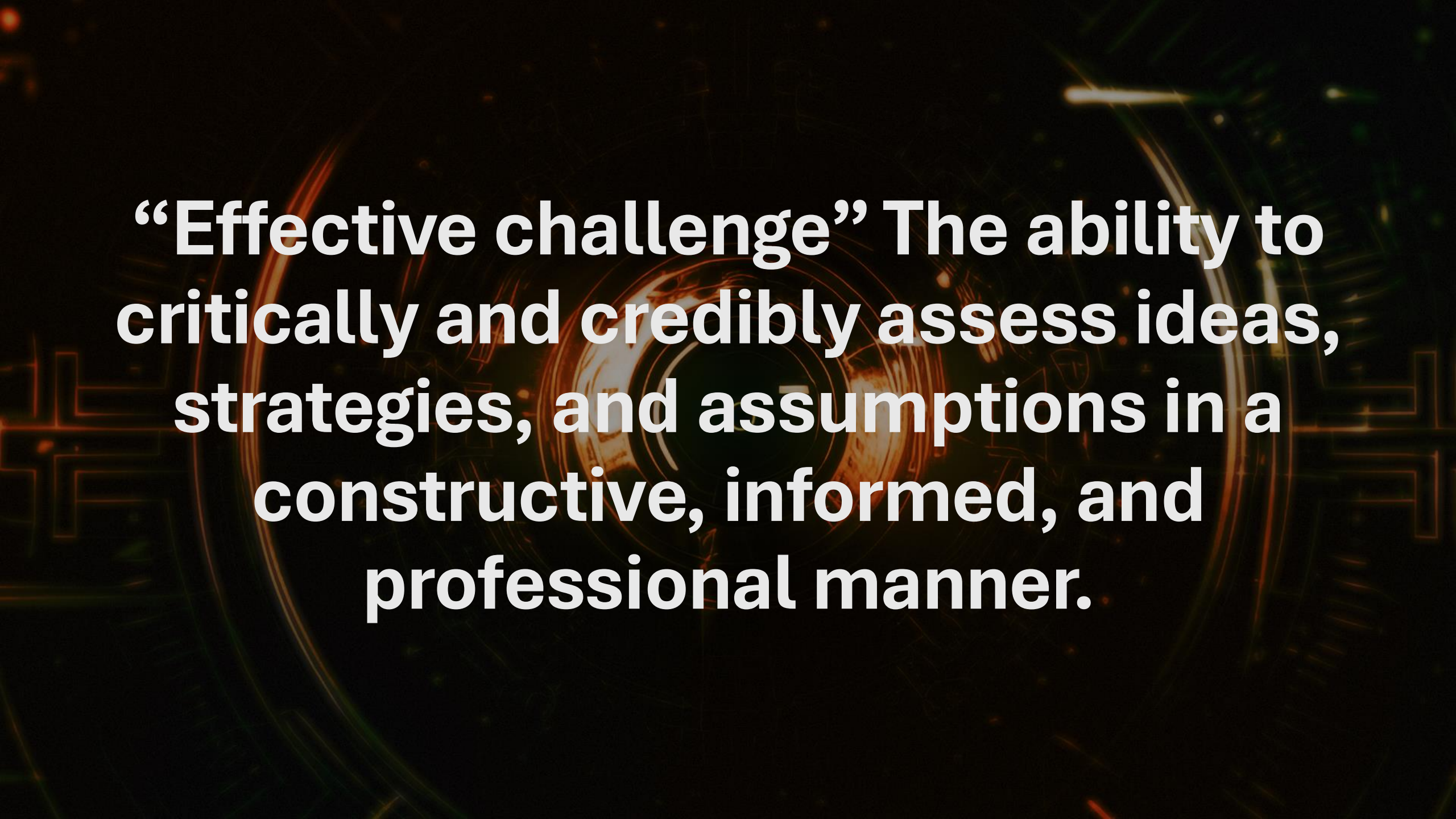




Cyber Confidence: Building Programs that Withstand Scrutiny

Victor Vinogradov

Cyber Security Leader



“Effective challenge” The ability to critically and credibly assess ideas, strategies, and assumptions in a constructive, informed, and professional manner.

Introduction

Vic Vinogradov

Former Regional Banking CISO

From 2015 to 2025, Vic served as CISO for Western Alliance Bancorporation, one of the nation's top-performing banking institutions. Vic led both first and second-line security and fraud programs through a period of rapid organic and acquisition-driven growth, overseeing a rise in bank assets from \$14 billion to over \$86 billion.

Vic held senior positions IT operations, and cybersecurity at Charles Schwab, American Express, and TÜV Rhineland. He holds a bachelor's degree in electrical engineering, a master's degree in information security, and multiple credentials including CISSP and the NACD/Carnegie Mellon Certificate in Cybersecurity Oversight. Vic also contributed to national policy efforts as a member of the Federal Reserve's Secure Payments Task Force.

www.linkedin.com/in/victor-vinogradov



Why “Effective Challenge”

- **Critical Analysis:** It involves gather evidence, questioning assumptions, identifying limitations, and proposing alternatives to improve outcomes.
- **Objective and Informed:** Those providing the challenge should have *relevant* expertise and a clear understanding of the subject matter.
- **Constructive Engagement:** The goal is not conflict, but incremental mitigation of risk within the risk appetite of the organization.



Effective Challenge: 3 Lines of Defense Model Financial Services

- **1st Line Business lines / IT** – Run the business, accept or mitigate risks, documents risk controls, performs control self assessment and testing.
 - **2nd line Risk** – Owns the risk management program, sets the “tone” for risk and provide effective challenge to the first line via assessment, negotiated thresholds for key risk indicators, risk oversight.
 - **3rd line Internal Audit** -Provides effective challenge via audit of the 1st and 2nd line.
 - **Regulatory bodies** - FRB, OCC, etc. provide oversight of all three lines of defense to ensure appropriate risk management.
-



Where does your organization use “Effective Challenge”



Internal:

Team level peer review of standardized architecture, designs and IT changes ?

Solicit enterprise-wide review of policies and standards?

Document justifications to deviate from standards ?

Collection of evidence proving control procedures are being followed?

Resilience and recovery, documented proof you can recovery from disruptive events?



External:

Red team / blue team testing, adversarial simulations, point in time and continuous PEN testing?

Use of external frameworks e.g., NIST CSF / CRI for defined effective evidence?

Data management, vulnerability management, staffing and skills assessments etc?

Quantitative financial risk modeling, peer benchmarking, third-party risk assessments?



Show me don't tell me.

Challenges and assessments are more effective when they are evidence based and performed by informed qualified entities.



NIST CSF / CRI Example of Effective Evidence

Cyber Risk Institute Profile Assessment Tool provides suggestions for effective evidence to credible challenges

Profile Subcategory	CRI Profile v2.1 Diagnostic Statement	Response Guidance	Examples of Effective Evidence (EEE) Packages
GOVERN / Risk Management Strategy / Technology Assimilation & Implementations	GV.RM-08.06: Technology programs and projects are formally governed and stakeholder engagement is managed to facilitate effective communication, awareness, credible challenge , and decision-making.	Organizations should establish roles and responsibilities for governance and oversight of the organization's technology programs and projects. The governance should provide credible challenge to the business decisions and operations, facilitate effective communication and reporting structure, and provide awareness of risks, threats, and opportunities.....	EEE-053: Project Governance, Management, and Quality Assurance Documentation EEE-054: Technology Service Performance and Support Monitoring Documentation EEE-099: Technology Delivery and Quality Assurance Documentation

Six NASD Principles for Board Oversight of Cybersecurity

Boards need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT Risk.

Boards should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular adequate time on board meeting agendas.

Boards should set the expectations that management will establish an enterprise-wide, cyber-risk management framework and reporting structure with adequate staffing and budget.

Board-management discussions about cyber risks should include identification and quantification of financial exposure to cyber risks, and which risks to accept, mitigate, or transfer.

Boards should encourage systemic resilience through collaboration with their industry and government peers and encourage the same from their management teams



Thank you



SYNERCOMM