021 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information • (11.06.21)18391.EN