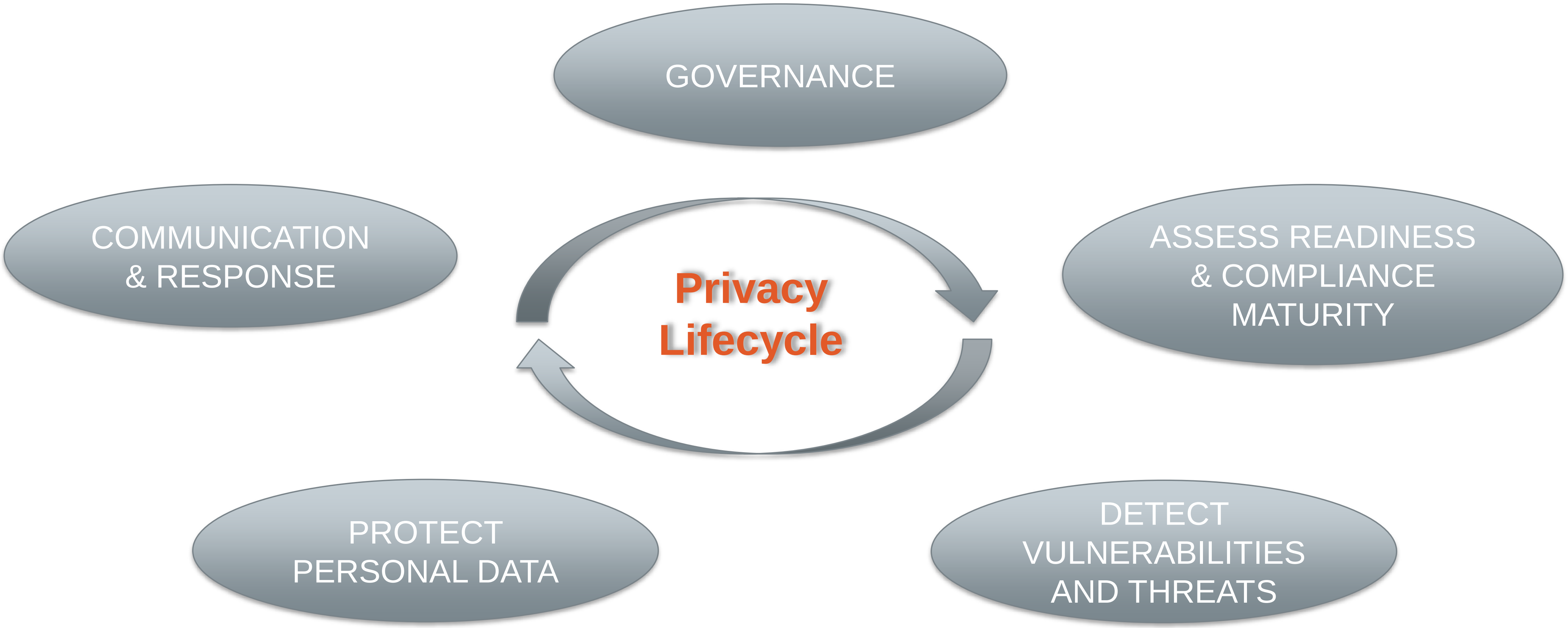
RECOMMENDATIONS FOR THE NIST PRIVACY FRAMEWORK

Mali Yared

February, 2019

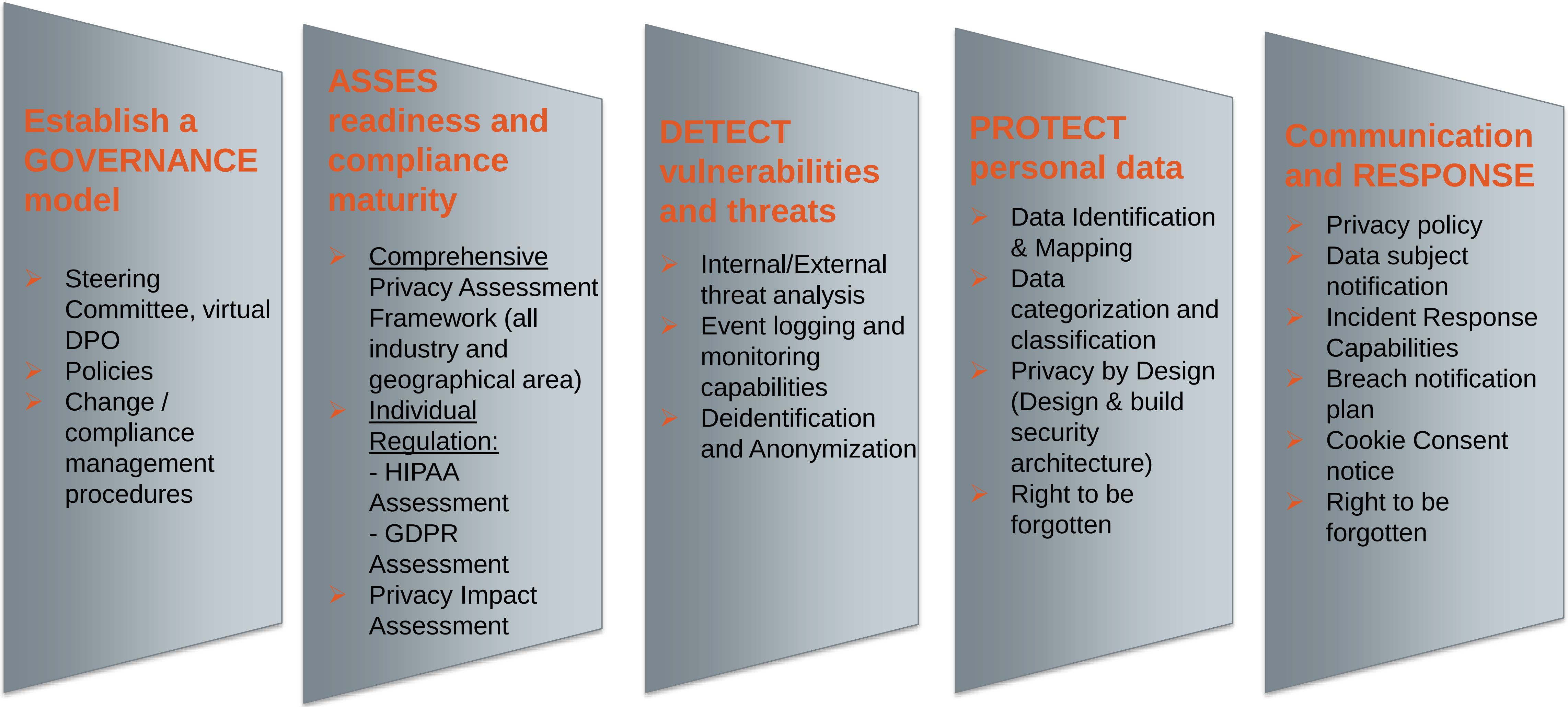
PRIVACY FRAMEWORK FUNCTIONS

Privacy or personal data protection regulations are spread across many industries, market segments, and geographical locations. Privacy Lifecycle can be broken down into 5 functions that closely mirrors the NIST CSF.


GOVERNANCE
COMMUNICATION & RESPONSE
Privacy Lifecycle
ASSESS READINESS & COMPLIANCE MATURITY
PROTECT PERSONAL DATA
DETECT VULNERABILITIES AND THREATS

PRIVACY FUNCTIONS BROKEN BY CATEGORIES

Privacy’s 5 functions can be further broken down into categories that explore areas in cybersecurity, legal and compliance, governance, and IT. Some categories are represented in the chevron’s below (these are only high level and can be further refined)



Establish a GOVERNANCE model

- Steering Committee, virtual DPO
- Policies
- Change / compliance management procedures

ASSES readiness and compliance maturity

- Comprehensive Privacy Assessment Framework (all industry and geographical area)
- Individual Regulation:
  - HIPAA Assessment
  - GDPR Assessment
- Privacy Impact Assessment

DETECT vulnerabilities and threats

- Internal/External threat analysis
- Event logging and monitoring capabilities
- Deidentification and Anonymization

PROTECT personal data

- Data Identification & Mapping
- Data categorization and classification
- Privacy by Design (Design & build security architecture)
- Right to be forgotten

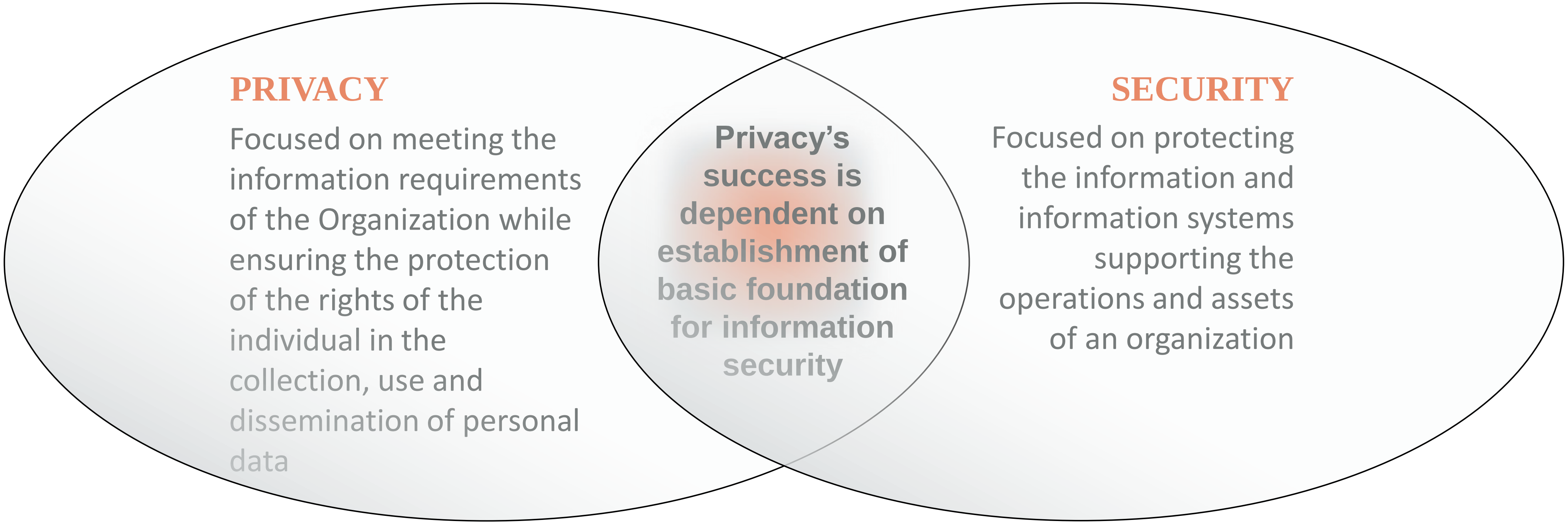
Communication and RESPONSE

- Privacy policy
- Data subject notification
- Incident Response Capabilities
- Breach notification plan
- Cookie Consent notice
- Right to be forgotten

PRIVACY & SECURITY OVERLAP

Cybersecurity firms are interested in Privacy as there are overlapping points of interest

- The requirements in Privacy, can be closely aligned with those in most of the current Cybersecurity frameworks.
- The protection measures used for cyber security can be directly, or with minor adjustment be applied to Privacy requirements



PRIVACY

Focused on meeting the information requirements of the Organization while ensuring the protection of the rights of the individual in the collection, use and dissemination of personal data

Privacy's success is dependent on establishment of basic foundation for information security

SECURITY

Focused on protecting the information and information systems supporting the operations and assets of an organization