

Privacy Program Frameworks

i4Series


April 2019

Disclaimer

The views and opinions expressed in this presentation are solely my own in my individual capacity, and do not reflect the opinions, policies, or positions of my employer or any affiliated organizations or agencies.



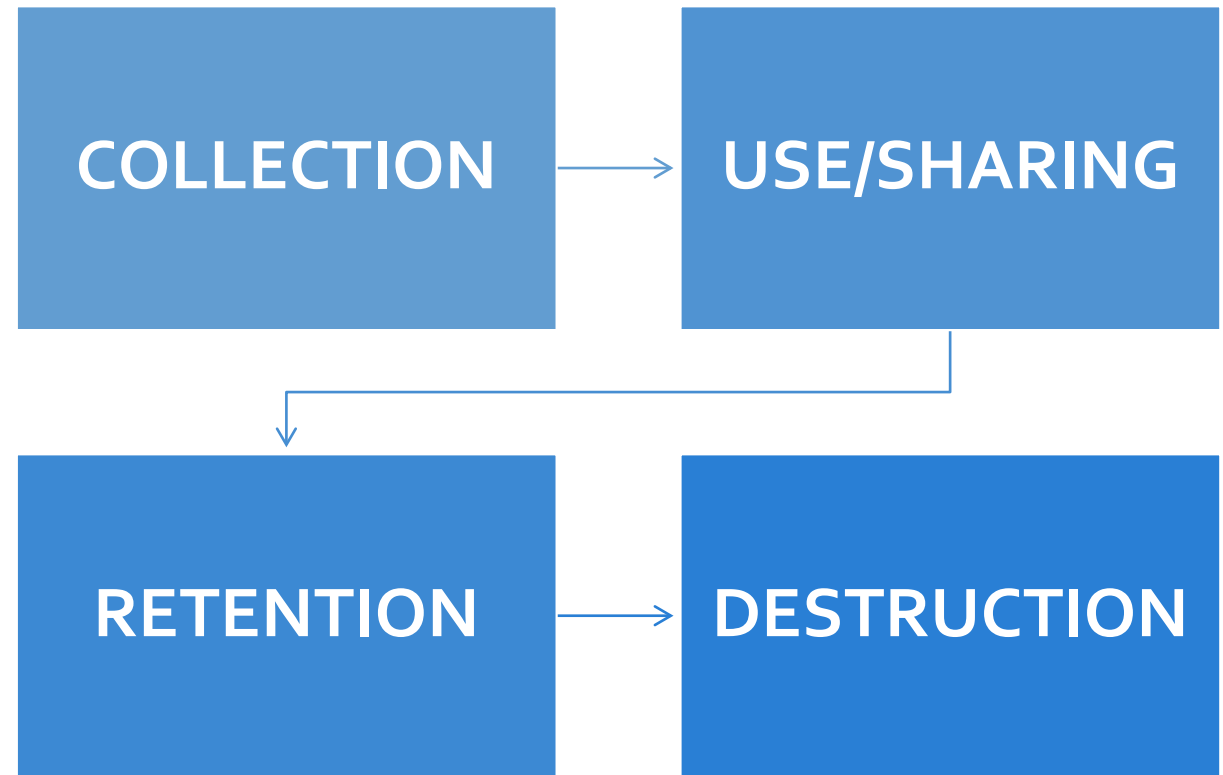
Information privacy



Information privacy

- Information self-determination.
- Empowering individuals by giving them notice and choices about how their information will be collected, used, shared, and stored.
- One size does *not* fit all.

Data has a life
of its own.



Seek balance
between
individual rights
and the
provision of
products or
services.



Legal requirements and consumer expectations are constantly evolving.

CULTURE
TECHNOLOGY
RISK TOLERANCE
SOCIAL NORMS



Privacy program frameworks



Fair Information Practice Principles (FIPPs)

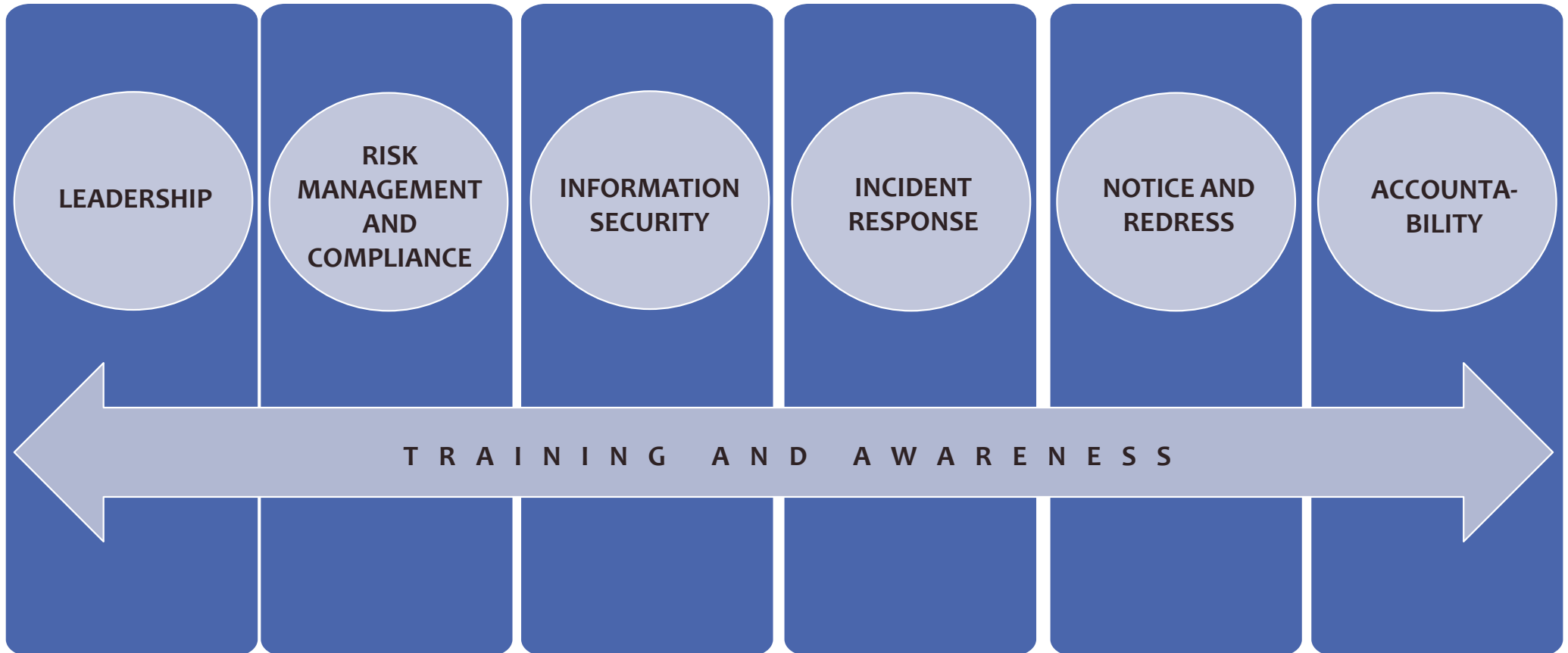
- Transparency
- Individual participation and redress
- Purpose specification
- Data minimization and retention
- Use limitation
- Data quality and integrity
- Security
- Accountability and auditing

Existing corporate compliance program components

- Written policies and procedures
- Designation of an accountable official or governance committee
- Education and training
- Audits and evaluations to monitor compliance
- Disciplinary mechanisms
- Processes and procedures to report complaints
- Investigation and remediation of systemic problems

Based on U.S. Sentencing Commission Guidelines
<https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8#NaN>

Elements of a privacy program



Source: Best Practices: Elements of a Federal Privacy Program, version 1.0, sponsored by the Federal Chief Information Officer Council Privacy Committee, June 2010


Industry standards

- National Institute of Standards and Technology
<https://www.nist.gov/>
 - Special publication 800-53, rev 5
 - Special publication 800-37, rev 2




Demonstrating privacy integration





Make it clear
that leadership
is on board.

- Designation of a privacy official.
- Policies and procedures reflective of privacy posture.
- Use of FIPPS to guide decision making.
- Resource commitment.



Get to know your data.

- Documented data locations and assignment of ownership.
- Identification of regulatory requirements.
- Enforcement of data retention and destruction policies.



Train your workforce.

- Go beyond annual training.
- Have a role based focus.
- Talk about incident reporting.

Conduct
privacy impact
assessments.

- Data intake
- Business processes
- Technologies
- Data sharing
- Data storage

Build in-house
expertise.

International Association of Privacy
Professionals

<https://iapp.org/>

Privacy professional certifications

- Privacy law
 - U.S. (private sector)
 - Asia
 - Canada
 - Europe
- Privacy program management
- Privacy technology



Resources

Resources

Federal Trade Commission – Business Center
<https://www.ftc.gov/tips-advice/business-center>

- Selected web pages
 - Privacy and security
 - Selected industries
 - Protecting small businesses
 - Legal resources (rulings)

Resources

Society of Corporate Compliance and Ethics
<https://www.corporatecompliance.org/>

Health Care Compliance Association
<https://hcca-info.org>

Theodora L. Wills
Chief Privacy Officer and
Director, Enterprise Privacy Office
The State of South Carolina
Department of Administration
Office of Technology and Information Services

Enterprise Privacy Office website:
<https://admin.sc.gov/technology/enterprise-privacy>