Activities and evidence of practices needed to satisfy ISO/IEC 27559

Legend: must do (black), do or justify (grey)

Context

Threat modeling

Map data flow & uses
- Assess security & privacy
- Threat of attack
- Mitigation controls

Transparency & impact

Assess impact of use, sharing
- Collection & use
- Harms
- PIAs & oversight

X

Data

Data features

Classify attributes
- Background available to adversary
- Vulnerable groups
- Dataset properties

Attack modelling

Select privacy model
- Attacks & metrics
- Context of use, sharing
- Demonstration or honest but curious

=

Identifiability

Measure identifiability

Combine context & data
- Disclosure scenarios
- Objective methods & benchmarks
- Adversarial testing

Mitigate identifiability

Re-evaluate after mitigation
- Data environment
- Tailored to use case
- Minimization or accepted methods

De-identification Governance

Integrate into info governance
- Org structures, roles & responsibilities
- Policies, procedures
- Disclosures defined, categorized

Monitor & mitigate
- Response: contain, manage, report
- Robust audit trail
- Crisis management, review

Determine responsibilities
- Internal function → Controller
- Trusted third party → Controller or processor (shared)
- External threat assessment → Processor

Activities and evidence of practices needed to satisfy ISO/IEC 27559

Explaining the main components

Context	x	Data	=	Identifiability
The context in which data is shared and used will influence the chance of a vulnerability being exploited. For this we need an assessment of privacy and security controls, as well as motives, involving checklists or reviews of where the data will be used. Being transparent and explaining practices to partners, people represented in the data, and the public, in language they can understand, will set expectations for privacy. Various aspects will also determine potential impact of disclosure, informing risk tolerance.		The goal is to produce useful data while protecting the privacy of people. Understanding the features of the data and how they may be exploited is used to evaluate potential vulnerabilities. Example: data and attribute types, dataset properties. Potential attacks and metrics are used for attack modeling specific to threats from the context of data sharing and use. There can be people targeted in the data or data that will be used to identify targets. Technical privacy models will quantify identifiability.		An attack on the data is conditional on the context in which it will be shared and used. This is simplified as context times data is equal to a measure of identifiability. A threshold is used on the measure of identifiability to determine how safe it is. To meet appropriate safety thresholds, changes can be made to the context in which data is shared and used, and in the data that is included. This means improving privacy and security controls where the data will be used, and minimizing what data is provided.

De-identification Governance

De-identification governance, as a specialized area, differs from general data governance. Integrating into enterprise information governance can ensure consistency and application for all related activities.

Monitoring changes to the environment in which data is used, with a robust audit trail, provides the ability to respond in case of need. There is always the possibility of a major incident that requires immediate action.

Who is accountable for data sharing and use, and who is responsible for de-identification governance, will depend on the division of activities between the custodian and the activities of de-identification.