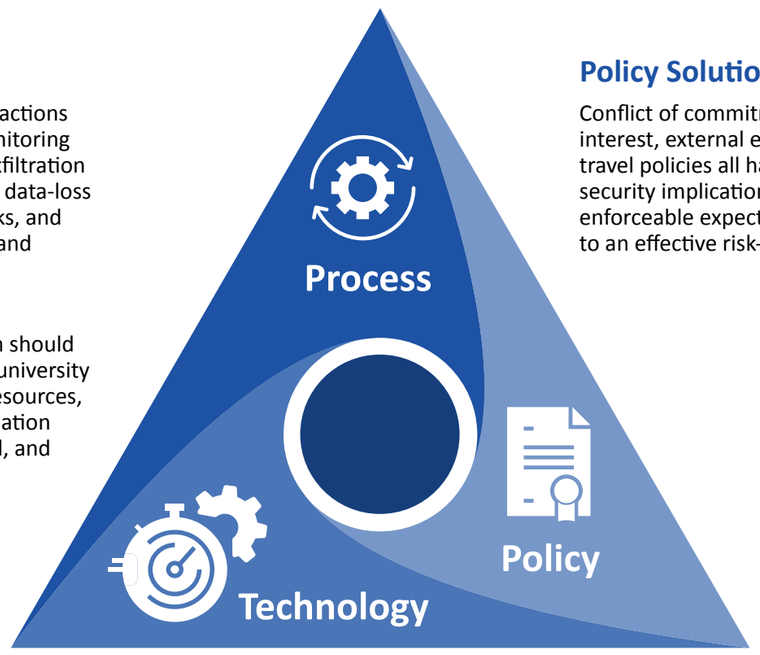
KEY STEPS IN BUILDING AN EFFECTIVE GLOBAL ENGAGEMENT PROGRAM

What Forms Can Countermeasures Take?

Process Solutions

Process solutions include such actions as vetting visiting scholars, monitoring computer networks for illicit exfiltration of research data, incorporating data-loss prevention systems on networks, and establishing risk-management and reporting frameworks.

Processes for securing research should be integrated into all facets of university operations, including human resources, training and awareness, information technology, international travel, and business administration.



Policy Solutions

Conflict of commitment, financial conflict of interest, external employment, and international travel policies all have important research security implications. Establishing clear, enforceable expectations in these areas is critical to an effective risk-management program.

Technology Solutions

Incorporating technical solutions into your risk-management process, such as secure computing enclaves that meet federal requirements, can provide a solid foundation for securing data while minimizing the burden on researchers.

1

Inventory your processes, policies, and technology solutions. Each plays a critical role in a successful Global Engagement Risk Assessment and Management Program.

2

Implement the Operational Security (OPSEC) process as the foundation for your Global Engagement Risk Assessment and Management Program.

The Operational Security (OPSEC) Process

A Simple Process to Structure Your Thinking

1. Identify Assets

Identify your sensitive data, including your research, intellectual property, export control information, and employee information. This will be the data you will need to focus your efforts on protecting.

2. Identify Threats

Identify what kinds of threats are present for each category of information that you deem sensitive. While you should be wary of third parties trying to steal your information, you should also watch out for insider threats.

3. Analzye Gaps

Analyze security gaps and other vulnerabilities. Assess your current safeguards to determine what, if any, weaknesses exist that might be exploited to gain access to your sensitive data.

4. Analyze Risk

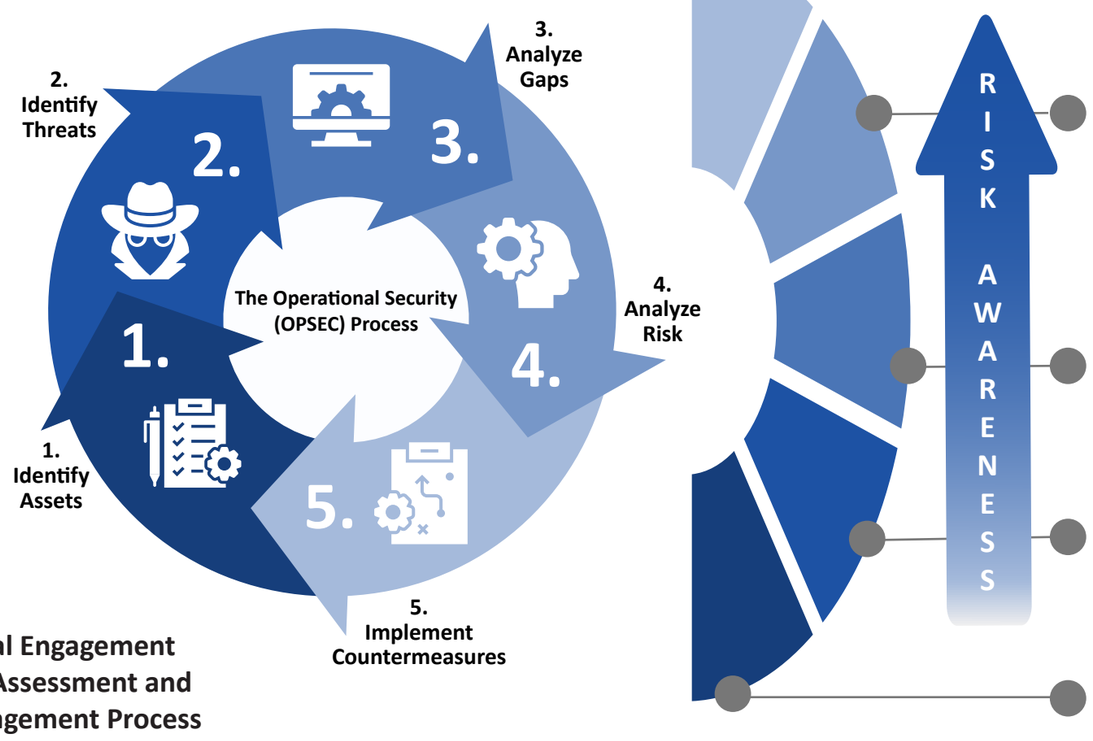
Rank vulnerabilities using factors such as the likelihood of data exfiltration, the extent of damage you would suffer, and the amount of work and time you would need to recover. You should prioritize mitigating the most likely risks.

5. Implement Countermeasures

Create and implement a plan to reduce threats and mitigate risks. Countermeasures should be simple and straightforward.

Global Engagement Maturity Model

The Research Security Capabilities Maturity Model provides an objective methodology for assessing an organization's overall security program.



Global Engagement Risk Assessment and Management Process

Level 5: Integration
Organizations operating at Level 5 have processes that are automated, documented, and constantly analyzed for optimization. Research security has been integrated into all aspects of organizational culture.

Level 4: Managed
The organization begins to measure, refine, and adapt its security processes to make them more effective and efficient based on the information it receives from its program.

Level 3: Implementation
Processes have become formal, standardized, and defined. This process maturation creates consistency across the organization.

Level 2: Repeatable Processes
Some processes become repeatable at this stage of maturity. A formal program has begun, although discipline is lacking. Some processes have been established, defined, and documented.

Level 1: Implementation
At this level, organized processes are not yet in place. Ad hoc and informal security processes are reactive and not repeatable, measurable, or scalable.

3

Use the Global Engagement Maturity Model to grow your program from initial capability to a fully integrated program.