Continuous Adaptive Risk Evaluation

November 11th, 2020 | FHCAREv02

CANDA Solutions
THINGS DONE

10500 Little Patuxent Pkwy, S. 620
Columbia, MD 21044

855.55.CANDA (22632)
info@candasolutions.com

WFMC Awards for Excellence in Case Management WINNER 2017

Inc. 5000 HONOREE

2018 GREATER WASHINGTON INNOVATION AWARDS™ FINALIST

Gartner

SUMMARY

Many organizations today are struggling with enterprise-wide risk visibility. To facilitate, centralize, improve and simplify Risk Management across different parts of any corporation there is a key necessity for an integrated and collaborative top-down and bottom-up approach.

Unfortunately, multiple risk factors including human ones can generate a high-risk profile, whether intentional or not. Thus, any Integrated Risk Management (IRM) solution deemed successful, must leverage the interdependencies of multiple Enterprise risks, internal and external factors, audits, prioritization, measurement, mitigation and reporting of consolidated threats to the Enterprise.

> *Enable risk management teams to move beyond yearly "risk management" checklists to make **continuous, adaptive**, and intelligent risk-optimized security control decisions.*
>
> "Seven Imperatives to Adopt a CARTA Strategic Approach"
> Gartner, Inc. | 3871363

CONTINUOUS ADAPTIVE RISK EVALUATION

Security as a 4th pillar of acquisition is a timely and crucial DoD (Department of Defense) initiative. The CMMC (Cybersecurity Maturity Model Certification) implementation is an imperative step towards Enterprise cyber defense goals but it is only a partial answer since many agencies and enterprises still operate in silos and many business functions are disconnected. Our out-of-the-box CARE approach aligns with 4 out of the 5 pillars of the National Counterintelligence Strategy released in February 2020.

The CARE module is based on an Enterprises' ability to baseline and prioritize critical programs, personnel, facilities, suppliers / vendors / subcontractors, and assets within the Fresh Haystack ecosystem to access, manage, investigate, and mitigate Risk continuously.

National CI Strategy Alignment

- ✓ Protects the National Security Infrastructure
- ✓ Reduces threats to Key US Supply Chains
- ✓ Counters the Exploitation of the US Economy
- ✓ Counters Foreign Intelligence Cyber & Technology Operations

Diagram on the next page demonstrates our approach to identifying Enterprise Risk baseline on multiple Risk Streams, prioritizing and evaluating them, documenting mitigations, scoring the baseline and producing Tailored Security Plan (TSP) tracking all activities needed for reducing risk exposure. For example, supply chain and cyber risk vectors specific to CMMC have capability to store and track not only controls related to each CMMC level, process or practice but also capture mitigation date/actions as well as artifacts proven completion of the particular control.

We propose to move from the theoretical concept of $f(R) = \mathbf{T}, \mathbf{V}, \mathbf{C}$ (i.e. *R – Risk, T – Threat, V – Vulnerability, C- Consequence)* to a *more adaptable risk* evaluation capability:

$$\text{e CARES} = \frac{\sum_a^z I_a * \mathbb{P}(a)}{\sum_a^z \mathbb{P}(a)}$$

a-z is one out of the Risk Streams below:

- Contracts – cCARES
- Suppliers/Vendors/Subs – sCARES
- Facilities – fCARES
- Personnel Security – pCARES
- Human Resources – hCARES
- Cyber / CMMC – nCARES
- Insider Threat/CI/CV – iCARES
- Physical Access – paCARES
- Assets/Equipment – aCARES

I – Impact
$\mathbb{P}$ - Probability
$R = I_a * \mathbb{P}(a)$
$\sum$ - the sum

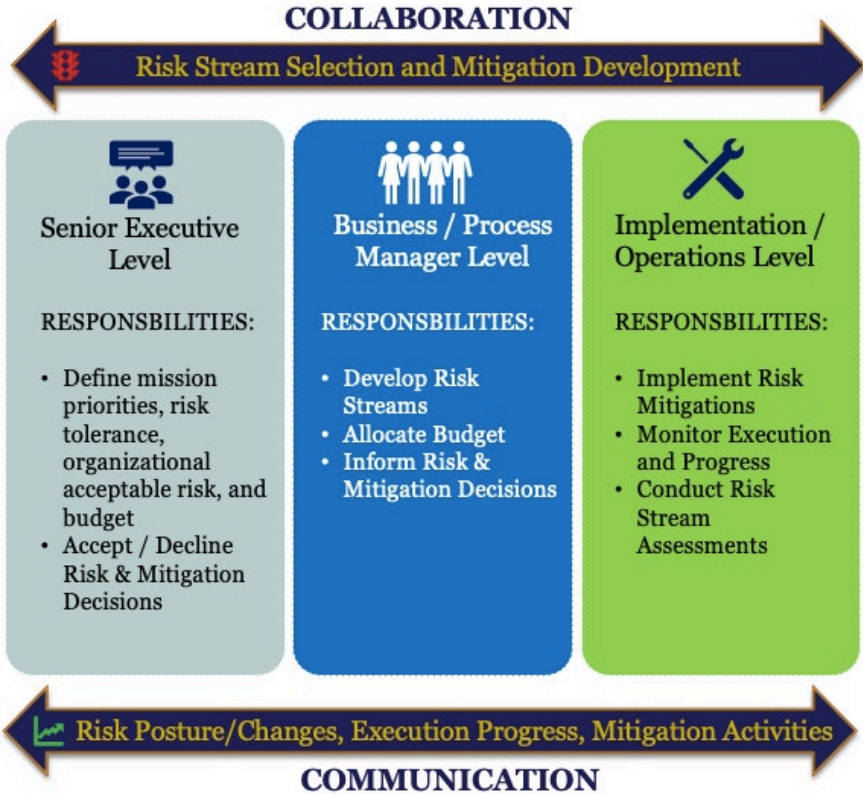
Each Risk Stream is prioritized using a wizard. All issues are documented, audited, weighted, and probability is added. The risk score is calculated for each risk stream and the total Enterprise Risk (eCARES) is a weighted mean of the individual risk streams. Guidelines and help to define the right settings for impact and probability (aka likelihood) are available and drive scoring algorithm.

If eCARES exceeds the acceptable baseline (i.e. 85 higher than 80), then the system will prompt for mitigation steps with dates that triggers the creation of the TSP version. This allows for tracking and reporting metrics and corporate risk over time. This technology enables a security risk OODA Loop

(Observe, Orient, Decide, Act) capability previously not possible within the Federal Government and DIB.

The notion of "Deliver Uncompromised" war-fighting capabilities must be part of the overall approach of the United States Government (USG) and the Defense Industrial Base (DIB) for protecting critical information and/or technology being wittingly or unwittingly lost, stolen, denied or degraded. Key elements of achieving this mission are:

- Breaking silos & enabling collaboration between organizational / functional business units
- Change Management & Open Communication Channels for an Enterprise



CONCLUSION

Fresh Haystack's modular ecosystem enables the realization of an Enterprise Risk Management capability that was previously limited by technology. We believe our IRM solution bridges this gap by converging the individuals, their profiles, access, networks, risks and activity into a single pane of glass for agencies and corporations to evaluate true risk exposure by consistently making intelligent data-driven decisions to access, track and capture mitigation opportunities while continuously delivering Trust and minimizing Enterprise risk.

