Unit 4 Seminar Activity 1: Review of NIST Privacy Tools and Alignment with Unit 3 Risk Assessment Methods

The National Institute of Standards and Technology (NIST) provides a suite of privacy engineering tools that support structured identification, analysis, and mitigation of privacy risks across the system lifecycle. Two core instruments underpin this approach:

**1. NIST Privacy Framework (PF) v1.0 (2020)**
A voluntary, enterprise risk–based structure composed of five functions—**Identify, Govern, Control, Communicate and Protect**—used to operationalise privacy risk management across organisational and technical processes. It is intentionally modelled on the NIST Cybersecurity Framework, enabling integrated adoption within existing SDLC governance structures.

**2. NISTIR 8062: Privacy Engineering and Risk Management (2017)**
This foundational publication introduces the **Privacy Risk Model**, which defines privacy risk as a function of:

- **Problematic Data Actions** (e.g., over-collection, inappropriate use),
- **Likelihood**, and
- **Impact** on individuals' rights and freedoms.

It also presents engineer-oriented methods, such as data action mapping, risk analysis tables and control alignment, forming the methodological basis for PRAM (the NIST Privacy Risk Assessment Methodology).

---

Alignment with Unit 3 Risk Methods and the SDLC

**Structured Risk Identification (ISO 31000 alignment).**
The PF's *Identify* function mirrors ISO 31000's focus on contextualisation of risk

sources. Within the SDLC, this supports **Requirements Engineering**, where data flows, actors, and processing purposes are defined to avoid privacy hazards early.

**Categorisation and Control Mapping (NIST RMF alignment).**
NISTIR 8062's data-action and control catalogues parallel the NIST RMF's control families (e.g., Access Control, Audit and Accountability). This supports the **Design** phase by embedding privacy-by-design controls such as data minimisation, purpose limitation and de-identification.

**Semi-quantitative Scoring (Risk Matrices from the Lecturecast).**
The Privacy Risk Model's likelihood–impact scoring aligns with classic SDLC risk matrices. During **Testing**, high-severity data flows (e.g., sensitive categories) trigger re-evaluation similar to OCTAVE or RMF continuous monitoring.

**Lifecycle-based Monitoring (Iterative SDLC).**
Both PF and NISTIR 8062 emphasise ongoing risk review—aligning with **Maintenance** phases in agile SDLCs, where evolving system behaviour requires repeated privacy audits in line with accountability obligations under GDPR-like regulations.

---

## Conclusion

NIST's privacy tools strengthen the risk assessment approaches from Unit 3 by adding formalised, engineering-oriented methods for evaluating privacy-specific risks. They support SDLC decision-making through structured identification, quantitative scoring and lifecycle-based monitoring. In a user-facing system, NISTIR 8062 can map problematic data actions to SDLC phase gates, ensuring that privacy risks are mitigated as systems evolve.

---

## References

NIST (2020) *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management Version 1.0*. National Institute of Standards and Technology. Available at: https://www.nist.gov/privacy-framework.

NIST (2017) *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems*. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.