MITRE | Insider Threat Research & Solutions™

Position Risk Designation Tool

Lightweight, Systematic Methodology to Designate Role-Specific Security Risk

What is the PRDT?

MITRE has developed a lightweight methodology for government and industry Insider Risk Programs to systematically, more objectively, and efficiently categorize which *roles* in an organization are inherently riskier than others. The “Position Risk Designation Tool” (PRDT) is a tailored tool and process which identifies the security risk associated with a specific role, not an individual (i.e., not the individual in the role, but the role itself).

The PRDT designates a risk level for a role based on objective criteria and information about the role including the role’s accesses, responsibilities, authorities, and autonomy, as well as determining the degree of damage such risks could pose to an organization and its’ strategic mission. The lightweight review of a role’s accesses and responsibilities could result in the role being deemed “high risk”, “moderate risk”, or “low risk”. By assigning a risk level for a role, the organization can implement focused mitigations for only the highest risk roles, reducing security burden for moderate or low risk roles. Examples of focused mitigations for high risk roles include: enhanced education and awareness, additional checks-and-balances and approvals for specific actions, reduced thresholds for security alerts and User Activity Monitoring alerts, and enhanced controls not in place for low or moderate risk roles.

What Types of Accesses and Responsibilities Does the PRDT Review?

An organization’s employees and contractors have a wide range of accesses, responsibilities, authorities, and autonomy, many of which are not obvious to those outside the role or are rarely collated. The PRDT is designed to focus on a broad range of accesses and responsibilities, rather than cyber-centric approaches that narrowly focus on privileged user accounts. The types of accesses and responsibilities include:

Processes & Procedures

Money & Funding

Intellectual Property & Inventions

Equipment

Computer Systems (Internal & External)

Materials, Substances, Supplies, & Chemicals

Sensitive Populations

Designs

Contracts & Legal Agreements

Methods, Knowledge, & Know-how

Data & Information

Facilities

Point of Contact: Dr. Deanna D. Caputo, Chief Scientist for Insider Threat Research & Solutions (dcaputo@mitre.org)

MITRE | Insider Threat Research & Solutions™

Website: https://insiderthreat.mitre.org

The view, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation. This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004.

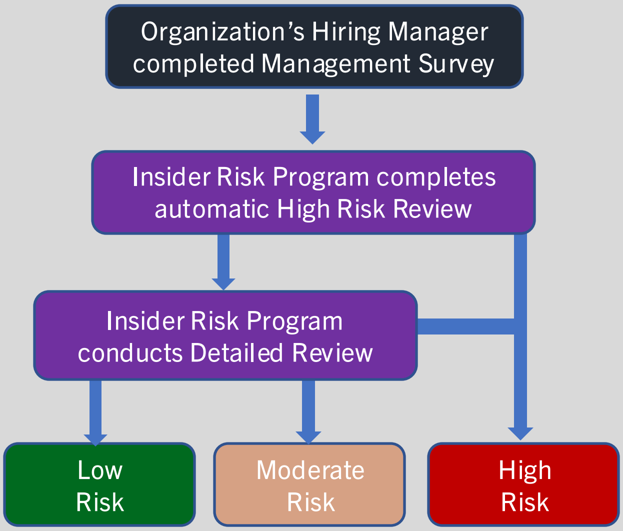
Position Risk Designation Tool

Lightweight, Systematic Methodology to Designate Role-Specific Security Risk

How is the PRDT Used?

By using the PRDT, an Insider Risk Program or other security program receives key information from the manager about a role's accesses, authorities, responsibilities, and autonomy. When a new role is created, or the accesses and responsibilities of an existing role significantly change, a relevant group (e.g., Human Resources) provides the hiring manager with a Management Survey which asks multiple-choice questions about the role. The PRDT is not needed for normal personnel changes (e.g., promotion, retirement, resignation, hiring).

Once the Management Survey is complete, which should take no more than 10 minutes, it is returned to the Insider Risk Program alongside the role's job description. Security then reviews the role's accesses, authorities, responsibilities, and autonomy against the PRDT's consistent set of criteria. The review is completed in two stages.


Organization's Hiring Manager completed Management Survey
Insider Risk Program completes automatic High Risk Review
Insider Risk Program conducts Detailed Review
Low Risk
Moderate Risk
High Risk

Overview of PRDT Process

First, the Insider Risk Program completes a swift, automatic high risk review which determines whether the role has any accesses and responsibilities that automatically designate it as "high risk". If it does, the role will be designated as high risk without spending any more time and effort. If it does not, the Insider Risk Program will complete a more detailed review based on information from the job description and the Management Survey. The detailed review involves progressively working through criteria in a simple spreadsheet tool which calculates whether the role should be designated "low risk", "moderate risk", or "high risk". There are several criteria used to make the determination. Example criteria include "rulemaking, policy, and major program responsibility (includes regulation or policy making, directing, implementing, advising and audits)" and "multi-organization impact (vs. single organization impact)".

How is the PRDT Built and Tailored for an Organization?

Before an organization can use the PRDT, the criteria used to designate a risk level must be tailored to the organization's strategic goals/mission and environment. The tailoring occurs through a series of facilitated focus groups where key organizational leaders (e.g., from business units, HR, legal, information security) discuss accesses, authorities, responsibilities, and autonomy in context of potential harm to the organization's strategic goals. By combining and analyzing information across the leadership focus groups, key terms and criteria are operationalized for each of the high, medium, and low risk levels.

How Does the PRDT Help Organizations?

- Prioritize insider risk program and security resources
- Focus education, awareness, behavior change, and outreach efforts
- Implement enhanced checks-and-balances and/or controls for higher risk roles
- Continue to dispel misconception that insider risk management "targets" and "profiles"
- Demonstrate objectivity in security risk mitigation processes to key stakeholders (e.g., HR, Legal)

Point of Contact: Dr. Deanna D. Caputo, Chief Scientist for Insider Threat Research & Solutions (dcaputo@mitre.org)

MITRE | Insider Threat Research & Solutions™

Website: https://insiderthreat.mitre.org