VENDOR GOVERNANCE AND SOURCING
CONTRACT MANAGEMENT
PROJECT TYPE: NEW HIRE
INDUSTRY: CONSULTING
ENTITY TYPE: FIRM

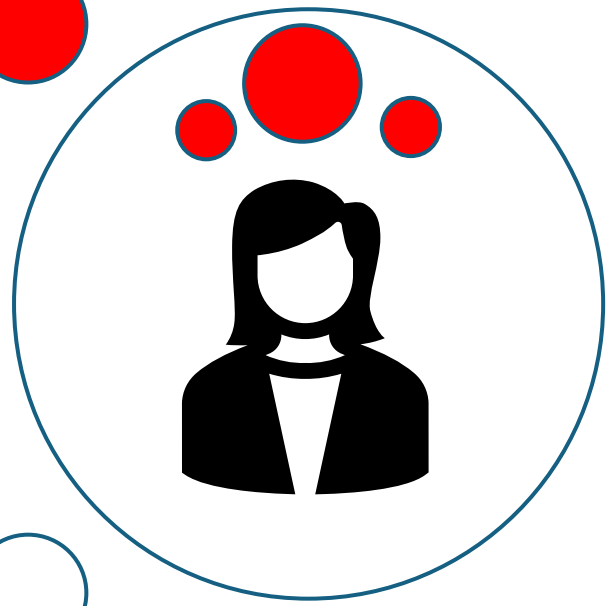
	Clear	Move to next step.
	Stop	Vendor risk pattern detected.

RISK TOLERANCE PATTERN

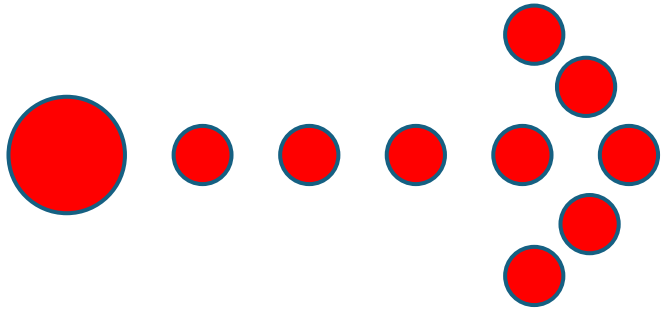
Project A: Corporation

Project B: Firm

Project C: Government



NEW HIRE / PROJECT



A visual representation of how Vendor Risk Assessment (VTR)) may appear to an Experienced Professional (EP).

KNOWN RISKS

SUPPLIER / VENDOR RISK PATTERN RECOGNITION

- ✓ ***Clear and Convincing.*** Clear and convincing evidence of Hacker activity surrounding the contract review, negotiation, and redlining function. Heightened activity in consulting roles, positions, and functions, with numerous reports of consulting firms hiring Independent Consultants and Experienced Professionals (EPs) with certain backgrounds to fulfill these roles.

- ✓ ***Known Targets.*** As a consequence of this activity and business plans, EPs are being singled out and targeted for real time hacking activity, including real time surreptitious recording and monitoring.

- ✓ ***Variances and Gaps.*** Hacker activity fueled by extreme variances (gaps) between: (1) the posted job description; and (2) the expected deliverables and output for the role. Evidence that Hackers find such gaps to be valuable for intelligence gathering purposes.

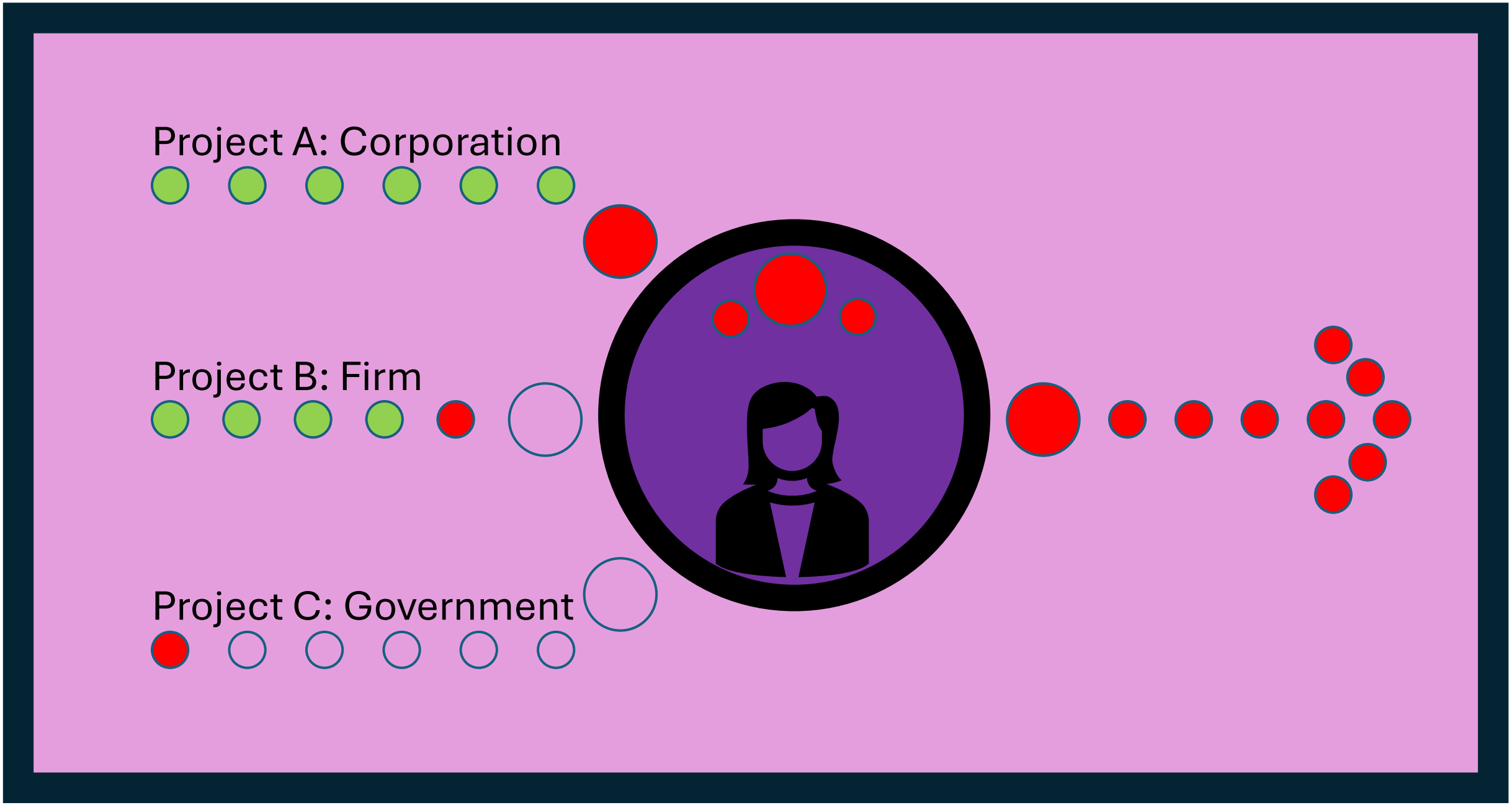
- ✓ ***Intelligence Gathering.*** Evidence that Hackers, in search of intelligence, typically at the request of, or on behalf of a Client, engage in a range activities to target EPs. Hackers generally offer highly-customizable options, allowing Clients to select from a menu of options, including the ability to request results based on the Target's industry, role, department, background, experience, areas of expertise.

- ✓ ***Legal & Enforcement.*** In fulfilling certain Hacking requests, evidence that Hackers routinely extract all available data and information, observing no boundaries, limits, or legalities. This, in turn, results in Hackers routinely extracting data and information that is: secret, classified, privileged, confidential, or proprietary.

- ✓ ***Proof.*** Proof of surreptitious recording, with Hackers exploiting gaps between: (1) the EP's knowledge, background, and experience; and (2) the project's particular specifications.

- ✓ ***Consequence.*** Experienced Professionals are particularly susceptible to unauthorized Hacker activity. There are also cases of unethical employment practices, with some firms knowingly hiring EP's with experience that extends far beyond the role or position, and with known expertise in Vendor Governance + Sourcing (VG+S).

- ✓ ***Lack of Consent.*** In most cases, Hackers operate under the cover of "Authorization," typically acquired from the Hacker's Client, which could include corporations, firms, and private clients. In these cases, such activity is performed without the EP's knowledge and consent.


HACKER ACTIVITY
TARGETED PROFESSIONAL
Project A: Corporation
Project B: Firm
Project C: Government