Information Risk Governance Committee (IRGC) Scope

Information Security
Protection of all information and information infrastructure

Information Privacy
Appropriate protection, use, and dissemination of information about individuals

Autonomy Privacy
The ability of individuals to conduct activities without observation

Balancing Process managing conflicting information risk priorities

In Scope for IRGC

Governance Risk Register
List of missing policies needed to adequately manage risk. Prioritization based on impact on Management Risk Register.

- What data about online activities may be collected and used by the institution to guard against cyber threats?
- Who at the Campus is allowed to approve exceptions to campus privacy and security standards?
- Who is responsible for enforcing privacy and security standards?
- Should there be a sanctions policy for mishandling of data or neglect of privacy or security responsibilities?
- Should high-risk positions have periodic, mandatory privacy and security training?

Out of Scope for IRGC

Management Risk Register
List of information risks where policy defines proper treatment of risk. Prioritization by traditional risk formulas (cost of impact times likelihood of realization, offset by cost of mitigation).

- Controls required to protect information and IT resources
- Minimum requirements for disaster recovery/business continuity for IT systems
- Systems/units most severely out of compliance with minimum security standards for information and IT resources
- Terms and Conditions inserted into contracts to provide equivalent security and privacy protections for partners and off-premise services.
- Approval process for non-routine access without consent to electronic communications
Information Risk Governance Committee (IRGC) Framework

(1) For a given issue: Succinct statement of problem, stakes, case for prioritization

(2) Input
Frame the issue:
- a) Scope
- b) Policy and Practice
- c) Key questions

Explore the issue:
- Expert testimony
- Benchmark data
- Supporting-committee (CISPC) analysis

(3) Review input

(4) Decide on principles to answer key questions

(5) Decide on campus approval path aka “routing slip”

(6) Endorse initial draft of policy

(7) “Route” policy through approval path

(8) Decide: approval path is complete and policy finished

(9) Output

I. Accounting of principles responding to key questions

II. Accounting of approvals and campus consensus

III. Final policy approval and referral to appropriate management

Stakeholder groups per routing slip:
- Deans
- VCs
- Academic Senate
- etc.

Final IRGC Decision