

CYBERSECURITY RISK AND EXPOSURE ASSESSMENT

CREM

See your organization the way an attacker does.

An independent assessment of what you could lose, how exposed you are today, and which attack paths really lead to your critical systems, delivered with a roadmap that tells you what to do and how to do it.

Business risk

What matters most and what a breach would cost.

Real exposure

Weaknesses proven exploitable, not just listed.

Clear action

A sequenced plan for what to fix first, and how.

Two questions every leader needs answered.

A maturity assessment tells you how well security is run. CREM tells you what could actually hurt you, and how close an attacker already is to making it happen.

RISK

What could we lose?

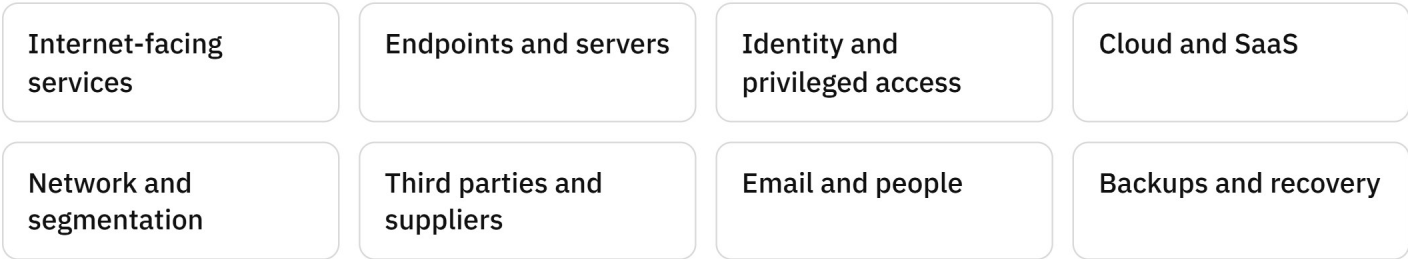
- Identify the systems and data that matter most.
- Model realistic threats: ransomware, data theft, fraud and outages.
- Rate likelihood and impact, and put a dollar range on the top scenarios.
- Build a risk register leadership can own and track.

EXPOSURE

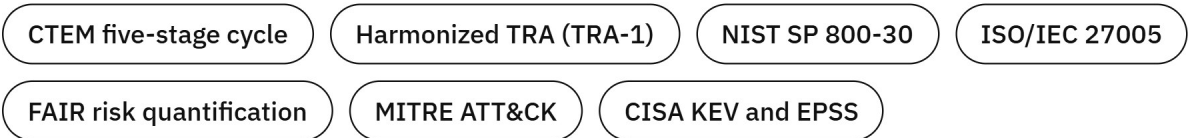
How could it happen today?

- Map your internet-facing attack surface as an attacker sees it.
- Find vulnerabilities, misconfigurations and weak identities inside.
- Rank them by known exploitation and likelihood of attack.
- Prove which attack paths actually reach your critical assets.

Where we look



BUILT ON RECOGNIZED METHODS



Not a spreadsheet of vulnerabilities. A plan.

Every iG2 CREM report includes a Recommendation Roadmap. Risks and exposures are grouped into the few actions that cut the most risk, each with clear steps, an owner, an effort estimate and a measure of done.

R-03 · Close the remote-access path to the finance server

SAMPLE ENTRY

WHAT	An internet-facing remote-access gateway has a known-exploited vulnerability. Testing confirmed a path from it to the finance file server.
WHY	Supports the highest-rated scenario, ransomware on finance systems, which would stop payroll and payments.
HOW	1. Patch the gateway to the vendor's fixed release and rotate its credentials. 2. Require phishing-resistant MFA for all remote access. 3. Segment the finance server from user networks, then re-test the path.
WHO · WHEN	Infrastructure lead, with the IT manager accountable · Now (first 30 days)
EFFORT	Low to medium: patching and MFA in days, segmentation in weeks
MEASURE	The attack path fails on re-test. The finance ransomware scenario drops from High to Medium.

NOW · 0-90 DAYS

Close proven attack paths to critical assets

NEXT · 3-12 MONTHS

Reduce exposure at its source

LATER · 12-24 MONTHS

Make exposure management continuous

Risk in business terms
Leaders see scenarios, likely impact and dollar ranges, so security spending can be weighed like any other investment.

Proven, not presumed
Priorities rest on validated attack paths, so your team fixes what attackers can actually use first.

Start with a snapshot. Grow into continuous coverage.

Your attack surface changes every week. Choose a one-time view, or keep risk and exposure under watch all year.

01	02	03	04	05	06
Scope	Discover	Analyze	Validate	Prioritize	Roadmap
Critical assets and business impact	External and internal exposures	Threat scenarios, likelihood and impact	Safe tests of real attack paths	Rank by risk to the organization	What to do and how, then brief leaders

CREM Snapshot

THE OUTSIDE-IN VIEW

Your internet-facing attack surface and its most urgent exposures, seen as an attacker sees them, with no access needed. Delivers an exposure summary and first-30-days actions.

CREM Assessment

FULL RISK AND EXPOSURE ASSESSMENT

Critical-asset scoping, threat scenarios, internal and external discovery, and attack-path validation. Delivers a risk register, the full report and a 24-month roadmap.

CREM Quantified

RISK IN DOLLARS

Everything in Assessment, plus FAIR-based loss estimates for the top scenarios to support budget, board and cyber-insurance decisions.

CREM Continuous

EXPOSURE MANAGEMENT AS A SERVICE

Monthly discovery and validation, a quarterly risk register refresh, roadmap progress tracking, and alerts when a weakness you have starts being exploited.

ig2 GROUP INC.

100% Canadian-owned · Burlington, Ontario

Your data. Your AI. Your defence.

ig2.ca

cs@ig2.ca

(289) 348-1530