



# TAKING SECURITY & RESILIENCE TO THE NEXT LEVEL

Next Peak is a **premier cyber, risk, and resilience** consultancy that provides deep **strategic advisory and operational** services. Our **flexible propositions** are tailored to clients' company size, industry and ambitions, designed to meet your cyber and risk maturity needs and journey.



**Greg Rattray**  
Partner/Co-Founder

- Former Global Chief Information Security Officer (CISO) & Head of Global Cyber Partnerships at JP Morgan Chase
- Former Director for Cybersecurity on the US National Security Council
- Established US national cyber exercise program as well as the Advanced Persistent Threat (APT) & Operational Collaboration concepts



**Jim Cummings**  
Partner/Co-Founder

- Former Chief Security Officer (CSO) at JP Morgan Chase, directing physical & cyber security, crisis management & business resiliency
- Former Director for Homeland Security on the US National Security Council
- Commanded both offensive and defensive U.S. Air Force cyber operations

Our approach is grounded in **deep business, financial services, and national security experience**, with demonstrated leadership and commitment to **delivering practical, business-driven solutions** to meet emerging threats across **cyber, technology, operational resilience, and third-party risks**, aligned with leading industry frameworks and best practices





## Cybersecurity & Technology Risk

We lead organizations through full program transformations by assessing maturity, co-creating roadmaps and plans to reach the target state, and then partnering to execute the plans, delivering a sustainable program built for continuous improvement.



### Risk & Maturity Assessments

Understand your organizations true cyber and technology risk exposure and maturity through tailored assessments aligned to industry frameworks, including the CRI Profile, NIST, & ISO27001.



### Program Design and Co-Creation

Transform your organizations operational posture by establishing a comprehensive strategy, modernizing controls and defenses, delivering Board ready program governance and measurement.



### Secure Architecture Design

Proactively protect your digital footprint and assets, ensuring operational resilience through secure and resilient design of your organization's technology and operational architecture, ensuring regulatory requirements and best practices are accounted for at every step.



### Operational Uplift

Improve the efficiency of your defensive operations and reduce cyber risk by identifying the high-risk gaps in your cybersecurity posture and uplifting requirements and controls.



### Exercising & Testing

Jointly designed exercises, and exercise programs, for cyber operational teams or executive leadership teams to ensure effective incident response.



## Operational and Cyber Resilience

We guide organizations through resilience assessments and uplift programs that cohesively address today's evolving threats—from natural and geopolitical to cyber and AI, to meet the increasing demand for operational continuity in a volatile world.



### Risk & Maturity Assessments

We assess your ability to maintain critical services before, during, and after severe but plausible disruptive scenarios. We test integration across crisis management, business, and technology, and deliver actionable recommendations with a roadmap aligned to industry frameworks.



### Resilient by Design Strategy and Program Design

We partner with your organization to create a comprehensive "Resilient by Design" strategy that extends beyond technology to cover data, physical asset, personnel, and third-party risks, to create a Board-ready implementation roadmap that aligns enhanced resilience capabilities with your critical assets.



### Program Implementation

Our team can help yours execute the roadmap and implementation plans, building sustainability and ownership to prevent “shelfware,” building in governance and measurement to support assessment of risk reduction.



### Scenario Exercises & Testing

Leveraging our deep experience in severe but plausible scenario development and exercise planning and execution, we co-create an exercise program and calendar to ensure critical asset recoverability is tested operationally and in tabletop scenarios.



# NEXT PEAK

## Third Party Risk Management

Next Peak has deep experience in helping organizations understand and address their third-party risk concerns. Our tailorable propositions are geared to help design, strengthen, and future-proof your Third-Party Risk Management (TPRM) Programs.



### Risk & Maturity Assessments

**Gain a clear view of your third-party exposure:** We identify and prioritize critical vendors, assess inherent and residual risk, evaluate policies and controls, and benchmark maturity to deliver a focused, actionable roadmap



### Program Design & Uplift

**Build a scalable, business-aligned TPRM framework:** We enhance operating models, embed risk-based tiering, trigger-based reassessments and structured issue management, strengthen governance, and implement meaningful metrics for continuous monitoring and reporting.



### IP Control Review

**Protect your most valuable intellectual property and sensitive information:** We assess third-party access, data protection, contractual safeguards, and monitoring controls to reduce the risk of leakage or theft.



### Contract & SBOM Review

**Strengthen contractual and technical protections:** We advise on vendor security clauses, audit rights, breach obligations, subcontractor flow-downs, and Software Bill of Materials (SBOM) transparency.



### Exercising & Testing

**Test your ability to respond:** We help you validate your resilience through realistic tabletop and technical simulations covering third-party failures, cyber incidents, and supply chain disruption.