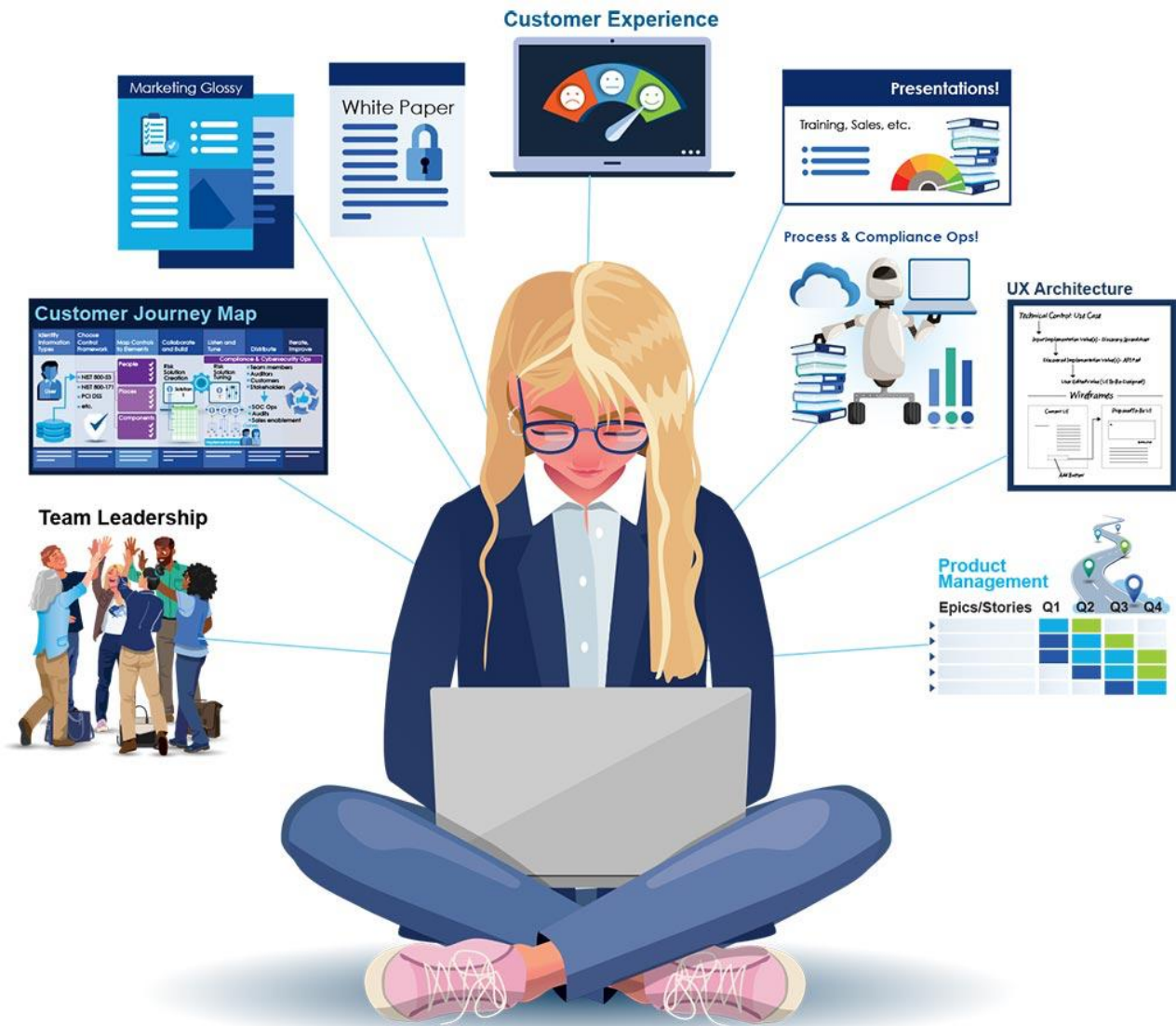


2024 25

Sarah Hensley

Annual Performance Report

"A jack of all trades is a master of none, but oftentimes better than a master of one."



The contents in this annual review document are far from all everything I accomplished - but reflect a sub-set of work that was completed and together represents the breadth and depth of my contributions to stackArmor in my first year.

2024/25 Goals	5
Product Management: Armory Plus	6
Armory Conceptual Infographic, Slide Deck	6
Armory High Level Architecture Illustration	7
Created Multiple Armory Model Infographics	8
Built out an Armory Journey Map Draft	9
Developed Armory Product Management Strategic Plan	10
Created Armory System User Manual DRAFT	15
Armory Program Management Implementation Guide	16
Developed Armory RBAC Management Tool.....	17
Developed ISV Customer Go/NoGo Analysis Tool	18
Created Armory Website Original Illustrations	19
Created stackArmor Internal Product Description	20
Supported Fawad to Evolve ThreatAlert Roadmaps	21
Engagement Management Leadership.....	22
Implemented Employee “SMART” Goals Template	22
Built a Robust Engagement Management Playbook.....	23
Created a ConMon Customer Escalation Guide	24
Established SOP Library and Template	25
Supported Multiple Customers as a Prime EM.....	26
Created a Role Based Training Template for Gecko	27
Established an EM Customer Retention Plan Program	28
Created EM Onboarding Role Based Training	30
Customer/User/Employee Experience	33
Established a Customer Newsletter	33
stackArmor Journey Map 1 Sales Journey	36
stackArmor Journey Map 2 ATO Journey	37
stackArmor Journey Map 3 ConMon Journey	38
Created Quick Reference Guides & Template	39
Full CX Program with Analysis/Management Tool	41
Customer CX Action Plan Program “Plan to Green”	42
Established stackAcademy for Role Based Training.....	44

CX/EX – Designed & Built Company Portal/Intranet	45
MVP Customer Advisory Board – NPS-Based Customer Satisfaction Tracking	47
Marketing & Content Development	48
Created a stackArmor Brand Guide	48
Designed Logos for the Armory and Armory 20x	53
Created Tyto Board Presentation Infographics.....	54
Created FedRAMP 20x Launch Infographics (GP)	55
Created Component Definition Paper Infographic.....	56
Created a New Armory 2 Pager	57
Created a Revised ThreatAlert 2 Pager	58
Delivered Brown Bag Session - Armory	59
SWFTAlert New Offering Infographics	62
Built Robust TechTrend Slide Deck	63
Illustrated and Animated stackArmor Offering Gears Infographic.....	66
Professional Growth.....	68
Attended UX Camp 2025.....	68
Took a Harvard Mini Course on Leadership	69
Read the Phoenix Project (per Ask from GP)	70

2024/25 Goals



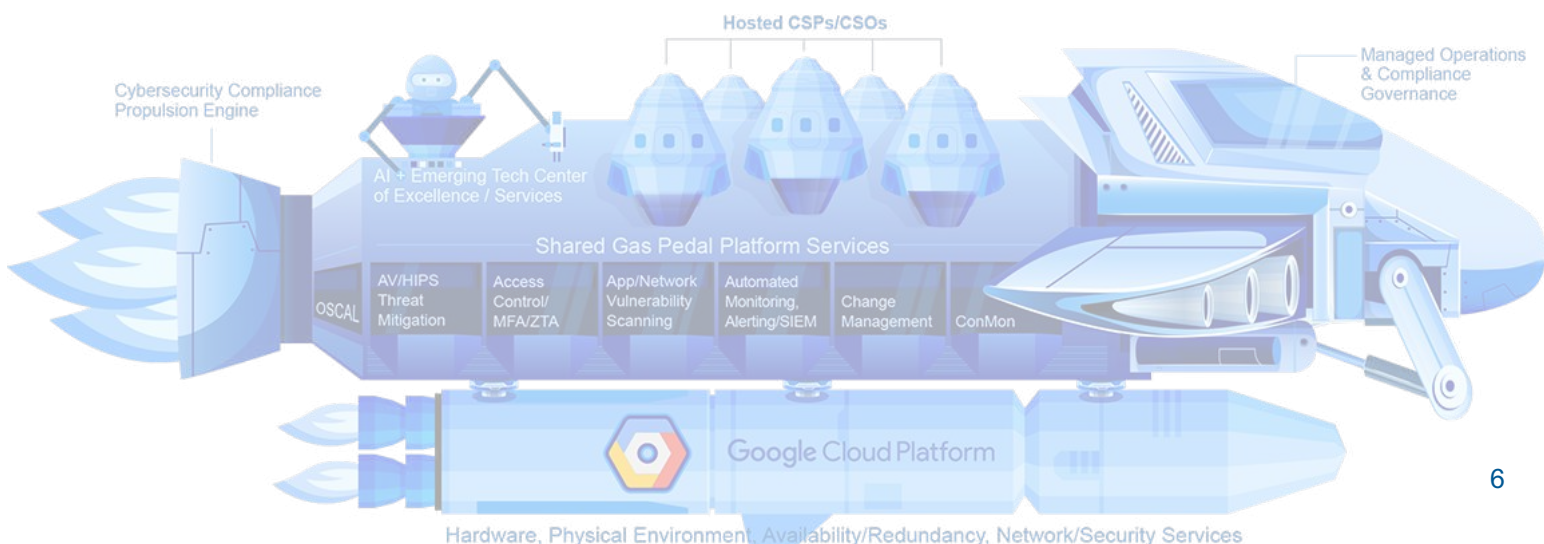
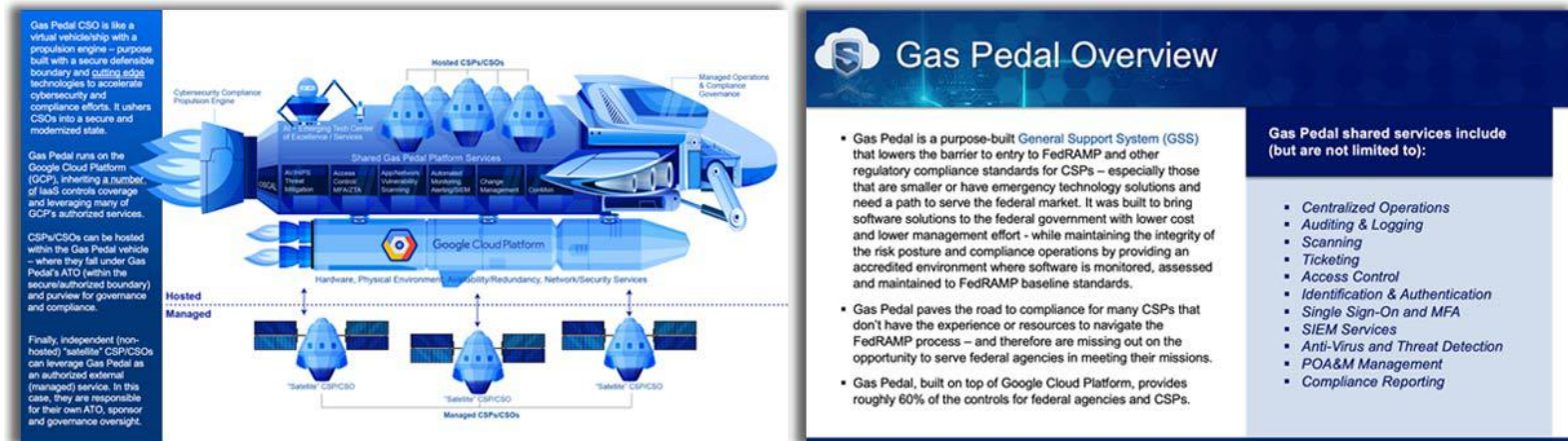
Goal		Status	Ref Links
First 3 Mos	Pre 1 - Tackle initial efforts as I ramp up at stackArmor a. Establish a total program establishment plan for Gas Pedal/Armory – Q3 2024 (done) b. Establish unique infographic (week 1) and Armory Logo – October 31, 2024 (both done) c. Establish the high level architecture infographic (for hosted & managed offerings) – (done) d. Establish a program as described in the CX C-level job description I presented to stackArmor early in 2024 (done – established a CX/CI program) e. Establish issue resolution tool to formalize & standardize service delivery maturity (done) f. Complete initial discovery on recurring issues that are damaging the CX, putting our contracts at risk – (done Q3, 2024, list exists and incorporated into the CX/CI tool)	All Completed in the first quarter of my employment, before establishing my formal goals ☺	a – pg. 10 b – pg. 6, 53 c – pg. 8 d – pg. 41-47 e – pg. 41 f – pg. 41
	1 Establish a Clear Description of the Customer Journey for stackArmor Service Offerings	Completed all 3 – Jan 2025	pg. 36-38
	2 Establish the customer journey map for Armory as a part of product management	Complete	pg. 9
	3 Create Armory Program Management Guide and PMO Establishment	Complete	pg. 16
	4 Author at least 3 blogs or articles for publishing (ask from GP)	Completed - Authored 3 Newsletters +	pg. 33-35
	5 Establish Clear Branding and Definitions around stackArmor IP and Offerings (ThreatAlert Security Workbench, Security Toolbox, Serverless Relay, Container Scanner, etc.)	Complete	pg. 20
	6 Create an Armory User Manual (with or without a RACI) – Appendix D of the SSP	Draft Completed – Effort shelved by CISO as not needed	pg. 15
	7 Productize a Pre-Readiness Assessment Offering (using Nozomi as a model)	Task Cancelled by Armory team	N/A

Product Management: Armory Plus

Armory Conceptual Infographic, Slide Deck

Original vector illustration created to visually communicate the concept of Armory using a ship, engine, and satellite metaphor.

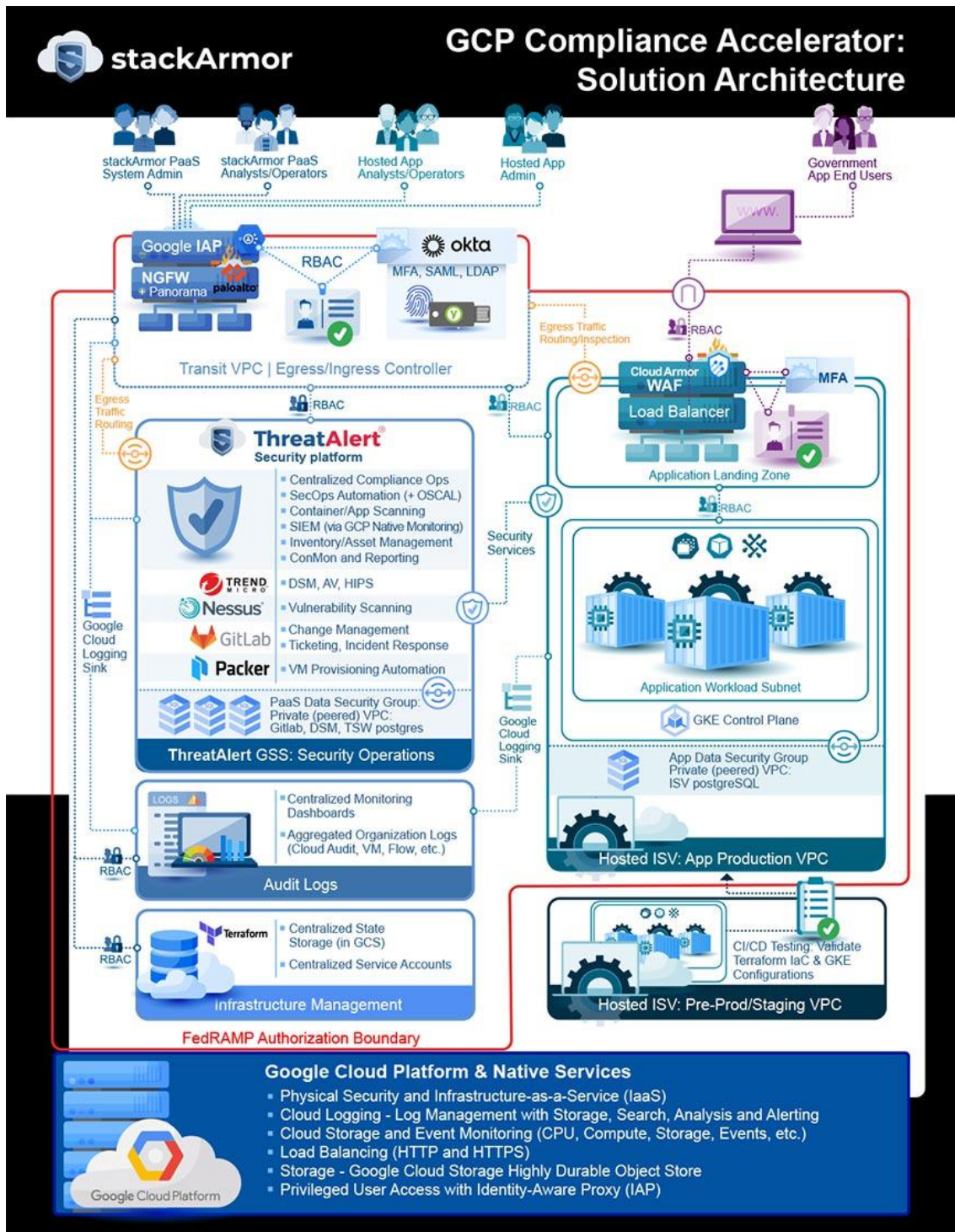
- Graphic **called out by FedRAMP Director Pete Waterman** as one everyone should stop and appreciate!!! 😊
- Used in multiple sales/marketing presentations
- **Animated this ship** in PowerPoint to tell the story of hosted and managed customers sing the concept of hosted “tenants” on the ship and managed “satellites” leveraging the ship’s services
- Also authored the overview description and created considerable content, which served as the foundation for verbiage still used today



Armory High Level Architecture Illustration

Original vector illustration created to visually communicate the critical architectural components of The Armory.

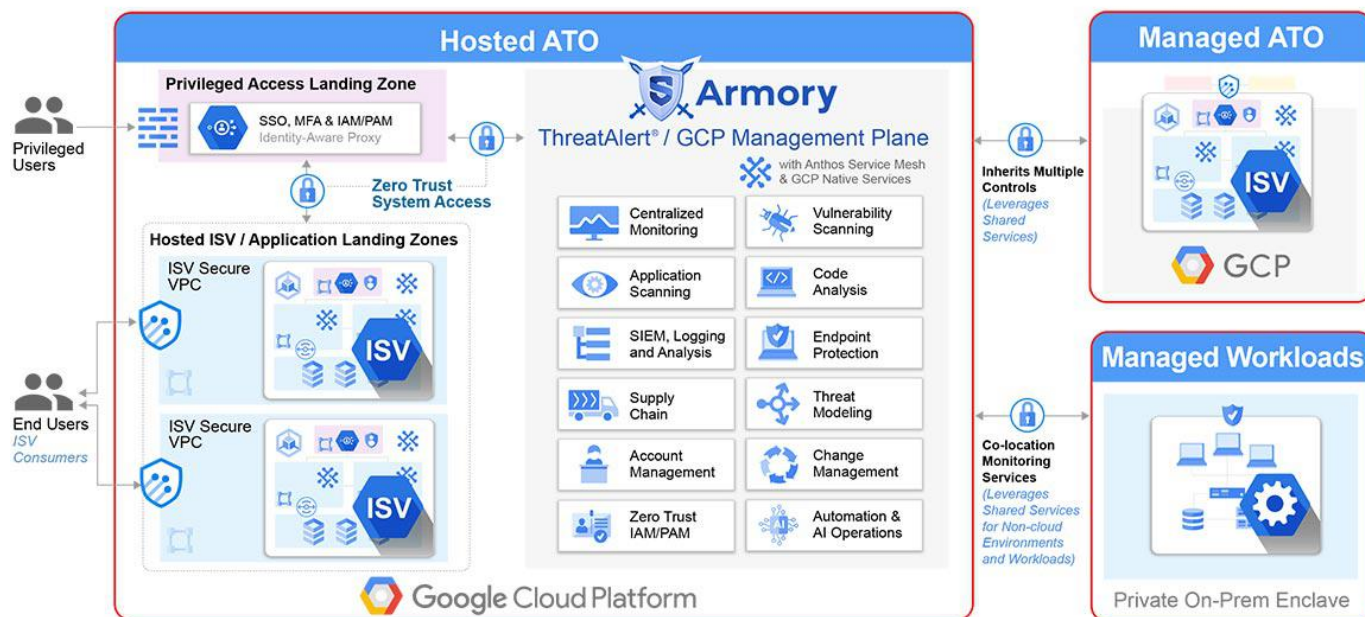
- *Source File in GitHub*
- *Used in Final SSP*
- *Leveraged for Multiple Sales and Marketing Presentations*
- *Multiple original icons & incorporation of Google Blue*



Created Multiple Armory Model Infographics

Original vectors created to visually communicate Armory deployment models and Armory's role in serving government agencies.

- All vector art, with versions created for GP and Martin saving both of these out by element and rebuilding in PowerPoint to allow them to edit. (I also created an animated version of both of these for Martin).
- Versions of these (and there have been many) have been used in multiple presentations.



Built out an Armory Journey Map | Draft

Created a draft of an Armory customer journey map, leveraging work done on non-Armory journey maps to save time.

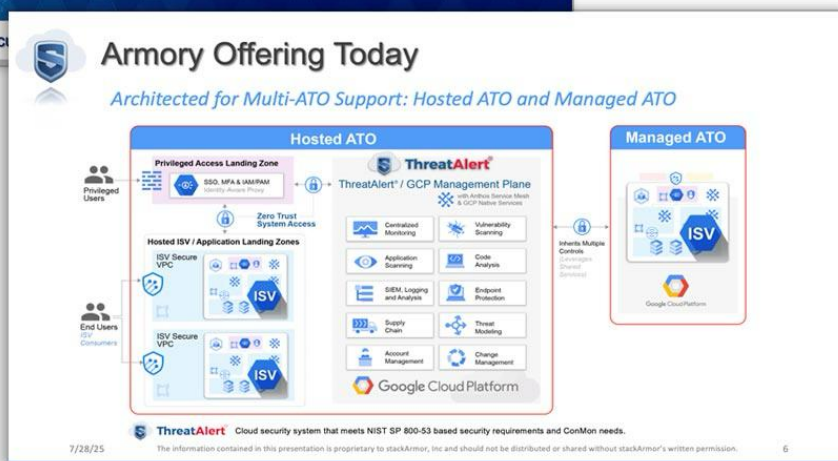
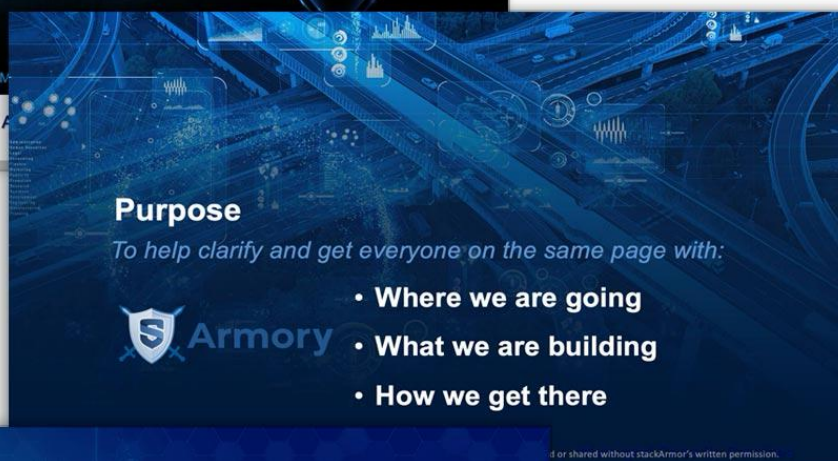
- *Journey Map is a key artifact of product managers and UX architects.* ☺
- *Created a combined Hosted/Managed map – we may want to break these out.*
- An animated version of this (once done) would be an excellent intro video for new customers!
- Fun fact – the blue castle is an original illustration I created initially for the Armory website (Martin asked for a “Game of Thrones” feel so I ran with that. In the end, we went with a different concept, but I decided for now to use this on the journey map☺.)



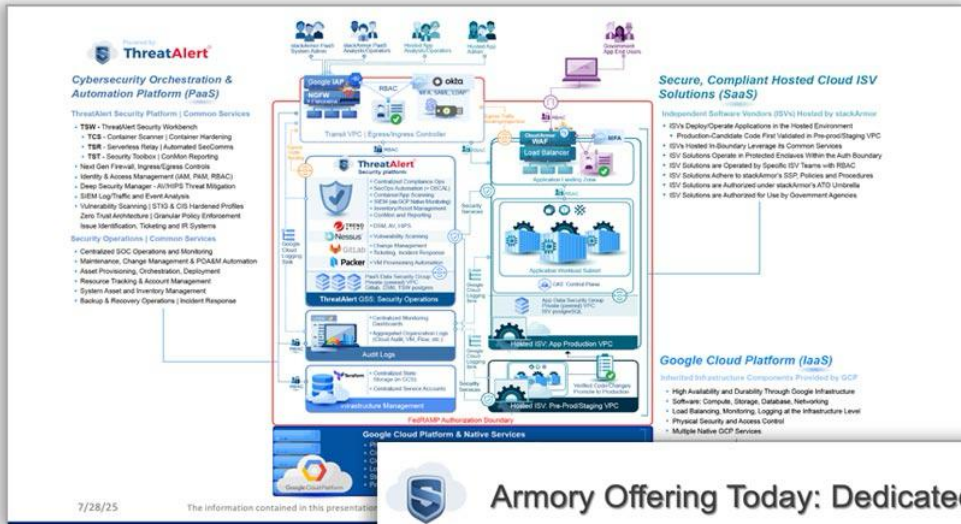
Developed Armory Product Management | Strategic Plan

Established an entire strategic product management plan to herd the proverbial cats and get everyone on the same page with the Armory AND other SA products. This plan was shelved early on by key C levels but remains a solid approach.

- Established mission, vision, resourcing, and path forward
- Contained SWOT analysis (standard for strategic plan)
- Established path to readiness (again, much of which was shelved)
- Defined plan for PMO, roadmap, user manual, etc.
- Also contained objectives for stackArmor's broader product offerings (e.g. ThreaAlert and the GSS suite)
- The marketing/content development tasks in the plan were completed



Armory Product Management | Strategic Plan Continued...



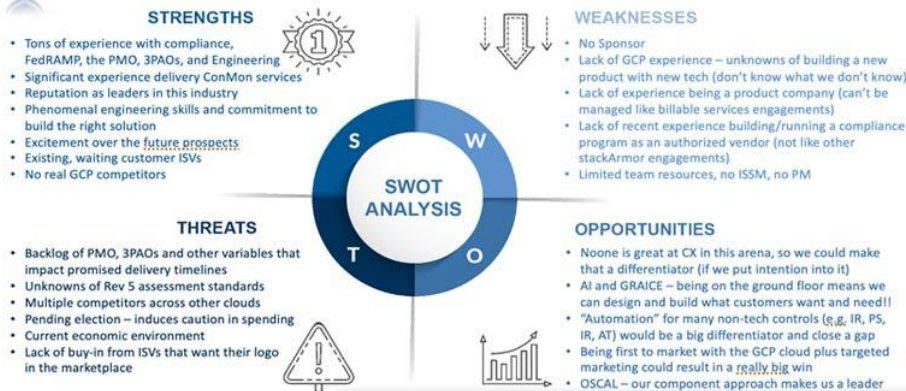
Armory Offering Today: Dedicated stackArmor Team

This was the proposed team... we aren't quite here yet...

FedRAMP P-ATO		
#	Role	Responsibility
1	Service Delivery Manager	Program Management, delivery and satisfaction
2	Project Manager	Project Management, tasks, deliverables, schedules
3	Sr. FedRAMP SME	Subject Matter Expert in FedRAMP, NIST and the package generation
4	FedRAMP SME	Supports in the development and delivery of package
5	Sr. Solutions Architect	Provides architectural guidance on landing zone, boundary protection, segmentation

employed to help deploy, configure and operationalize Customer accounts for logging, monitoring and

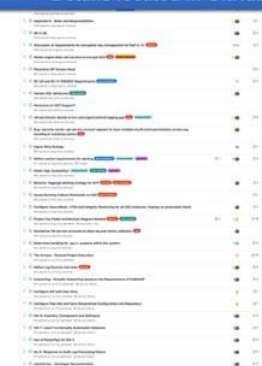
Armory Offering Today: SWOT Analysis



Path to Operational Readiness: Outstanding Tech Tasks

- ☐ We need to understand the time-to-operational.
 - ☐ The traditional stackArmor services delivery schedule doesn't accommodate a new product design/build effort (which is what Armory is).
 - ☐ The team has, to this point, been managing their tasks in GitHub.
 - ☐ There are 30 outstanding items, with no easy way to export the information to a project management tool or even CSV format (this is essentially the product backlog).
 - ☐ Given this would be a 1-time effort, we need to consider whether we make the investment to restructure the tasks into a different tool and format or run with this backlog as is and track it through to completion.
- ☐ I'll work with Johann to try to come up with a relatively solid weekly estimate of task completion and time-to-operational.
- ☐ We will begin to track as a product backlog burndown.

Details located in GitHub





Armory CX/Customer Journey

- Currently there is no defined customer journey.
- **Plan:** Create a customer journey map, that doubles as a marketing artifact as well as being a key infographic to communicate amongst our team how the product offering is consumed by users for better development and product



7/28/25

The information contained in this presentation is



Armory Product Roadmap

- Currently there is no formal product roadmap.
- **Plan:** Create a basic product roadmap to clearly define the initial MVP, then lay out target feature enhancements over the next few quarters. While it may change, it's important to have a working source of truth for where we are headed and helps guide foundational product decisions.

COMING SOON

- I haven't yet started this, but it's clear that we need a roadmap
- Without a roadmap, the team will build and the product will evolve as the waves of inspiration or opportunity or new ideas hit, which isn't all bad, but needs to be countered with a more strategic approach



Armory User Manual/User Guide

- Currently there is no user manual (SSP Appendix D), but there IS a set of playbooks, which significantly reduces the amount of content needed.
- **Plan:** Create an Armory user manual. I found this one of the most requested and appreciated artifacts previously, as it specifically tells users things they want to know about what Armory means for them...

COMING SOON

- This has not been initiated, but the CIS/CRM is a basis.
- I have starter content so I'm not starting from nothing...
- It serves as a supplement in the

7/28/25

The information contained in this presentation

Armory Product Marketing

As the product nears completion and looks to onboard its first ISVs, we should establish a clear marketing and branding approach...



Marketing, Branding, Content Development

- Currently there is no defined branding, plan, or even a name for the offering.
- **Plan:** Create initial branding guide for the to-be-named offering, and then update all of the content I've created thus far to reflect the final. Branding will include a logo (if any), color palette, imagery guidelines, etc.

COMING SOON

- Need to choose a name
- Need a content and blog calendar (white papers, glossies, infographics, etc.)
- This is important for the broader context of taking Gas Pedal to market
- I'll be working on this over the next couple weeks as a part of everything else, and look to reviews/approval from the C Suite...
- This will also include broader ThreatAlert branding and brand clarity...

7/28/25

The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

21

Beyond Armory

Leveraging this shift

The information contained in this presentation is proprietary to stackArmor, Inc. and should not be distributed or shared without stackArmor's written permission.



Beyond Armory – stackArmor's Suite of "Products"

As an add-on, as we move fully into being a "product" company as well as a services company, I've been asked to help build some brand recognition and clarification of our offerings with regard to ThreatAlert. Armory is jumping into the deep end, but we've already been in the "product" pool for a while



ThreatAlert®

- **Threat Alert Platform – Products + Services**
 - **ThreatAlert Security Workbench (TSW)**
 - **TSR (ThreatAlert Serverless Relay)** | automated SecComms
 - **TST (ThreatAlert Security Toolbox)** | ConMon Reporting Scanner) | Container Security

stackArmor, Inc. and
should not be distributed or shared without stackArmor's written permission.

23

What's next?

Along with the things covered in this deck.



Next Steps

- ❑ We need to finalize a name for project "Gas Pedal". (looks like Armory is happening...)
- ❑ We need to figure out resourcing and commitment to building the offering program to be able to support customers and navigate assessments alike – which requires a significant up-front investment. Hoping we can figure out how to creatively support this with existing resources.

Proposed "Monthly" Status Snapshot Dashboard

Project Schedule:
Green

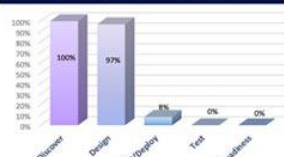
Tasks Accomplished

- GitHub tech build issues were updated
- Created first role-based training (beyond IR/CP)
- Created first draft of Armory PMO Guide
- Created template for Gas Pedal operational checklists

Planned Short-Term Tasks

- ❑ Identify key program milestones
- ❑ Address GitHub Issue Backlog (tech team)
- ❑ Continue maturing A&A Package Drafts
- ❑ Finalize PMO structure, Roles and Responsibilities for Armory CSO
- ❑ Author first draft of SSP Front Matter
- ❑ Search/Identify CSO ISSM
- ❑ Develop Armory CX plan/approach
- ❑ Establish PMO meeting cadence

Project Completeness by Phase



Key Issues

- Align stackArmor teams on task at hand re: the effort remaining to launch Armory
- Alienating initial customers as our launch is delayed...

As we look to start onboarding track and communicate with the gaining administrative control over ng and more about day-to-day

stractions, or edits... want to make sure I have time to

stackArmor, Inc. and
should not be distributed or shared without stackArmor's written permission.

25



7/28/25

The information contained in this presentation is proprietary to stackArmor, Inc. and should not be distributed or shared without stackArmor's written permission.



THANK YOU

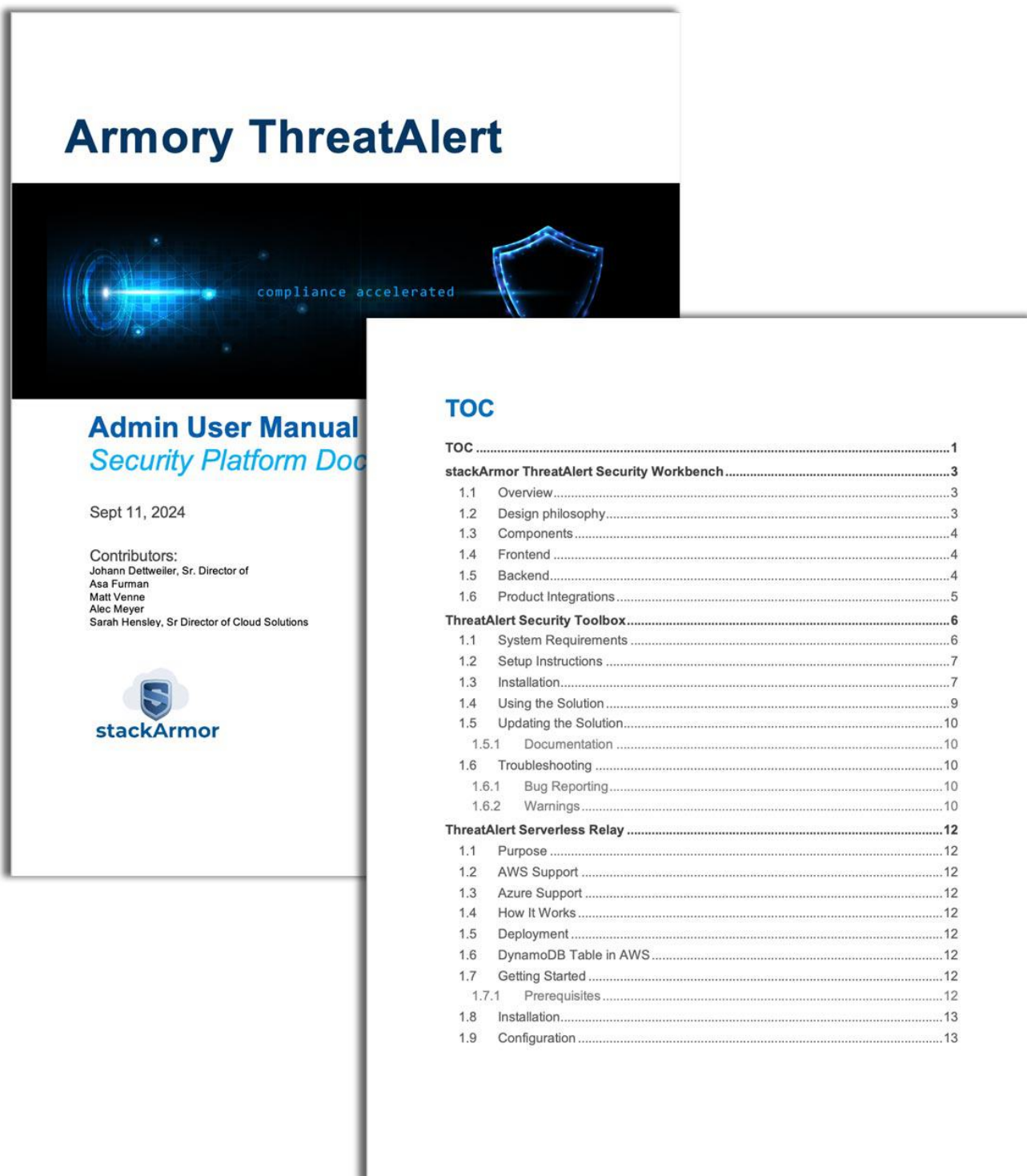
www.stackarmor.com

The information contained in this presentation is proprietary to stackArmor, Inc. and should not be distributed or shared without stackArmor's written permission.

Created Armory System User Manual | DRAFT

Established initial user manual DRAFT – focusing on the ThreatAlert GSS stack operations – leveraging ReadMe files from GitHub before this was shelved and deemed unnecessary in lieu of the playbooks and limited support resources.

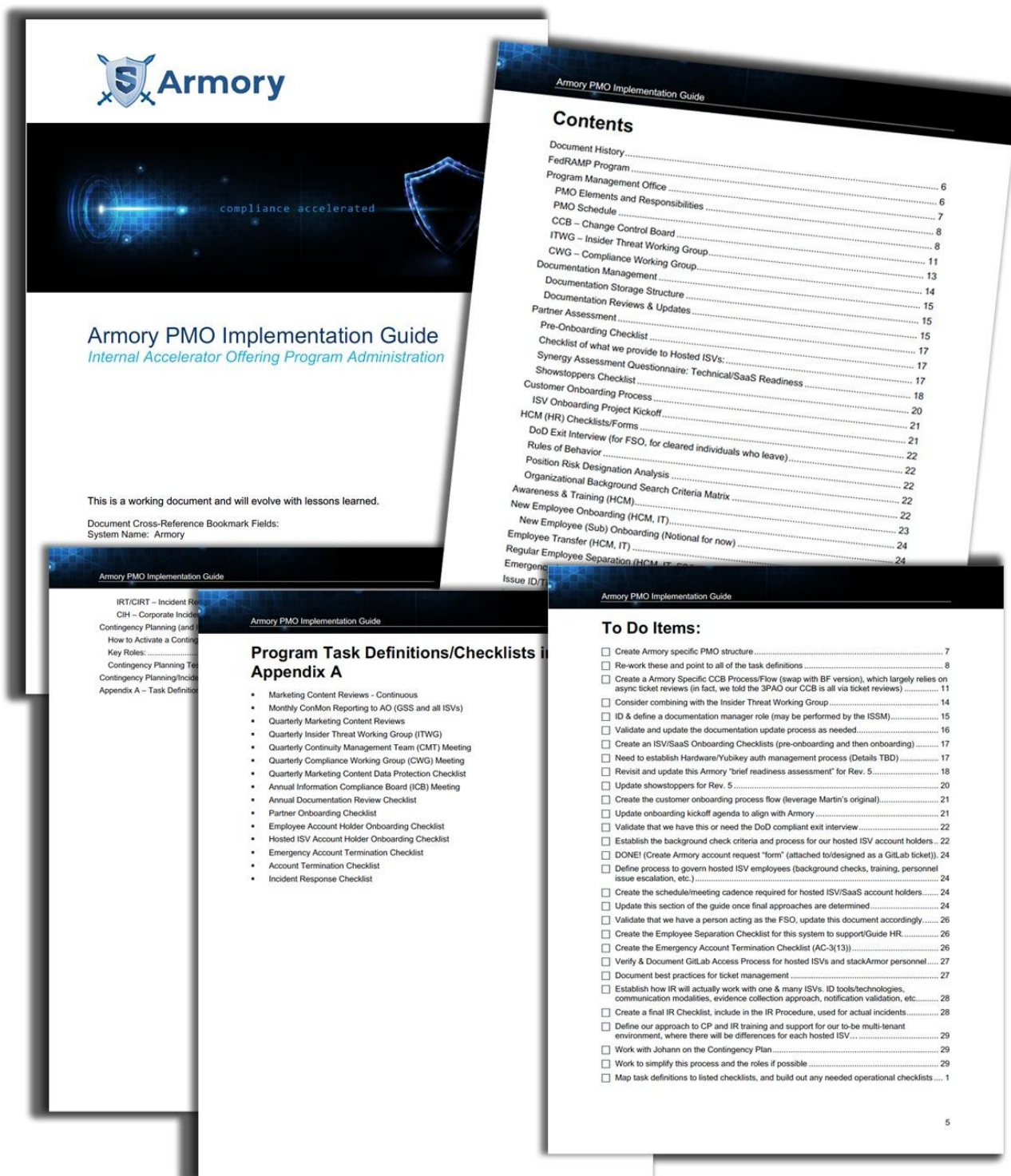
- *Established an initial draft in September 2024*
- *Draft focused on users who would be providing system operations leveraging the GSS stack within the Armory*
- *See the initial Draft cover and TOC below (the draft remains around 13 pages long, hasn't been updated since being shelved)*
- [*the-Armory-user-manual-draft1.docx \(sarah\)*](#)



Armory Program Management Implementation Guide

Created a solid draft of a PMO guide for an Armory program, but this was shelved, and in the meantime, the many changes in FedRAMP AND updates to our system's automations will render many sections of this irrelevant moving forward.

- Established an initial draft in Fall of 2024
- Draft focused on establishing a PMO office and operational guidelines for running a compliance program
- See the initial Draft cover and TOC below (the draft remains around 30 pages long, hasn't been updated since being shelved)
- *Armory-Implementation-Playbook-v2.docx (Sarah, antiquated draft)*



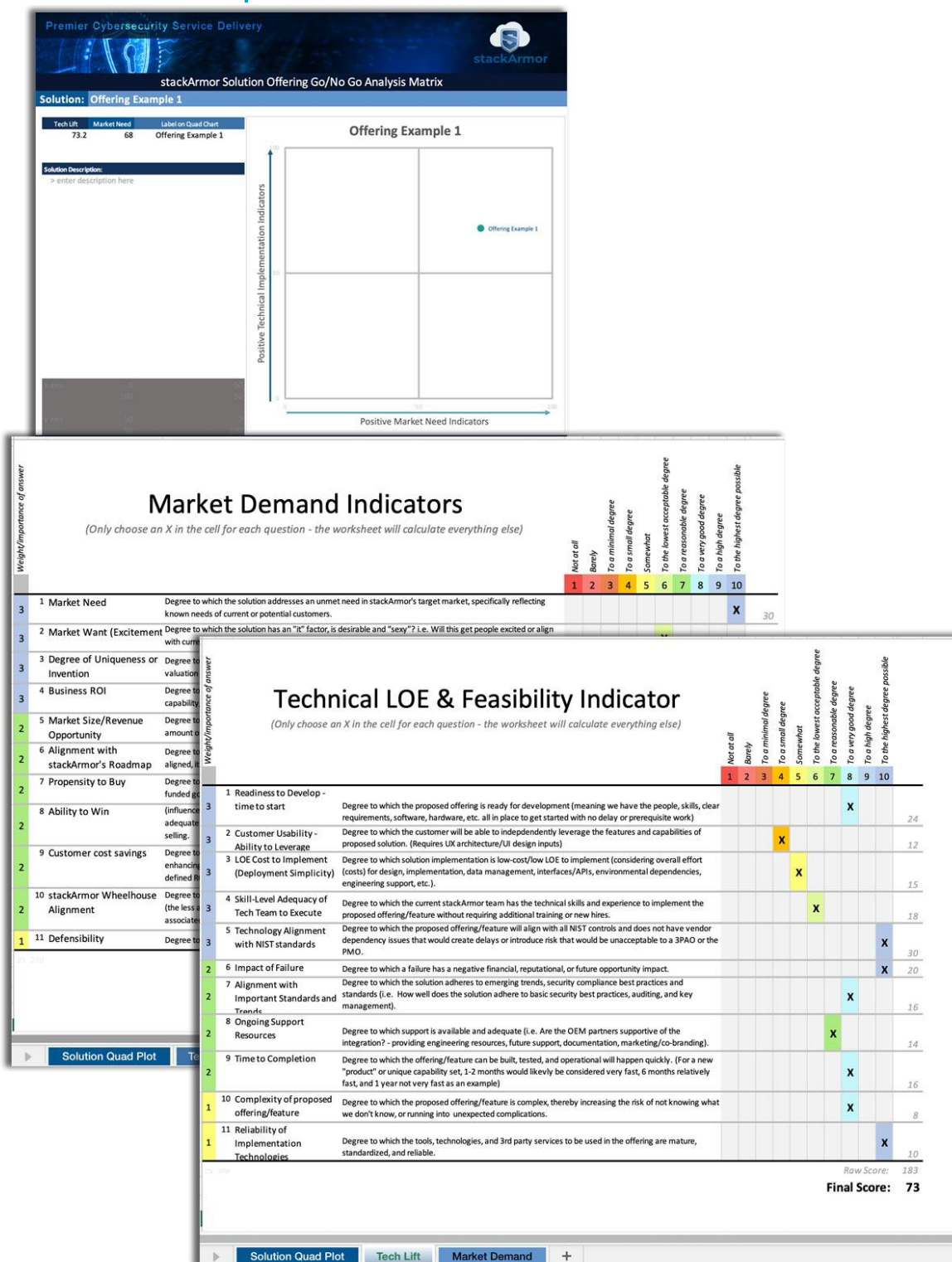
Created a tool in Excel (evolving an earlier version of a similar document I also created) to help Armory and Armory customers (and stackArmor customer for that matter) define their company roles and access requirements.

- [illegible]

Developed ISV Customer Go/NoGo Analysis Tool

Developed a standardized approach to assessing whether ISVs are a good fit for Armory or stackArmor customers (low risk, high reward)

- Used formulas and Visual Basic to enable a great UX (enforces only a single selection for each analysis question, and plots a potential customer on a Quadrant like Gartner's Magic Quadrant.)
- Used language in the rating scale to reduce subjectivity as much as possible.
- While I don't think this is something we would use (I realized after), it is a great tool and important to analyze the risk of taking on any particular customer, so I actually am very proud of this!
- [stackArmor-Go-NoGo-Assessment-matrix.xlsm](#) (Sarah)



Created Armory Website Original Illustrations

Created an *original complex vector illustration* (no photography) to showcase The Armory (for the website and product literature) based on look and feel guidance (and some “AI art” he had created) from Martin.

- Currently serves as the Hero image on the Armory website/webpage
- Image used on multiple sales and marketing artifacts
- A second version was created on white background (quite a bit of work to alter the image to be on white instead of the dark...)
- Source is an Adobe Illustrator file



Created stackArmor Internal Product Description

Created a 2-pager providing clarity around stackArmor's internal product suite, mostly for internal use due to lack of understanding of our own solutions.




- Leveraged Asa and team's read me pages in GitHub as a core source of information
- Created my own visual representations of the solutions (and iconography) to help "translate" and reduce cognitive load





Supported Fawad to Evolve ThreatAlert Roadmaps

Contributed a handful of feature suggestions, but mostly helped transform his backlog into tactical and strategic product roadmaps.

- Largely helped present Fawad's information in more of a roadmap format, both simplifying and clarifying through content re-structuring in a roadmap context and including multiple visual cues.
- Contributed significantly on the business value content of planned capabilities.
- Worked to identify quarters targeted for tactical items, with TBD for all strategic items.

ThreatAlert® Tactical Roadmap			  			ATOM - Landing Zone Builder ThreatAlert GSS Platform ThreatAlert eDocs OSCAL TSW - Security Workbench									
ID	Capability (Epic)	Business Value	Cloud								Q1 '25	Q2 '25	Q3 '25	Q4 '25	TBD
T-1	OS Shift: Upgrade GSS	Strengthens security posture while reducing operational overhead through improved system stability and streamlined support. Ensures FIPS compliance and minimizes vulnerability exposure, leading to more efficient incident response and enhanced system reliability.	AWS	x	x	x									
			GCP	x	x	x									
			Azure	x	x	x									
T-2	ATOM Enhancements	Accelerates time-to-market through standardized, automated infrastructure deployments while significantly reducing human error. Ensures consistent security controls and compliance across environments, streamlining audit preparation and operational efficiency.	AWS	x	x	x									
			GCP	x	x	x									
			Azure	x	x	x									
T-3	OSCAL Enhancements via GitLab Connection	Streamlines compliance documentation through automated OSCAL integration. Accelerates FedRAMP authorization process by standardizing control implementation and evidence collection. Enables real-time compliance visibility for stakeholders and reduces manual documentation burden.	AWS				x								
			GCP				x								
			Azure				x								
T-4	Automate ATOM Release Workflow	Minimizes deployment risks by eliminating manual errors while significantly reducing deployment time. Improves team productivity through automated workflows, enabling focus on high-value development activities and innovation.	AWS	x	x	x									
			GCP	x	x	x									
			Azure	x	x	x									
T-5	TST Security Toolkit	Strengthens boundary security while streamlining reporting cycles through automated environmental API queries. Ensures consistent security standards across all releases, reducing post-deployment incidents and accelerating secure delivery.	AWS		x	x									
			GCP		x	x									
			Azure		x	x									
T-6	GSS Hardened to FedRAMP High baseline (Remove)	Hardening is required to navigate FedRAMP Readiness assessment (RAR) and Full assessment required for ATO.	AWS												
			GCP	x	x	x									
			Azure												
T-7	Security Dashboard Enhancements	Improve value of data and context within which information is presented by tying to NIST CSF.	AWS												
			GCP												
			Azure												
T-8	Azure Automated Log Ingestion	Standardize and automate SIEM log ingestion to improve reliability and quality of SecOps by enabling TSR (Serverless Relay) in Azure.	AWS												
			GCP												
			Azure												
T-9	Implement Configurable Remediation Timeframes	Improve manageability and flexibility of ThreatAlert by enabling configurable remediation timeframes to support multiple frameworks, risk postures, and requirements specific to each customer.	AWS												
			GCP												
			Azure												
T-10	GovStack Integration	Support automated incident response (IR) using GovStack workflows, which is a significant and necessarily compliant operational enabler for IR activities.	AWS		x	x									
			GCP		x	x									
			Azure		x	x									

ThreatAlert® Strategic Roadmap			  			ATOM - Landing Zone Builder ThreatAlert GSS Platform ThreatAlert eDocs OSCAL TSW - Security Workbench									
ID	Capability (Epic)	Business Value	Cloud								Q1 '25	Q2 '25	Q3 '25	Q4 '25	TBD
S-1	LLM framework	Significant improvement in speed, accuracy, and manageability of ConMon operations with AI analyst using ConMon playbooks for automated incident response and noise reduction. Analyst force multiplier.	AWS												
			GCP												
			Azure												
S-2	Gitlab pipelines	Create continuous deployment pipelines in Gitlab rather than in each CSP. This allows us to quickly deploy our framework in each CSP being technology neutral.	AWS												
			GCP												
			Azure												
S-3	Multi-Cloud Architecture	Create a deployment method that is triggered by a Github action to deployment Gitlab and corresponding pipelines in each CSP.	AWS												
			GCP												
			Azure												
S-4	Next Gen SOC	Slack as a SOC, with integrated workflows for incident response and automatic anomaly detection.	AWS												
			GCP												
			Azure												
S-5	Threat intelligence integration	Integrate with global threat database and feeds with TSW.	AWS												
			GCP												
			Azure												
S-6	3rd party connectors	Create 3rd party connectors in TSW for additional product integration i.e. ServiceNow, Qualys, other security tools.	AWS												
			GCP												
			Azure												
S-7	AI-Powered FedRAMP Controls Monitoring	Automated continuous monitoring of FedRAMP controls using AI to detect drift from compliance baselines, predict potential compliance issues, and generate required documentation for audits. (Significantly reduce manual compliance work and improve security posture.)	AWS												
			GCP												
			Azure												
S-8	NIST CSF AI Risk Assessment Framework	Develop an AI-powered framework that maps potential AI/LLM vulnerabilities and risks to NIST CSF controls, helping organizations understand and mitigate AI-specific security risks in their environment. This would be particularly valuable as organizations adopt more AI tools.	AWS												
			GCP												
			Azure												
S-9	SecureRAG - SBU Data Analysis Platform	Create an internal, air-gapped RAG (Retrieval Augmented Generation) platform specifically designed for analyzing and querying Sensitive but Unclassified (SBU) data with robust security controls and audit capabilities.	AWS												
			GCP												
			Azure												
S-10	Zero Trust AI Operations Platform	Implement a zero trust architecture specifically designed for AI operations, ensuring all AI model interactions, training data, and outputs are properly authenticated, authorized, and logged according to federal security requirements.	AWS												
			GCP												
			Azure												
S-11	AI-Enhanced Alert Investigation and Reporting Platform	Develop an intelligent system that automates alert investigation, correlation, and reporting across multiple security tools while providing meaningful summarization at different time intervals. This reduces alert fatigue, speeds up investigation time, and provides better security insights to all stakeholders.	AWS												
			GCP												
			Azure												

Engagement Management Leadership

Implemented Employee “SMART” Goals Template

Created a standardized “SMART” goal management template to help mature and improve the employee experience and emphasize the importance of employee growth.

- Used this for myself as well as Amal, Mike and Shawn.
- Template helps ensure goals are specific, measurable, attainable, relevant and time-bound (SMART).
- Template can be found in the templates folder in the CX/CI SharePoint Intranet site.

Employee: <Name>
Supervisor: <Name>
Review Date: Friday, Nov. 1, 2024
Occasion: Annual goal review

Goals

Professional Growth Goals

<Specifically what you want to accomplish> 2
<Specifically what you want to accomplish> 3
<Specifically what you want to accomplish> 4

Goal 1: <Specifically what you want to accomplish>			
Specific	Measurable	Attainable	Relevant
How success will be measured:	How goal will be accomplished:	Purpose of the goal:	Target for completion:

Notes:

Built a Robust Engagement Management Playbook

Created an Engagement Management Playbook that clearly defines the role of EM at every step in the end-to-end customer journey – which was the result of a couple months of analysis and UX/EX work.

- The playbook is a foundation for onboarding, training, job description creation, cross-team collaboration and role clarification, etc.
- This was a direct result of confusion or lack of standardization over the exact role of those on the PM/EM team.
- Reviewed with multiple teams. Would love to do a brown bag on this.
- Current version is located on the CX/EX Intranet Site.



Created a ConMon Customer Escalation Guide

Created a simple escalation guide for our customers in response to some feedback that customers weren't sure how to escalate.

- This one is an example of one we provided Dewberry – but the only thing that changes is the customer name and the project team names.
- Got great feedback already from Checkmarx and Dewberry on this.
- I created not just a phone tree, but a matrix with examples of types of issues and the related appropriate escalation path.



Issue Escalation Process for ConMon Engagements



Figure 1. – General Escalation Path

Dewberry Specific Escalation Path:

Escalation*	Role/Title	Team Member	Email
1 Project Team	Security Engineer Lead	Jacinta Bailey	jbailey@stackarmor.com
	Security Analyst Lead	Sachendra Karmacharya	skarmacharya@stackarmor.com
	Compliance Consultant	Kristen Page	kpage@stackarmor.com
	Backup Engineer	Aaron Molina	amolina@stackarmor.com
2 Engagement Management Team	Engagement Manager (EM)	Vy Nguyen	vnguyen@stackarmor.com
	EM Backup (e.g. PTO coverage)	ID'd as needed	will be shared As needed
3 Director/Sr. Director Team	Sr Director of Cloud Ops – Oversees analysts & engineers	Chad Buckhaults	cbuckhaults@stackarmor.com
	or - Director of Cloud Ops	Ryan Mishoe	rmishoe@stackarmor.com
	Sr Director Cloud Solutions/CX, Oversees EMs	Sarah Hensley	shensley@stackarmor.com
	Sr Director of Cybersecurity & Compliance	Rene-Claude Tshiteya	rtshiteya@stackarmor.com
	or - Director of Compliance	Tony Steiner	tsteiner@stackarmor.com
4 Chief Team	Chief Delivery Officer (CDO) - Oversees all Customer Engagements	Dave Musci	dmusci@stackarmor.com
	Chief Information Security Officer (CISO) - Oversees Risk and Compliance Efforts	Johann Dettweiler	jdettweiler@stackarmor.com
	Chief Solutions Officer (CSO) - Oversees Solution Offerings	Martin Rieger	mreiger@stackarmor.com

*Teams are encouraged to use shared collaboration/chat channels such as Slack if available on a project.

1



Issue Escalation Matrix for ConMon Engagements

Type of Issue Escalation	Level 1 Escalation	Level 2 Escalation	Level 3 Escalation	Level 4 Escalation
Operational Team/Role	Project Team	Engagement Management Team	Director/Senior Director Team	Chief Team
SecOps day-to-day Operational Issues	Assesses and addresses immediate SecOps issues, first line for day-to-day tactical troubleshooting (Analysts, Engineers)	Primary POC - Provides engagement oversight, additional logistics support and administrative support including reach-back if needed, supporting the team in tactical solution delivery (EM)	Establishes programs, resources projects, and provides guidance to the teams for issues the team is unable to resolve, implements strategic and proactive solutions at the program level (Sr Dir of Cloud Solutions)	Establishes strategic vision for delivery teams, provides leadership to directors and senior directors, and ensures delivery is aligned with vision (CDO)
Compliance Issues	Analyzes, researches as necessary, and advises on issues involving regulatory compliance (Compliance Consultants)	Provides engagement oversight, logistics and administrative support and issue tracking related to compliance issues (EM)	Establishes programs, resources projects, and provides SME guidance to the compliance teams and customers for ambiguous or complex compliance issues (Sr Dir of Cybersecurity and Compliance)	Establishes strategic vision and approach to the interpretation and implementation of compliance controls across the company, and provides thought leadership on all things compliance (CISO)
Incident Issues	Identifies, triages, gathers information on, and initiates incident response activities (Analysts, Engineers, Compliance Consultants)	Provides engagement oversight, supports incident response activities that are administrative tasks and helps coordinate communications across teams (EM)	Establishes processes and provides guidance and oversight for incident management, and ensures teams adhere to all system plans and analyzing the incident on a broader scale (Sr Dir of Cloud Solutions)	Establishes strategic vision and approach to the interpretation and implementation of compliance controls across the company (CDO)
Contract or SOW Issues	Delivers services aligned to the SOW (Analysts, Engineers, Compliance Consultants)	Interprets and ensures service delivery is aligned to the current SOW (EM)	Establishes programs and processes to deliver against contracts, provides reach-back support and input into contracts as well as issue resolution, change requests involving scope variations, and renewals (Dir of Cloud Solutions)	Establishes offerings, service delivery guardrails, and pricing models aligned to the company vision, and incorporates into contract language. (CSO)

Figure 2. – Issue Escalation Matrix for Common Issue Types

2

Established SOP Library and Template

Established SOP library and simple SOP template for EM team to help standardize customer engagement management for common or complex tasks.

- The first 2 SOPs are for **terminating a customer contract** and **transitioning a team member on/off a project**.
- The EM SOP library is in the CX/EX Intranet Portal.

The image displays three overlapping screenshots of a Service Delivery SOP document. The top document shows the 'Team Member Transition Checklist' section, which includes a paragraph about managing team members and a 'Document History' table. The middle document shows the 'Contents' section with a table of contents. The bottom document shows the 'Transition Pre Work' section, which includes a checklist for resource assignment, customer communication, access requests, environment overview, compliance, and creation of access of modification.

Service Delivery SOP
SOP: Team Member Transition (onto a new project)

Team Member Transition Checklist

Managing team members assigned to projects is a collaborative effort and requires careful consideration of the many variables impacted by a change. Additionally, all changes to team members need to be communicated with the customer, preferably in a collaborative manner that will be perceived by customers as beneficial.

Document History

Version	Date
Draft 1	Mar 27, 2025

Contents:

Team Member Transition Checklist	1
Transition Pre Work	3
Transition	3

Service Delivery SOP
SOP: Team Member Transition (onto a new project)

Transition Pre Work

- Resource Assignment Collaboration**
 - ☐ Meet and review staffing change with line managers, consider customer needs, team member wants, team member skills, and impacts to other engagements that may be impacted.

Transition

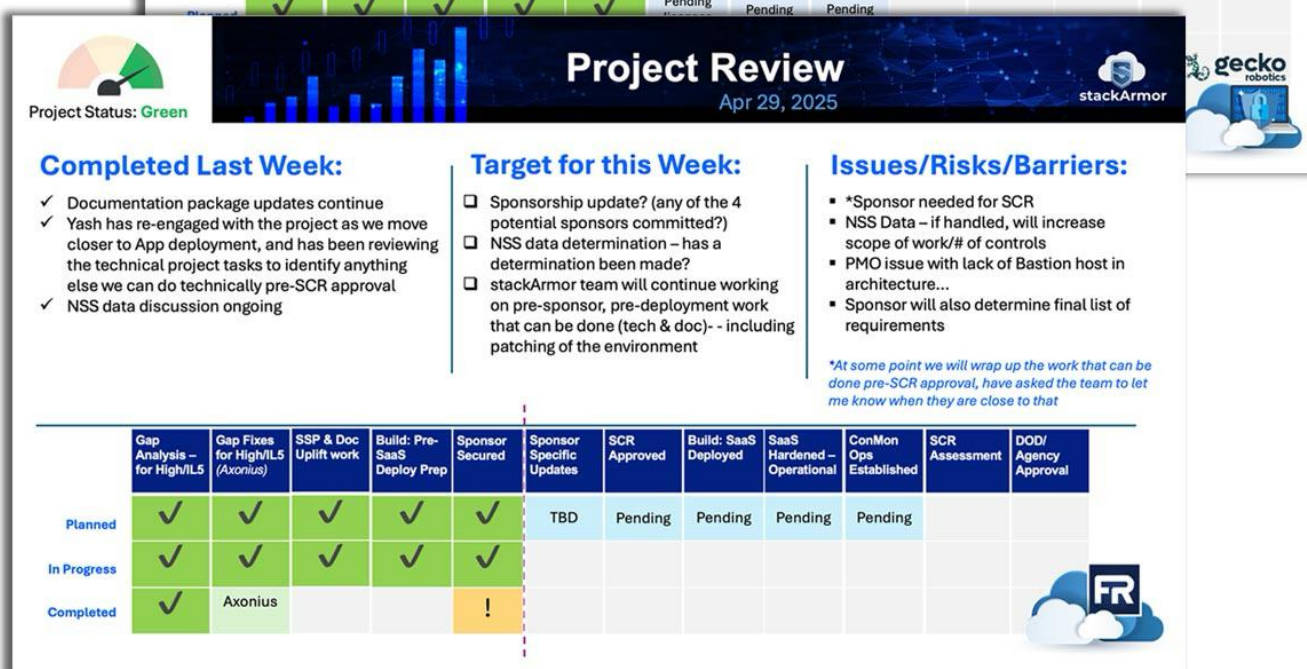
- Customer communication**
 - ☐ Send a message to the customer POC confirming the transition (who and timeline). This message should always follow an actual conversation with the customer and ensures there are no issues before starting the access process.
- Invitation to the Internal Meetings/Communication chains**
 - ☐ Invite team member to the internal/external ConMon Meetings.
 - ☐ Invite team member to the internal/external Slack channels.
 - ☐ Provide information for SharePoint / Box Access for the project.
- Access Requests (Engineer/Analyst)**
 - ☐ Create Gitlab new user access modification ticket
 - ☐ Ticket approved - Access to the applications in the environment.
 - ☐ Appgate
 - ☐ Gitlab
 - ☐ Splunk
 - ☐ TSW
 - ☐ DSM
 - ☐ Nessus
 - ☐ AWS (Identity Center controlled out of master account) - Customer will need to assist.
 - ☐ Yubikey, if needed
- Environment Overview**
 - ☐ Engineer/Analyst to walk through the environment with new team member.
 - ☐ Engineer/Analyst to walk through the items they are working on now/project specifics.
 - ☐ Engineer/Analyst to give insight on things they need to be aware of, such as:
 - ☐ Understanding of the SLA timeframes.
 - ☐ How patching is handled, etc.
 - ☐ Typical customer requirements.
- Compliance**
 - ☐ Gitlab ticket should have the requirements needed.
- Creation of Access of Modification, if applicable (TBD)**
 - ☐ Removal of team member.

3

Supported Multiple Customers as a Prime EM

Supported multiple projects as the EM, and created a Quad type of weekly project review used on those (and now by others).

- Am/was the primary EM on Gecko, Qanapi, Axonius (before transitioning to Mike B.), and Co-EM on Rally and Clarity for ConMon operations.
- Expanded my skills with SmartSheet to support these
- Learned many things about the details of delivery and SecOps ☺
- Gecko, specifically, expressed that they “loved” this report



Created a Role Based Training Template for Gecko

Created a role-based training template for Gecko to help them establish their own internal training program to meet compliance requirements.

- I used the template I made for stackArmor, and swapped out images (and colors) from Gecko's website
- Created a final attestation page as well with a Gecko training logo
- It's these little things that can really matter 😊

Gecko Robotics | Role Based Training

Training Topic Here
Date: May 22, 2025

Target Roles:

- **Role 1, Role 2**
Any company roles who <include activity for which this training is aimed>
- **Role 3, Role 4**
Any company roles who <include activity for which this training is aimed>
- **Role 5, Role 6**
Any company roles who <include activity for which this training is aimed>

Training Objectives

- Objective 1
- Objective 2
- Objective 3

Guiding NIST 800-53 Controls

Primary:

- **CM-3 (example)** – Configuration Change Control – Requires a change management and control process, with **part d** focused specifically on implementing changes to a production environment.

Secondary (related controls):

- **CM-5 (5)** – Access Restrictions for Change – Privilege Limitation for Production and Operation related to those allowed to make system changes (must be reviewed quarterly).
- **CM-9** – Configuration Management Plan, which describes how system components or configuration items (CI) are brought under control (updated annually or as needed).
- **SA-10** – Developer Configuration Management – Requires the developer of the system or its components to follow similar change control guidelines.

Training Agenda

- Control Review - NIST 800-53 guidance (if applicable)
- Review of System Specific Implementation Details (from System SSP)
- Training Topic 1
 - Training Topic 1a
 - Training Topic 1b
- Training Topic 2
- Next steps

System Specific Implementation Approach
(Things that matter as stated in the System SSP)

Include any implementation statement details or procedures that might apply, and that the trainees need to be familiar with.

Topic 1

SubTopic 1a

- Content
- Content

SubTopic 1b

- Content
- Content

Thursday, August 7, 2025

Training Summary

- Key takeaway 1
- Key takeaway 2
- Key takeaway 3

August 7, 2025

Questions?

<Topic> Role-Base Training: Certificate of Completion

This certificate serves as attestation that I have completed the <topic> role-based training course – and that I understand and will incorporate the information presented in the training as I perform my job duties.

Name: _____

Title/Role: _____

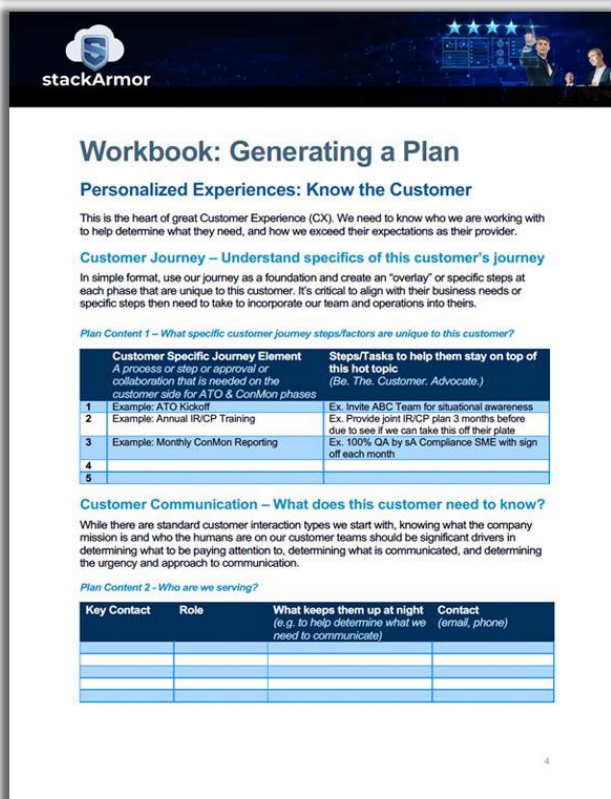
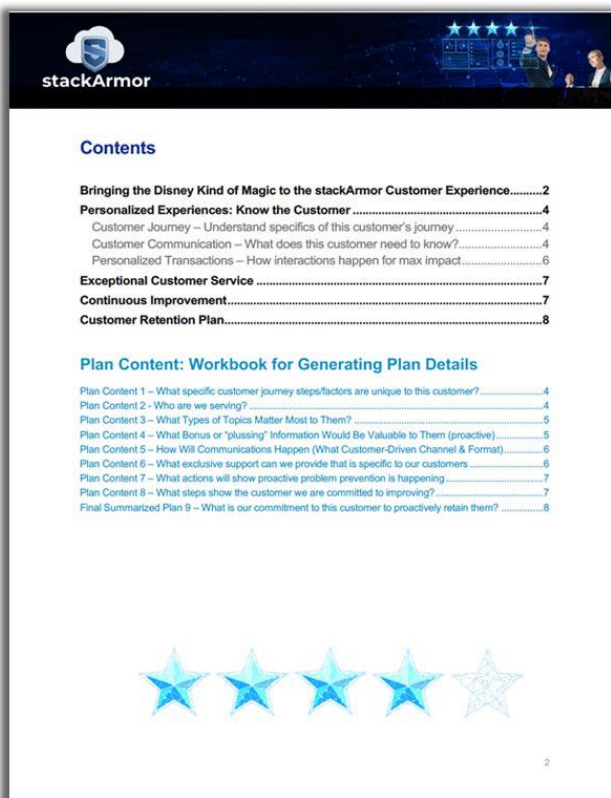
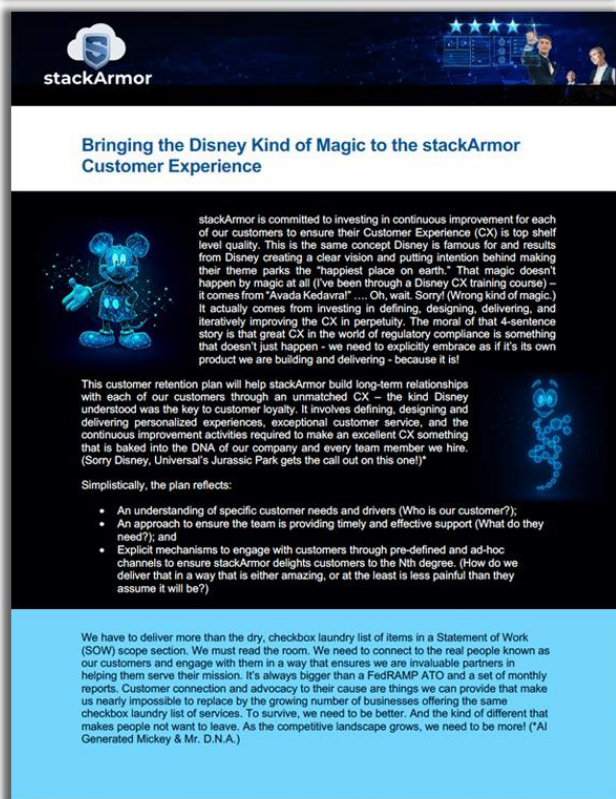
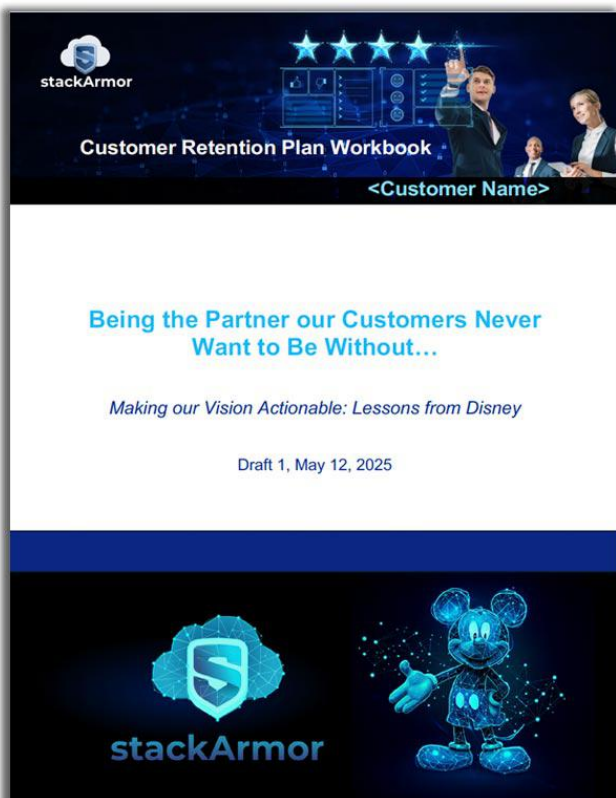
Date: _____

Signature _____

Established an EM Customer Retention Plan Program

Developed a structured Customer Retention Plan program and workbook for the EMs to implement with all of their customers – taking a proactive approach to customer stickiness.

- Presented the program at the team meeting we had at the Tyto office.
- Combined the program with a mini training on customer success management – the Disney way! ☺
- Program is relatively new – still working through how we hold ourselves accountable.



Customer Retention Plan Program Cont... Last page is the actual simple “plan” for each customer and is the output from working through the workbook.

Plan Content 3 – What Types of Topics Matter Most to Them?

	Customer “Hot Topic” <i>Not the one at the mall, the high priority topic(s) that matter most to the customer(s) – can be info or task centric</i>	Steps/Tasks to help them stay on top of this hot topic <i>(Be. The. Customer. Advocate.)</i>
1		
2		
3		
4		
5		

Plan Content 4 – What Bonus or “plussing” Information Would Be Valuable to Them (proactive)
(Topics reflect proactive, above and beyond communications/support (we can’t take all the bad away from an effort, but we can make this whole process less painful than they expect it to be... another Disney CX concept)) – also, Plussing is a Disney term for going beyond what’s required to surprise and delight your customers

	Above and Beyond Topics for Customer <i>Topics that would matter to this customer that they may not ever realize they need to know about or be on top of.</i>	Steps/Tasks to provide proactive communication, or unsolicited support <i>(What we want to share that they may not even know to ask for.)</i>
1		
2		
3		
4		
5		

5

Personalized Transactions – How interactions happen for max impact

Communications (e.g. messages, deliverables, ad hoc conversations) should be tailored based on customer/individual preference as much as is reasonable to do so, and should be valuable/helpful to them. If we don’t know what they want to see/hear and/or who they want to see/hear it from, we need to ask them and/or help them figure it out. Need a win-win.

Plan Content 5 – How Will Communications Happen (What Customer-Driven Channel & Format)

	Communication Types <i>What types of communication are needed with this customer, or NOT desired?</i>	How this Happens <i>(The format and channel)</i>
1	Example: Weekly Project Updates	Ex. pptx slide(s) reviewed by EM on weekly recurring video call
2	Example: Weekly ConMon Reviews	Ex. .docx Report reviewed by Analyst Lead at weekly recurring video call, with EM taking and posting all notes and managing task tracking.
3	Example: Changes to Certain Regulations	Ex. Monthly Newsletter for general changes, Slack AND email notification and description for time-sensitive or changes highly relevant to this customer
4	Example: Issue Resolution	Ex. A. All information will be shared by the leads only and provided in the context that the customer is in charge and needs to approve any resolution steps. B. The team will hold a project-specific brown bag to discuss the tone and tenor of communications (e.g. this is their system, not our system)
5		

Plan Content 6 – What exclusive support can we provide that is specific to our customers

	Exclusive Support Types <i>What types of exclusive support or content?</i>	How this Happens <i>(The format and channel)</i>
1	Example: Updates on FedRAMP 20x program changes	Ex. Exclusive customer newsletter
2	Example: FedRAMP Training	Ex. Exclusive training sessions on the FedRAMP program – like a brown bag for customers
3		
4		
5		

6

Exceptional Customer Service

Plan Content 7 – What actions will show proactive problem prevention is happening

	Proactive Activity <i>What will we do to let them see our proactive participation in their success?</i>	How this Happens <i>(The format and channel)</i>
1	Share topics that may become problems for them	Ex. To-Be-Designed Monthly “Things to Think About” customer specific report
2	Provide reminders of recurring (bi-annually or annual) compliance controls that they must be on top of	Ex. Establish shared “calendar” or tracker in Slack for Quarterly and annual ConMon requirements (e.g. signing ROB, IR/CP, Reviewing Documentation – and set up notifications for them
3	Iteratively review their responsibilities with them to see if they need help	Create calendar reminder (in Slack) to explicitly ask them, as a part of a named “quarterly support check” as an example, how they are doing with items to-be determined (e.g. ISSM ticket reviews, approvals, Supply Chain vendor management, etc.)
4	Equip customers to learn, grow	Provide role-based training that has a win-win for us and them (e.g. GitLab ticket best practices)
5		

Continuous Improvement

Plan Content 8 – What steps show the customer we are committed to improving?

	Continuous Improvement Activity <i>What?</i>	How this Happens <i>(The format and channel)</i>
1	Customer Satisfaction Surveys	Send the link to the NPS survey once every 6 years to key customer team members
2	Acquire and maintain updated NPS	Assertively encourage customers to complete the survey
3	Customer Input Elicitation	Add a standing question for monthly meetings to explicitly ask the customer what they’d like to see from our team that would improve their experience? Or Customer Advisory Board involvement
4	Share technology capabilities or enhancements on a recurring basis and as needed	Add section to monthly internal newsletter highlighting our proprietary capabilities with clear description of how this benefits customers
5		

7

Customer Retention Plan for <Customer Name>

The following activities will be undertaken, tracked, and reported on quarterly as we mature our explicit approach to managing customer satisfaction and delivering a delightful Customer Experience (CX).

Final Summarized Plan 9 – What is our commitment to this customer to proactively retain them?

	Proactive Retention Activity <i>What are we doing to ensure a “sticky” customer experience</i>	Details/How
1		
2		
3		
4		
5		
6		
7		
8		

8

Created EM Onboarding | Role Based Training

Built out an EM Onboarding Role-Based Training for new EMs to standardize and clarify the job of the EMs at stackArmor.

- Put this training to the test with both Mike B and Shawn B to help ensure their successful onboarding
- Used the template I created for Armory (stackArmor) Role Based Training.
- EM-Role-Based-Training-EM-Onboarding-April2025.pptx.

Let's Grow! 

Engagement Management (EM) Role Based Training

EM Onboarding Training



stackAcademy

Proprietary and Confidential

 **Target Role(s):**

- **Engagement Managers**
Any person playing the role of Engagement Manager, Project Manager, or Service Delivery Manager on stackArmor customer engagements

Training Objectives

- Intro to stackArmor Offerings (Under Development)
- Establish Awareness of the Mission and Vision and EM Practice Team
 - Understand the "core" team members with whom the EM will interact
- Understand the end-to-end customer journey for stackArmor engagements (Sales > Authorization > ConMon)
- Understand the role of Engagement Managers across each phase of the end-to-end journey
 - Activities
 - Tools
 - Templates/Resources
- Understand EM Best Practices
- Understand the Path Forward

August 3, 2025 Proprietary and Confidential

 **Engagement Management Practice**

Mission:
To put cutting-edge cloud solutions into the hands of government, educational, and critical infrastructure organizations by accelerating the path to cybersecurity compliance for CSPs.

Vision:
To be THE trusted leader for cybersecurity and compliance advisory and acceleration solutions – and the partner our customers never want to be without.

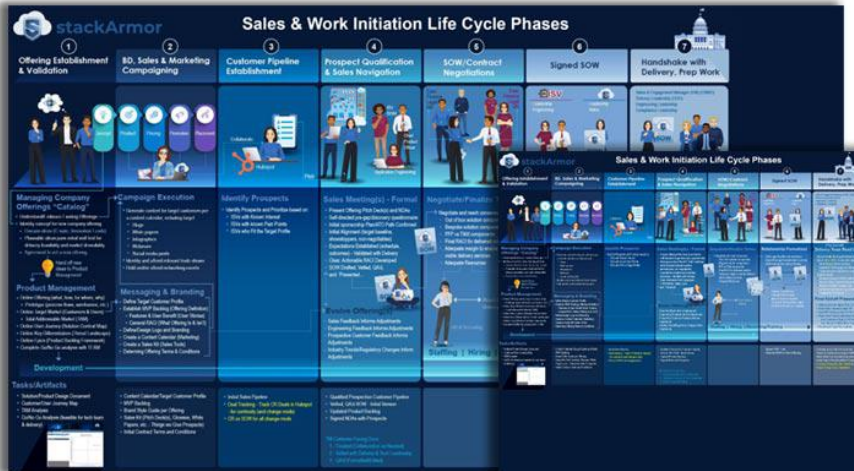
 4

Engagement Management Core Team

- **Dave Musci** – Chief Delivery Officer
 - **Sarah Hensley** – Sr. Director of Cloud Solutions
 - Amal Abughannam – Senior Engagement Manager
 - Vy Nguyen – Engagement Manager
 - Mike Brigantic – Engagement Manager (starts Apr 7)
 - Shawn Bessey – Jr. Engagement Manager (starts Apr 21)
- **Ryan Mishoe** – Director of Cloud Operations
 - Jennifer Miller – Solution Delivery Manager (a type of EM)
- **Chad Buckhaults** – Sr. Director of Cloud Solutions

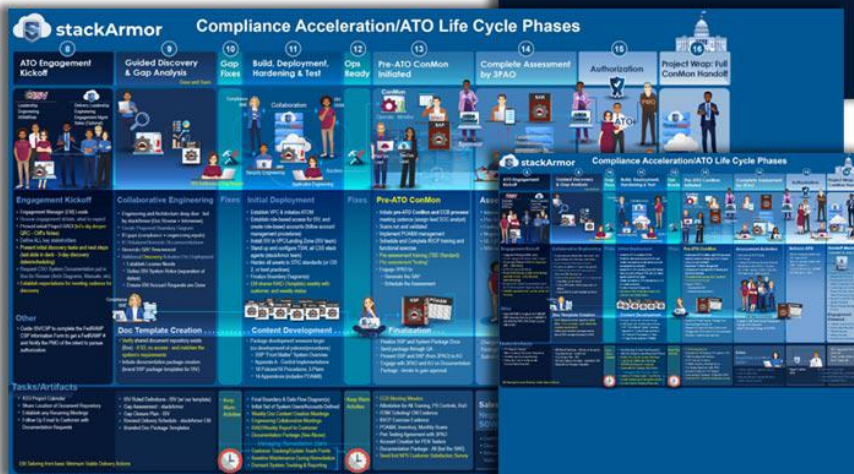
Sunday, August 3, 2025 Let's Grow!  5

Engagement Management Onboarding | Role Based Training cont...



Sales Phase and the EM

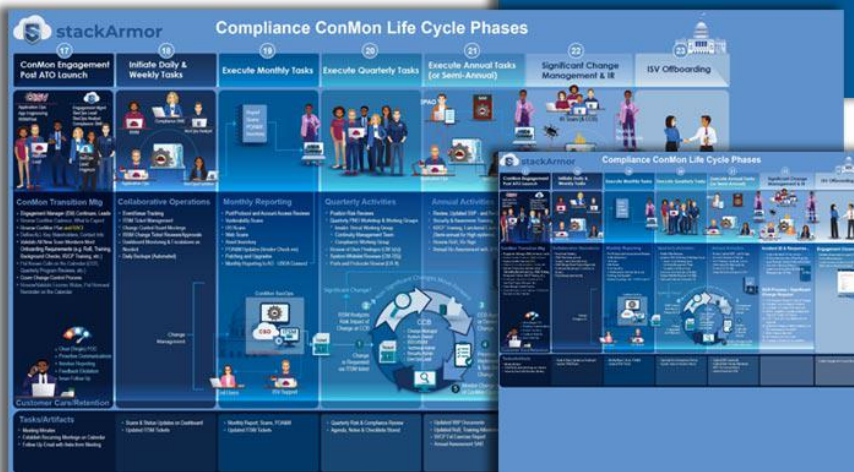
The Sales Phase of the end-to-end journey has the least impact to the Engagement Manager. However, given that the Engagement Manager is the primary point of contact throughout the life of an engagement, they are in a unique position to identify new sales opportunities and to provide lessons learned to the sales team with regard to Statement of Work (SOW) or contract improvements.



ATO Phase and the EM (Also called "Delivery" at stackArmor)

The ATO Phase of the end-to-end journey, often referred to as "delivery" at stackArmor, requires a significant investment from the EM. The EM will take full ownership over the engagement in terms of making sure:

- The project work aligns with the SOW.
- The project team is aware of any pressing issues or project nuances.
- The team has appropriate resources, and those resources charge appropriately.
- The project teams are trained and fully leveraging our latest tech/automation/processes.
- The project team stays on schedule for required tasks.
- The customer is kept fully informed and engaged in the process (weekly meetings, Slack, email, weekly reports, project plan updates, etc.)



ConMon Phase and the EM (Also called "SecOps" at stackArmor)

The ConMon (ongoing) Phase of the end-to-end journey, also referred to as "SecOps" at stackArmor, is less about traditional project management as these are continuous tasks rather than linear, milestone-centric tasks. Given the prescriptive nature of compliance management, there are still plenty of things to manage, including:

- Representing the Customer's Needs – managing and tracking both internal and external team communications (ensuring a workable cadence to keep the customer engaged and informed in perpetuity for the life of the engagement.)
- Ensuring key milestones are met (monthly, quarterly, semi-annual, annual tasks.)
- The project teams are trained and fully leveraging our latest tech/automation/processes.
- Keeping a pulse on the customer's experience and satisfaction including explicit feedback requests on a periodic (maybe quarterly) basis.
- Working with sales to proactively identify additional value-add services we could provide.

For actionable details:

Engagement Management Playbook

This resource was created to help specify the job tasks associated with Engagement Management at each step in the end-to-end customer journey.

This is a working document will evolve with lessons learned and new ideas.



CX/EX SharePoint Portal: More Resources

The CX/EX SharePoint Portal is a New Portal

- Part of stackArmor's commitment to improving both the customer and employee experience – knowing the 2 are interrelated.
- This is evidence of a vision and is increasingly evidence of vision realized as we continue to evolve the site and content.
- The goal is to provide more easily consumable content for employees (with extension to customers) based on known areas where we need to improve and standardize delivery. It's designed to hold things like:
 - Document and report templates
 - Training modules for role-based training topics
 - Guidance
 - Operating procedures

... link to an employee Idea Tank to encourage ... feedback.

... nt.us/sites/Customer-and-Employee-Experience-CX-EX



EM Best Practices: Soft Skills bring Solid Results

- Communicate clearly, early and often – using both informal and formal channels, consistently providing meeting agendas and notes, and following up on verbal conversations with written re-caps.
- Build trust across teams by paying attention, showing up prepared, and having integrity in following up on promises.
- Manage change and uncertainty with empathy – remembering our customers are putting tremendous trust in us for one of their biggest commitments and are often under great stress themselves.
- Navigate competing priorities and personalities with patience, insight and self awareness.
- Lead with influence, not authority.

Employee Specific Plans

We'll start with a plan, and remain open to altering course as it makes sense

Target Project Assignments

- **Project 1** – <Description of target project>
- **Project 2** – <Description of target project>
- **Project 3** – <Description of target project>
- **Project 4** – <Description of target project>

Target Project Assignments

- **Project 1**
- **Project 2**
- **Project 3**
- **Project 4**

Path Forward

1. Nothing is set in stone, and new ideas are encouraged.
2. We will figure all these out together, and tackle as a team, allowing you to build a comfort level before being expected to take charge.
3. The team will start inviting you to existing meetings and start to identify tasks on each project that make the most sense to start partially or fully handing off.
4. You are free to learn in the way that works best – so please think about and communicate what works for you in terms of the amount of guidance and direction you prefer as we go. (The goal is to allow you to be fully independent as quickly as you are comfortable.)
5. I'm here to help you be successful, make this a place you can grow, and remove things getting in your way – fully leveraging your potential.

Let's Grow!

Homework

- ☐ Review the Engagement Management Playbook - Track questions for review with team
- ☐ Review the end-to-end journey maps - Track questions for review with team
- ☐ Review the CX/EX SharePoint Site - Track questions for review with team
- ☐ As we provide project artifacts, review and as with the others - Track questions for review with team


As you start reviewing information, you will have many question. Just write them down, and make sure to share them during meetings with your mentor or team members.

Customer/User/Employee Experience

Established a Customer Newsletter

To address feedback of not being proactive enough and to increase our value/stickiness, I designed a monthly/bi-monthly customer newsletter we now share.

- I generated or selected/collaboratively edited all content for the first few – leveraging some Johann posts for certain sections.
- Created many customer illustrations, including **one of Johann (below)** for the CISO section! lol ☺
- We actually got positive feedback on the delivery of the 3rd, with Gecko commenting "Thanks for this Sarah - my account team at Vanta provided similar comments... **Their info was not nearly as well outlined though.**"



stackArmor 411
Keeping You in the Know
stackArmor Newsletter ed. 1 | April 2025

stackArmor Updates | FedRAMP 20X Changes

In this newsletter we want to share with you updates within the FedRAMP eco-system especially around the FedRAMP 20X program as well as stackArmor's continuous efforts to drive innovation.

1 - Impact to Marketplace Listings

The Federal Risk and Authorization Management Program (FedRAMP) has recently published some changes to their handling of FedRAMP Marketplace designations, primarily impacting Cloud Service Providers (CSPs) who have lost their only ATO on file. These changes are consistent with the FedRAMP 20x position that Agency sponsorship is currently the only path to ATO.

With the recent disbandment of the Joint Authorization Board (JAB) and Agency budget cutbacks, some CSPs may find themselves in a situation where they no longer have an Agency or government entity providing the required sponsorship oversight over a system's continuous monitoring (ConMon) activities. According to the announcement, FedRAMP Authorized cloud service offerings (CSOs) without an active agency authorization to operate (ATO) may remain in the FedRAMP Marketplace as FedRAMP Authorized if those CSOs:

- **Submit Monthly ConMon Deliverables**
CSPs must maintain an acceptable risk posture and continue to upload monthly ConMon deliverables (updated POA&M and inventory, scan files, deviation requests) to their FedRAMP secure repository.
- **Conduct an Annual Assessment**
If a service offering is due for an Annual Assessment during this period, the CSP will still need to complete the Annual Assessment.
- **Deliver a Risk Briefing**
The CSP will need to brief any agency looking to use your cloud solution on the current risk posture of the CSO, with a focus on any areas that require agency risk acceptance (e.g. Unresolved Findings with Vendor or Operational Dependencies as an example.)

stackArmor is your trusted partner in all things FedRAMP and cybersecurity compliance. Let us know what we can do to help!

stackArmor www.stackarmor.com



Note to be added to the Marketplace Listing for CSO ATOs without a sponsor:
For these CSOs, there will be a note added to your Marketplace listing that says something like the following: "This cloud service offering lacks continuous monitoring oversight from FedRAMP or any federal agency. Agencies considering using this service should review the Cloud Service Provider's security documentation in their secure repository, directly coordinate with the CSP and conduct their own evaluation before making an Authority to Operate (ATO) decision. Once an agency issues an ATO, agencies should submit their ATO letters to FedRAMP."

2 - Analysis of FedRAMP 20X Changes

In addition to the Marketplace listing changes already mentioned, stackArmor's experts have developed a simple easy to use information resource to help customer understand what else is changing and how they might stay abreast of these changes. Please see the attached addendum.

3 - Growing the stackArmor Team of Experts

We have continued to invest in our people to improve our service delivery and improve our ability to meet our customers' FedRAMP related questions and concerns. We are very excited to announce the joining of Michael Brigranic and Rene Tibshley who were formerly with the FedRAMP PMO supporting agency reviews. Mike joins our growing team of engagement managers who focus on excellence in the delivery of FedRAMP compliance acceleration and cybersecurity engineering services, while Rene brings his subject matter expertise to our compliance advisory and operations team.

Don't Miss our 2025 FedRAMP Updates Webinar

stackArmor has teamed up with Carahsoft, the leader in public sector cloud solutions for federal and public sector organizations, to provide an exclusive webinar that will showcase how commercial ISVs as well as federal agencies can take actionable steps to meet new and emerging federal cybersecurity mandates including assessing AI systems risk.

Register for [this webinar](#) | Topics include:

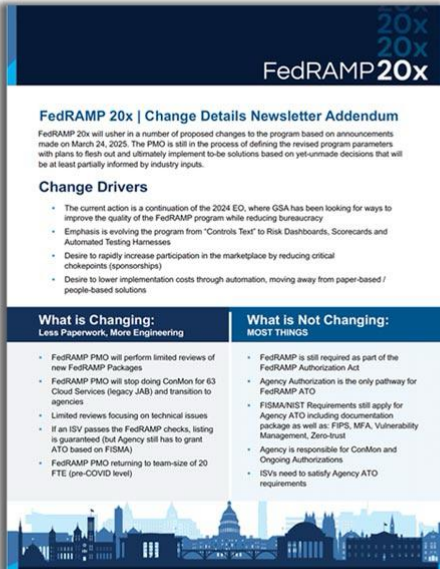
- Developing and managing digital compliance artifacts using OSCAL
- Using SBOMs and ABOMs to track systemic risk
- Implementing a highly automated continuous monitoring program

Speakers & Agenda:

- 5-Minute Introduction from Josh Dries (Head of ISV at Google Public Sector) about Google Public Sector
- 15-Minutes from Johann Dettweiler, stackArmor CISO on the Announcements and updates to FedRAMP 20x
- 15-Minutes from Kenny Scott (Paramity CEO) on Paramity and OSCAL
- 15-Minutes from Rick Henry (Lineaje CISO) on Lineaje and SBOM/ABOM and BOMBOTS!
- 10-Minutes of Panel QA with Johann as the MC

May 14, 2025
1:00-2:00 pm EST
Online
[Register](#)

stackArmor **carahsoft** **Paramity** **LINEAJE**




FedRAMP 20x | Change Details Newsletter Addendum

FedRAMP 20x will usher in a number of proposed changes to the program based on announcements made on March 24, 2025. The PMO is still in the process of defining the revised program parameters with plans to flesh out and ultimately implement to-be solutions based on yet-unmade decisions that will be at least partially informed by industry inputs.

Change Drivers

- The current action is a continuation of the 2024 EO, where GSA has been looking for ways to improve the quality of the FedRAMP program while reducing bureaucracy
- Emphasis is evolving the program from "Controls Text" to Risk Dashboards, Scorecards and Automated Testing Harnesses
- Desire to rapidly increase participation in the marketplace by reducing critical chokepoints (sponsorships)
- Desire to lower implementation costs through automation, moving away from paper-based / people-based solutions

What is Changing: Less Paperwork, More Engineering	What is Not Changing: MOST THINGS
<ul style="list-style-type: none">• FedRAMP PMO will perform limited reviews of new FedRAMP Packages• FedRAMP PMO will stop doing ConMon for 63 Cloud Services (legacy JAB) and transition to agencies• Limited reviews focusing on technical issues• If an ISV passes the FedRAMP checks, listing is guaranteed (but Agency still has to grant ATO based on FISMA)• FedRAMP PMO returning to team-size of 20 FTE (pre-COVID level)	<ul style="list-style-type: none">• FedRAMP is still required as part of the FedRAMP Authorization Act• Agency Authorization is the only pathway for FedRAMP ATO• FISMA/NIST Requirements still apply for Agency ATO including documentation package as well as: FIPS, MFA, Vulnerability Management, Zero-trust• Agency is responsible for ConMon and Ongoing Authorizations• ISVs need to satisfy Agency ATO requirements



The FedRAMP 20x Program Change Process

To work through to-be and proposed changes and establish new parameters and requirements for the FedRAMP program, the FedRAMP PMO will:

1. Leverage 4 community working groups to gather input on key topics including Rev. 5 Controls Monitoring, Automating Assessments, Applying Existing Frameworks, and Continuous Reporting
2. Share work products throughout the working group effort using GitHub
3. Propose models where "sponsorship" is not required to get listed in the marketplace
4. Go through public comment process
5. OMB review and CIO Council review
6. Communicate changes to Agencies and industry
7. Implement changes

*The scope of the proposed changes is limited to FedRAMP Low which is a very small fraction of workloads. Regardless, the change process will need to follow the approvals process as outlined above.

5 Things Cloud Service Providers (CSPs) Should Do

- CSPs should engage in the FedRAMP 20X working groups and stay abreast of the changes being considered and provide their input as necessary
- CSPs should evaluate current posture and review competitive landscape and explore differentiation strategies e.g. move to FedRAMP High or DOD IL-4/5
- CSPs with AI capabilities should move aggressively towards meeting FedRAMP requirements to take advantage of the accelerated pathway to delivering commercial software to agencies
- CSPs should continue to meet current guidance and requirements for Continuous Monitoring as agencies are still responsible for the ATO and meeting federal security requirements
- CSPs should be proactive in highlighting benefits, efficiencies and cost savings for government through the use of commercial capabilities.

Please send us an email to schedule an appointment to ask us any questions you might have around some of the changes associated with FedRAMP 20X.
info@stackarmor.com

stackArmor

Let the FedRAMP 20x Authorizations Begin!

July 15, 2024, the Office of Management and Budget (OMB) released [M-24-15](#) on Modernizing the Federal Risk and Authorization Management Program (FedRAMP). Much of the past year's FedRAMP initiatives have focused improving program efficiencies, defining "smarter" approach to vulnerability management, and evolving the cloud marketplace. The program had to figure out how to modernize and scale dramatically in order to get thousands of cloud solutions into the hands of government agencies at a pace that would far exceed the long, drawn out processes of years past. Exactly 1 year later, 4 cloud service offerings (CSOs) have received the very first FedRAMP 20x authorizations!

A quick recap of the FedRAMP 20x initiative:

- 4 months ago, FedRAMP launched 20x – a new approach to assessing and authorizing cloud services (at the low baseline) based on actual security outcomes.
- 3 months ago, FedRAMP released draft materials outlining how the 20x approach would work.
- 2 months ago, FedRAMP opened the 20x Phase One pilot and began testing and

FedRAMP 20x v Rev 5

So you might be wondering what the heck is FedRAMP 20x as compared to the standard FedRAMP Rev 5 baseline? Well, as exciting as 20x is, the more traditional FedRAMP Rev 5 isn't going away quite yet – and 20x isn't ready for prime time. FedRAMP 20x is an approach to authorization that involves cloud-native continuous security assessment that's as simple or complex as a cloud service offering needs for it to be – but *initially* is only being piloted for SaaS systems at a *low* baseline.

FedRAMP 20x:

- Emphasizes automated validation and continuous monitoring using machine-readable data.
- Leverages existing commercial security frameworks to reduce documentation burden.
- Utilizes an automated platform and APIs for submissions and validation.
- Focuses on Key Security Indicators (KSIs) to summarize security capabilities.
- Aims to streamline the authorization process and accelerate cloud service adoption.
- Includes a pilot program for FedRAMP Low authorization using KSIs and automated validation.

FedRAMP Rev 5:

- Relies heavily on document-based reviews and manual exchanges.
- Uses traditional, point-in-time security assessments.
- Requires extensive, often redundant, FedRAMP-specific documentation.
- Authorization is achieved through agency sponsorship and a lengthy process.
- Continuous monitoring relies on manual reporting and assessments.

A Quick Look at the Differences

Feature	FedRAMP 20x	FedRAMP Rev 5
Authorization:	• Direct to FedRAMP (pilot)	• Agency Sponsorship
Baseline(s):	• Low Only	• Low, Moderate, High
Assessment:	• 20x Assessment	• 3PAO: Full Assessment
Reporting:	• Automated	• Manual Reporting, Point in Time Reports
Cloud Service Offerings:	• SaaS with No/Minimal 3rd Party Connections	• IaaS, PaaS, and SaaS with More Complexity
Frameworks:	• Leverages Commercial Frameworks	• FedRAMP-specific Documents

Vulnerability Management is Evolving!

FedRAMP Request for Comment 0012 (RFC-0012)

Comments accepted until Aug 21, 2025

In support of the industry's move toward continuous vulnerability management and automated security operations, FedRAMP is asking for feedback on a newly proposed Continuous Vulnerability Management Standard. Comments are open to all!

The standard sheds a light on FedRAMP vulnerability management, with a shift toward a risk context rather than the current reliance on risk scores alone. The standard prioritizes realistically exploitable, the use of continuous reporting requirements, and the feature already designed and evolved.

Taken *directly from the draft standard*, the policy include the following:

- Defining new plain-language terminology.
- Including all weaknesses in the draft.
- Encouraging urgent mitigation of critical vulnerabilities.
- Establishing requirements for assessing severity.
- Directly defining potential adverse impacts.
- Prioritizing the discovery, mitigation, and remediation of vulnerabilities.
- Setting expectations for continuous monitoring and reporting.
- Requiring POAMs only when necessary.

FedRAMP 20x | Insights from our CISO



stackArmor CISO
[LinkedIn Profile](#)

stackArmor continues to engage with the FedRAMP PMO as thought leaders in the community forum and helping define the future of the program by bringing invaluable industry experience to the conversations. We continue to be excited about being a part of defining the future of the program.

We continue to keep our customers apprised of updates throughout the program's evolution. The following insights are from our own CISO, Johann Detweiler.

Johann Detweiler, CISSP, PMP

Heading in a Positive Direction

Whether 20X becomes the "accepted" route to non-sponsored FedRAMP authorization, it's still a step in the right direction. Regardless, the program is pushing systems towards autonomous understanding of systems around key security principles and requirements. Ultimately, that's a great thing.

20X could serve as an ideal way to demonstrate "Readiness"

What better way to demonstrate to agencies that your organization is prepared for the rigorous FedRAMP authorization than providing them access to a dashboard where system state is assessed in a manner that makes your systems near-real time security state completely transparent?

This program will change the way we assess systems

Gone will be the days of your technical engineering team having to spend hours upon hours of hundreds of pieces of "evidence" that represent a single point in time. Instead, assessors will evaluate the scope and quality of your validation assertions and render verdicts on the system processes. Once "trust" is established, the assessment becomes as simple as a single machine-readable artifact.

While there is some confusion and perhaps and general hesitancy around 20X, I encourage Service Providers to embrace the program and dive in. You will never regret implementing the capabilities needed to understand key security aspects of your system's running state in an automated fashion.



Always Looking for Feedback and Ideas

As we continue our commitment to a stellar Customer Experience (CX) we will continue to ask for feedback from customers. Your feedback will be used to inform our continuous improvement initiatives, and shared with our product teams as needed to ensure our customers' voices are heard and reflected in our solution roadmap.

We are once again providing a link to our quick 3-question survey, which allows you to share what's working, what isn't, and what ideas you may have about things stackArmor could do differently. We look forward to getting your response, and plan to use the information to ensure we are hitting the mark!

Please Complete our Brief
3 Question Survey

Link to Survey:

<https://app.smartsheet.com/b/form/034a95f17a0a433c886092ba950a8b89>

If you prefer to talk directly to someone at stackArmor to share your thoughts, our Sr. Director of Cloud Solutions, Sarah Hensley, is heading up our customer experience (CX) efforts and can be reached at sarah@stackarmor.com. Sarah is looking forward to working more closely with all our customers in the weeks and months ahead!

stackArmor 411

Keeping You in the Know

stackArmor Newsletter ed. 2 | May 2025

stackArmor is Now a Tyto Athene Company!

Lots of good things are happening! Just this month, Tyto Athene, a federal systems integrator of mission-focused digital transformation solutions (and portfolio company of Arlington Capital Partners), announced the acquisition of stackArmor, Inc.



"By combining the capabilities of Tyto and stackArmor, we're able to deliver secure and cost-efficient digital infrastructure that accelerates the mission of our government and defense customers through automation," said Gaurav "GP" Pat, Principal of stackArmor. "We share a deep commitment to public sector innovation, and we look forward to joining the Tyto family to propel business growth and operational excellence."

Better Together

Tyto connects government and defense leaders with technologies to seamlessly integrate and modernize enterprise-level operations, increasing mission resiliency, capability and flexibility for U.S. agencies around the globe. As a wholly-owned subsidiary, stackArmor will provide Tyto with industry-leading cloud strategy, migration and cloud managed services for regulated industries in compliance with FedRAMP, FISMA, CMMC, HIPAA, StateRAMP, CIIS and NIST standards. stackArmor will also provide its cyber automation and

Tyto / stackArmor FAQ

So what does this all mean for stackArmor customers? Rest assured, the recent acquisition means nothing but good things for our customers both today and moving together into the future.

Q: What does this mean for my system and business operations today?

A: This will not impact our day-to-day operations. In the near-term, expect business as usual.

Q: What will happen to the team assigned to my system?

A: There will be no changes to the current teams.

Q: What happens to "stackArmor"?

A: stackArmor will continue to be called stackArmor and will simply now be designated as a Tyto Athene company.

Q: How does this benefit me?

A: The investment by Tyto Athene means many improvements and expanded offerings, such as:

- **Greater Connections with Government and Public Sector Entities:** stackArmor is able to leverage Tyto Athene's extensive experience in serving federal DoD and Public Sector entities, improving our collective insights around serving those entities and making us a better advocate for our customers who serve them.
- **Accelerated Growth & Expanded Reach:** Joining Tyto Athene allows stackArmor to scale its industry-leading compliance and cloud solutions, better serving our customers and in turn - their customers.
- **Enhanced Resources & Support:** With Tyto's backing, stackArmor gains additional expertise and resources to innovate and refine its ThreatAlert platform and cyber automation tools, ensuring customers benefit from cutting-edge security and compliance solutions.

stackArmor Releases ThreatAlert Security Workbench 1.3

May saw the beginning of the rollout of ThreatAlert Security Workbench (TSW) 1.3. This release includes multiple changes that are a specific result of collaboration with the FedRAMP PMO in support of some of the new FedRAMP Rev. 5 requirements - specifically around the inclusion of compliance findings in the POA&M and more robust management and automation of all security and compliance findings. Findings in our systems are supported by stackArmor's proprietary Findings Lifecycle Manager (FLM). A quick overview of changes to this latest version include:

1. Task definitions that guide SecOps activities are now bundled into the TSW application (no longer require manual upload via the admin panel.) Customizations can be implemented under source control in GitLab. Refer to threatalert-configurations in GitLab for further information.
2. TSW now utilizes Python 3.11 and Django 5.1 - bringing numerous performance, feature and security improvements.
3. TSW now fully supports deployment on GCP compute VMs.
4. 3.1.0 additionally introduces three new integrations:
 - OpenSCAP Finding Lifecycle Manager (FLM) integration.
 - Tenable Web Application Scanner FLM integration.
 - Microsoft Defender for Cloud FLM integration.
5. TCS integration changes - this version implements a change to behavior of the ThreatAlert Container Scanner integration as a result of ongoing engagement with the FedRAMP PMO and clarification regarding their stance on C...

FedRAMP 20x | Insights from our CISO



Johann Detweiler, CISSP, PMP
stackArmor CISO
[LinkedIn Profile](#)

Positive changes are happening!

Since the release of FedRAMP 20x just one month ago, the PMO has already started to deliver on the promise of a faster authorization process. Regarding updates on agency authorized packages, the FedRAMP PMO has:

- Authorized 29 new cloud services (73 total this year), surpassing 400 authorized products.
- Granted seven new cloud services FedRAMP Ready designations (40 total this year), maintaining a clear queue for readiness assessment reports (RARs).



FedRAMP 20x

Our 2025 FedRAMP Updates Webinar is Almost Here!

stackArmor has teamed up with Carahsoft, the leader in public sector cloud solutions for federal and public sector organizations, to provide an exclusive webinar that will showcase how commercial ISVs as well as federal agencies can take actionable steps to meet new and emerging federal cybersecurity mandates including assessing AI systems risk.

Register for [this webinar](#). | Topics include:

- Developing and managing digital compliance artifacts using OSCAL
- Using SBOMs and AIBOMs to track systemic risk
- Implementing a highly automated continuous monitoring program



Speakers & Agenda:

- 5-Minute Introduction from Josh Dries (Head of ISV at Google Public Sector) about Google Public Sector
- 15-Minutes from Johann Detweiler, stackArmor CISO on the Armory and updates to FedRAMP 20x.
- 15-Minutes from Kenny Scott (Paramify CEO) on Paramify and OSCAL
- 15-Minutes from Nick Misty (Lineaje CISO) on Lineaje and SBOM/AIBOM and BOMBOTS!!!
- 10-Minutes of Panel QA with Johann as the MC

stackArmor carahsoft Paramify LINEAJE Google Public Sector

We want your feedback!

Earlier in 2025, we established a Customer Experience (CX) program to reflect our commitment to being a valuable partner in the cybersecurity and compliance engineering endeavors of our customers. In response to our initial feedback, we've already established more engagement management support, more training, and more direct feedback from customers to our product teams to ensure our customers' voices are heard and reflected in our solution roadmap.

That said, we are just getting started! Your feedback is invaluable in ensuring we continue to do more of what's working and adjust for what isn't. At the end of the day, your success is our success.

We want to invite you to take our quick 3-question survey, which allows you to share what's working, what isn't, and what ideas you may have about things stackArmor could do to. We look forward to getting your response, and plan to use the information as a part of our journey in continuous improvement.

Please Complete our Brief 3 Question Survey

Link to Survey:

<https://app.smartsheet.com/x/form/034d5517a0e433b866692ea92a2b89>

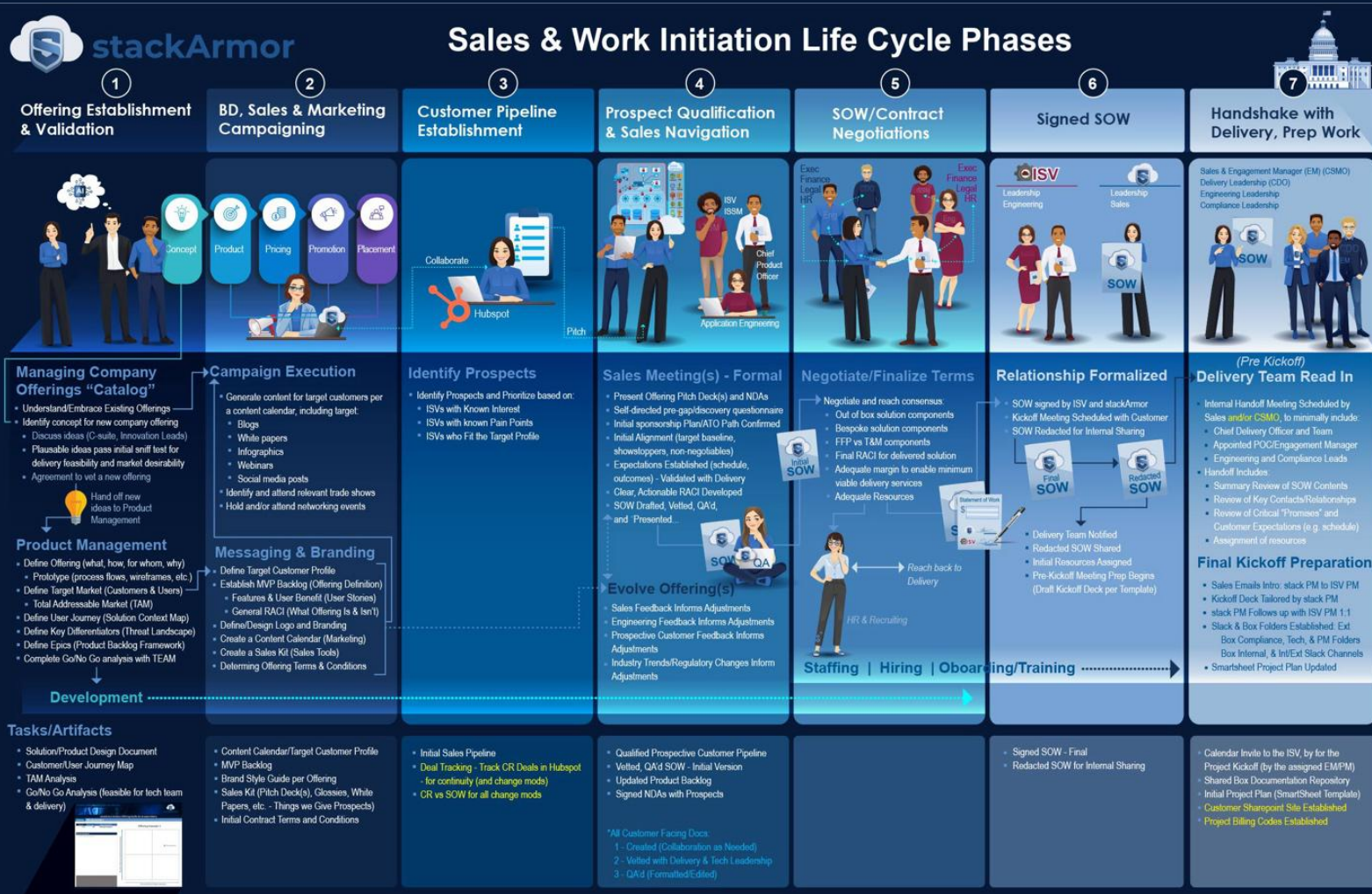
If you prefer to talk directly to someone at stackArmor to share your thoughts, our Sr. Director of Cloud Solutions, Sarah Hensley, is heading up our customer experience (CX) efforts and can be reached at sarah@stackarmor.com. Sarah is looking forward to working more closely with all our customers in the weeks and months ahead!

stackArmor

stackArmor Journey Map 1 | Sales Journey

Invested early in mapping out the customer journey, which is the foundation of managing and maturing all stackArmor operations across practice areas. This one is for sales/pre-delivery phases.

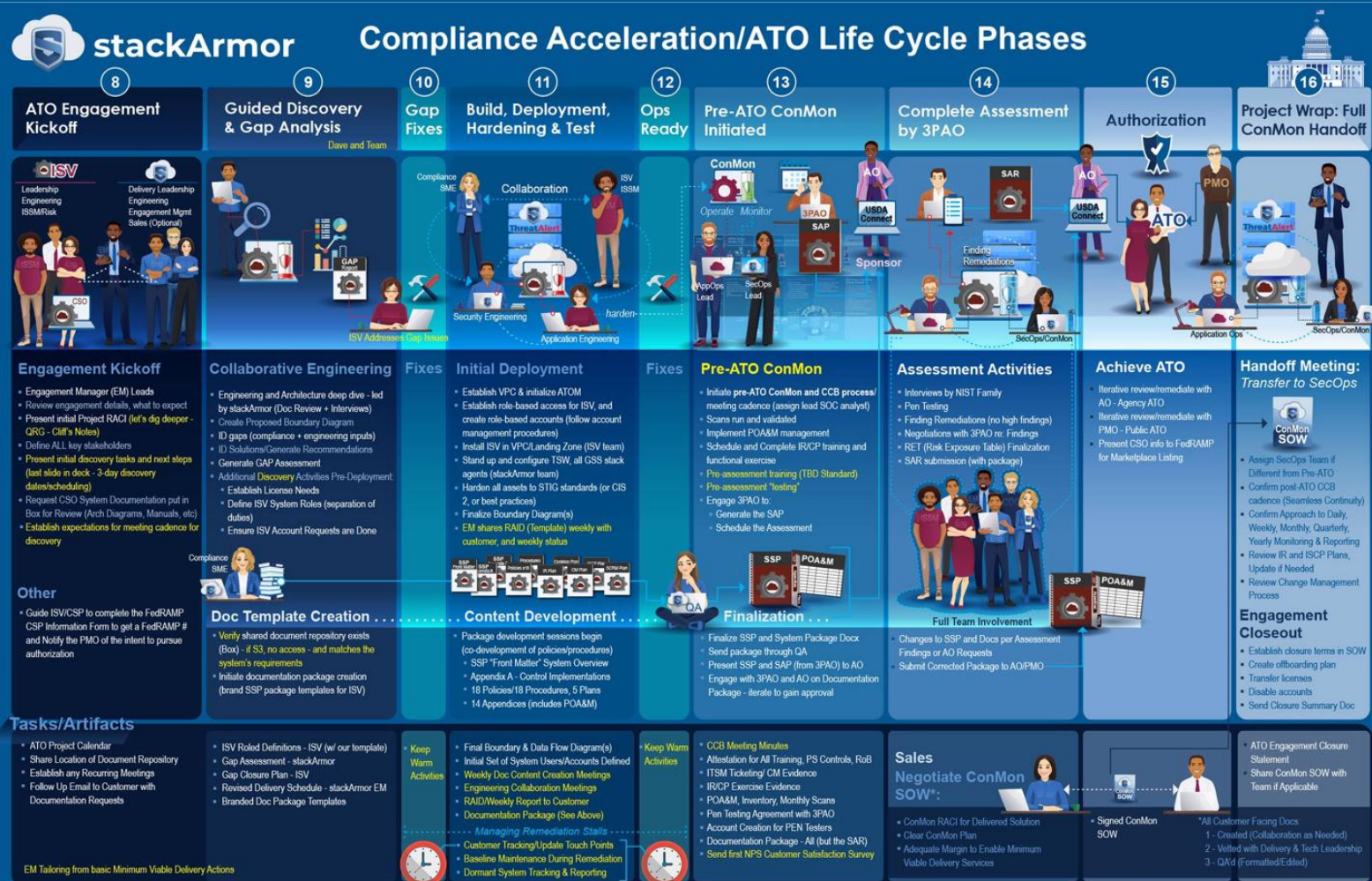
- This complex journey map identifies the “happy path” process, roles involved, activities that should occur, and artifacts created across the first 1/3 of the end-to-end customer journey.
- Map enables clear definition of roles/responsibility across teams, and activities all customers and team members can expect
- All journey maps are available on the CX/CI Intranet site.



stackArmor Journey Map 2 | ATO Journey

Invested early in mapping out the customer journey, which is the foundation of managing and maturing all stackArmor operations across practice areas. This one is for the delivery/ATO phases.

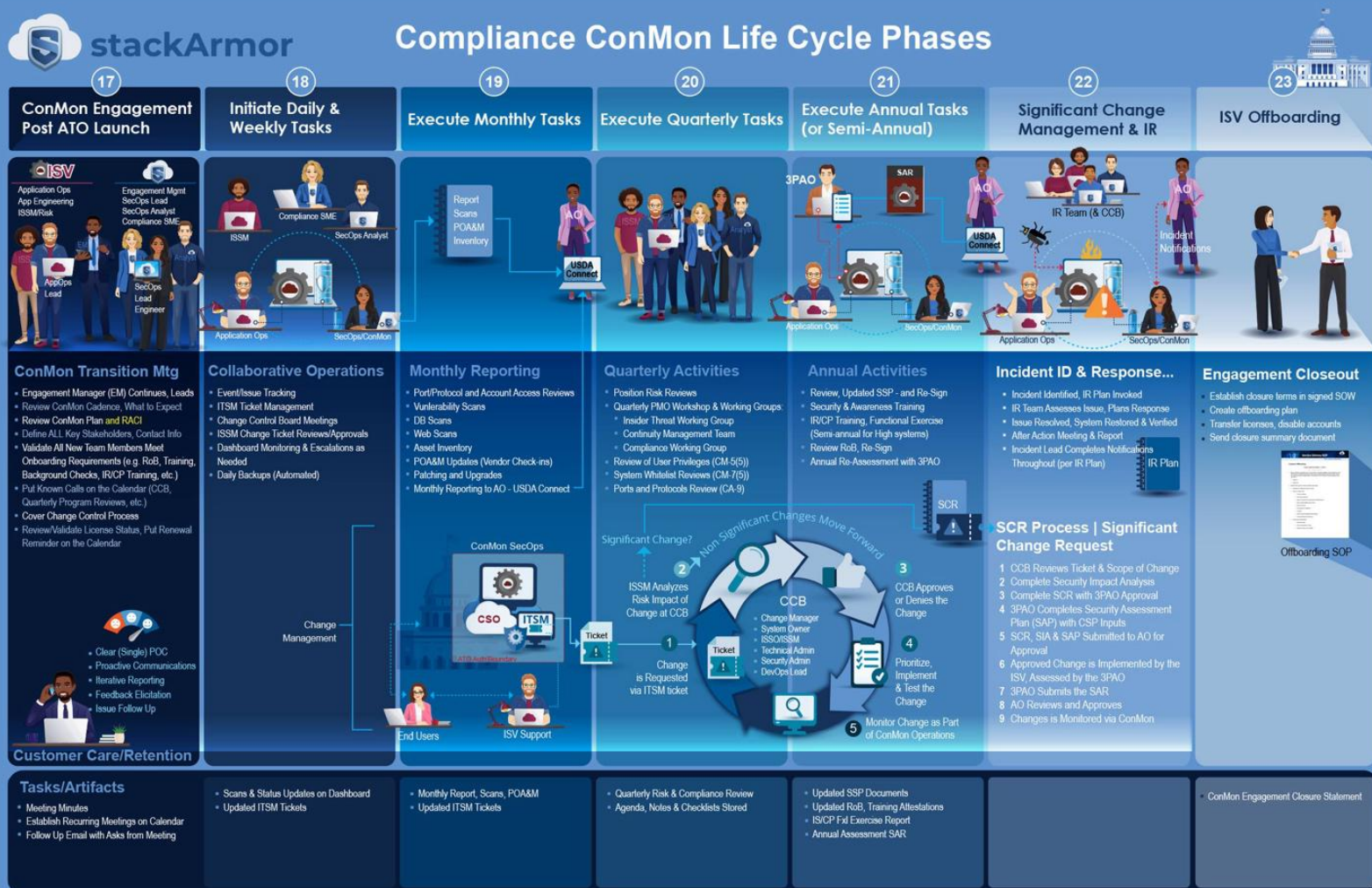
- This complex journey map identifies the “happy path” process, roles involved, activities that should occur, and artifacts created across the second 1/3 of the end-to-end customer journey.
- Map enables clear definition of roles/responsibility across teams, and activities all customers and team members can expect
- All journey maps are available on the CX/CI Intranet site.



stackArmor Journey Map 3 | ConMon Journey

Invested early in mapping out the customer journey, which is the foundation of managing and maturing all stackArmor operations across practice areas. This one is for the ConMon phases.

- This complex journey map identifies the “happy path” process, roles involved, activities that should occur, and artifacts created across the final 1/3+ of the end-to-end customer journey.
- Map enables clear definition of roles/responsibility across teams, and activities all customers and team members can expect
- All journey maps are available on the CX/CI Intranet site.



Created Quick Reference Guides & Template

Created a Quick Reference Guide template and a couple guides (as needed) to provide customers. This is a growing library of customer-facing guides.

- The template (2nd example) is simple and clean looking.
- First 2 guides were a [documentation package creation guide](#) and an [external connection guide](#), both for specific customers but now available for any customers!



Documentation Package Development: FedRAMP High

Quick Reference Guide

The stackArmor team will collaborate with customer app teams to ensure the right information is incorporated into the documentation package. This will be done through the following series of meetings:

Session	Task	Controls	Customer Team People/Roles Needed
1	AT and PS interview session	AT: 7 PS: 10	AT - Personnel responsible for oversight/ enforcing/ monitoring of training (security, role-based, social engineering) and retaining records. PS - Personnel responsible for personnel security including onboarding/ termination/ transfers/ position descriptions and for monitoring external personnel security.
2	PL and CA interview session	PL: 6 CA: 16	PL & CA – Senior Managers, Information Security Personnel, Technical Administrators, Help Desk personnel.
3	IR and CP interview session	IR: 26 CP: 35	IR & CP - Senior Managers, Information Security Personnel, Technical Administrators, Help Desk personnel
async review	MA, MP, and PE draft creation stackArmor will draft policies & procedures for asynch reviews	MA: 14 MP: 12 PE: 27	MA, MP & PE - Senior Managers, Information Security Personnel, Technical Administrators, Help Desk personnel. (Mostly inherited from an authorized cloud provider.)
async review	stackArmor begins compiling SSP sections 1-12, which will be reviewed asynchronously by the customer and iteratively edited/updated as needed.		
4	AC interview session	AC: 49	Senior Managers, Information Security Personnel, Technical Administrators
5	IA interview session	IA: 31	Senior Managers, Information Security Personnel, Technical Administrators
6	CM interview session	CM: 36	Senior Managers, Information Security Personnel, Technical Administrators
7	SA interview session	SA: 26	Senior Managers, Information Security Personnel, Technical Administrators, Developers
8	SC and SI interview session	SC: 39 SI: 39	Senior Managers, Information Security Personnel, Technical Administrators
9	SR interview session	SR: 14	Senior Managers, Information Security Personnel, Technical Administrators
10	RA and AU interview session	RA: 12 AU: 31	RA & AU – Senior Managers, Information Security Personnel, Technical Administrators

See the following page for a brief description of each family.



QRG: FedRAMP High Doc Package Development

Control Families in Scope for FedRAMP High

- **Access Control (AC):** Managing who has access to what resources.
- **Audit and Accountability (AU):** Tracking and reviewing system activity.
- **Awareness and Training (AT):** Educating users about security policies and procedures.
- **Configuration Management (CM):** Managing and controlling system configurations.
- **Contingency Planning (CP):** Preparing for and responding to system failures or disasters.
- **Identification and Authentication (IA):** Verifying user identities.
- **Incident Response (IR):** Responding to and recovering from security incidents.
- **Maintenance (MA):** Ensuring ongoing system maintenance and support.
- **Media Protection (MP):** Protecting physical storage media.
- **Personnel Security (PS):** Managing the security of personnel.
- **Physical and Environmental Protection (PE):** Protecting physical facilities and the environment.
- **Planning (PL):** Developing security plans and policies.
- **Risk Assessment (RA):** Identifying and assessing security risks.
- **Security Assessment and Authorization (CA):** Assessing the security posture of a system and gaining authorization for its use.
- **System and Communications Protection (SC):** Protecting system and communication channels.
- **System and Information Integrity (SI):** Ensuring the integrity of system and data.
- **System and Services Acquisition (SA):** Managing the acquisition of new systems and services.
- **Supply Chain Risk Management (SR):** Managing risks in the supply chain.

FedRAMP QRG | External Services and System Connections

The information presented in this QRG is intended to be a general guide to better understand how the use of external systems and services is managed for FedRAMP authorized solutions. Each authorized solution and its customers have a unique risk tolerance that will impact and guide decisions about the use of external systems and services.



Note: All federal data and metadata in transit (SC-8) and at rest (SC-28), and all cryptographic functions (e.g., hashing, random number generation, etc.) (SC-13), must utilize FIPS-validated encryption.

Use of FedRAMP Authorized Services

For FedRAMP authorized systems, any connection that processes, stores, and/or transmits federal data or metadata needs to be FedRAMP authorized.

Those connections will go on table 6-1 of the SSP which captures the following information:

- CS/CSO Name (Name on FedRAMP Marketplace)
- CSO Service
- Authorization Type (JAB or Agency) and FedRAMP Package ID #
- Nature of Agreement
- Impact Level (High, Moderate, Low, LI-SaaS)
- Data Types
- Authorized Users/Authentication

Table 6.1 Leveraged FedRAMP Authorized Services

#	CS/CSO Name (Name on FedRAMP Marketplace)	CSO Service (Names of services and features - services from a single CSO can be all listed in one cell)	Authorization Type (JAB or Agency) and FedRAMP Package ID #	Nature of Agreement	Impact Level (High, Moderate, Low, LI-SaaS)	Data Types	Authorized Users/Authentication

Use of Non FedRAMP Authorized Services

Any external connections that aren't FedRAMP authorized cannot process, store and/or transmit sensitive federal data or metadata (typically, these should be limited to update sources).

These will be documented in Table 7.1 which captures the following information:

- System/Service/ API/CLI Name (Non-FedRAMP Cloud Services)
- Connection Details
- Nature of Agreement
- Still Supported?
- Data Types
- Data Categorization
- Authorized Users/Authentication
- Other Compliance
- Description
- Hosting Environment
- Risk/Impact/ Mitigation

Table 7.1 External Systems/Services, Interconnections, APIs, and CLIs Without FedRAMP Authorizations

#	System/Service/ API/CLI Name (Non-FedRAMP Cloud Services)	Connection Details	Nature of Agreement	Still Supported?	Data Types	Data Categorization	Authorized Users/Authentication	Other Compliance

***1- Non-FedRAMP Authorized Cloud Services, 2- Corporate Shared Services, 3- Update Services for In-Bound

Rev 1.0 – 01.15.2025

Connection Ports, Protocols and Services

There are no hard rules that explicitly prohibit the use of any specific ports and protocols.

All ports, protocols and services in use within the system boundary must be defined and their use justified by populating details in Table 9-1 in the SSP:

- Service Name
- Port #
- Transport Protocol
- Reference #
- Purpose
- Used By

Table 9.1 <Insert CSO Name> Services, Ports, and Protocols

Service Name	Port #	Transport Protocol	Reference #	Purpose	Used By

stackArmor is Here to Help

The stackArmor compliance team works with our customers during documentation development to help gather any information about a system's external connections that wasn't captured during initial discovery.

A review of ports and protocols will be guided by stackArmor's proprietary and standardized Task Definition approach. Each customer's Table 9-1 ports, protocols report will be generated automatically assuming customers follow the guidance in stackArmor's Ingress Rules Description Playbook - which will be made available to our customers and details the description specification for Security Group Ingress rules to meet **System Security Plan table 9.1 and SSP Appendix Q Cryptographic Modules Table** requirements. The playbook also provides implementation guidance and context to assist in meeting these requirements.

The team will be looking at all of their external connections as part of the Gap Analysis process and will highlight any use cases that might be problematic, not allowed, or require a risk acceptance.

Additional Resources

Details and instructions on what information each of the fields required can be found in the **FedRAMP SSP Template**: Pages 11-13 for 6.1, pages 15-17 for Table 7.1, and pages 24-25 for Table 9.1.

Rev 1.0 – 01.15.2025



Build a CX program, including a supporting analysis and response/ management tool to standardize and partly automate the analysis and establishment of plans to health for key weaknesses in stackArmor's business.

- *Information is from myself as a customer, and feedback from other stackArmor customers, as well as employees.*
- *The tool was used with a task force team to add robustness to the analysis.*
- *Program put on back burner as other duties grew... but it's legit!*

Executive Dashboard



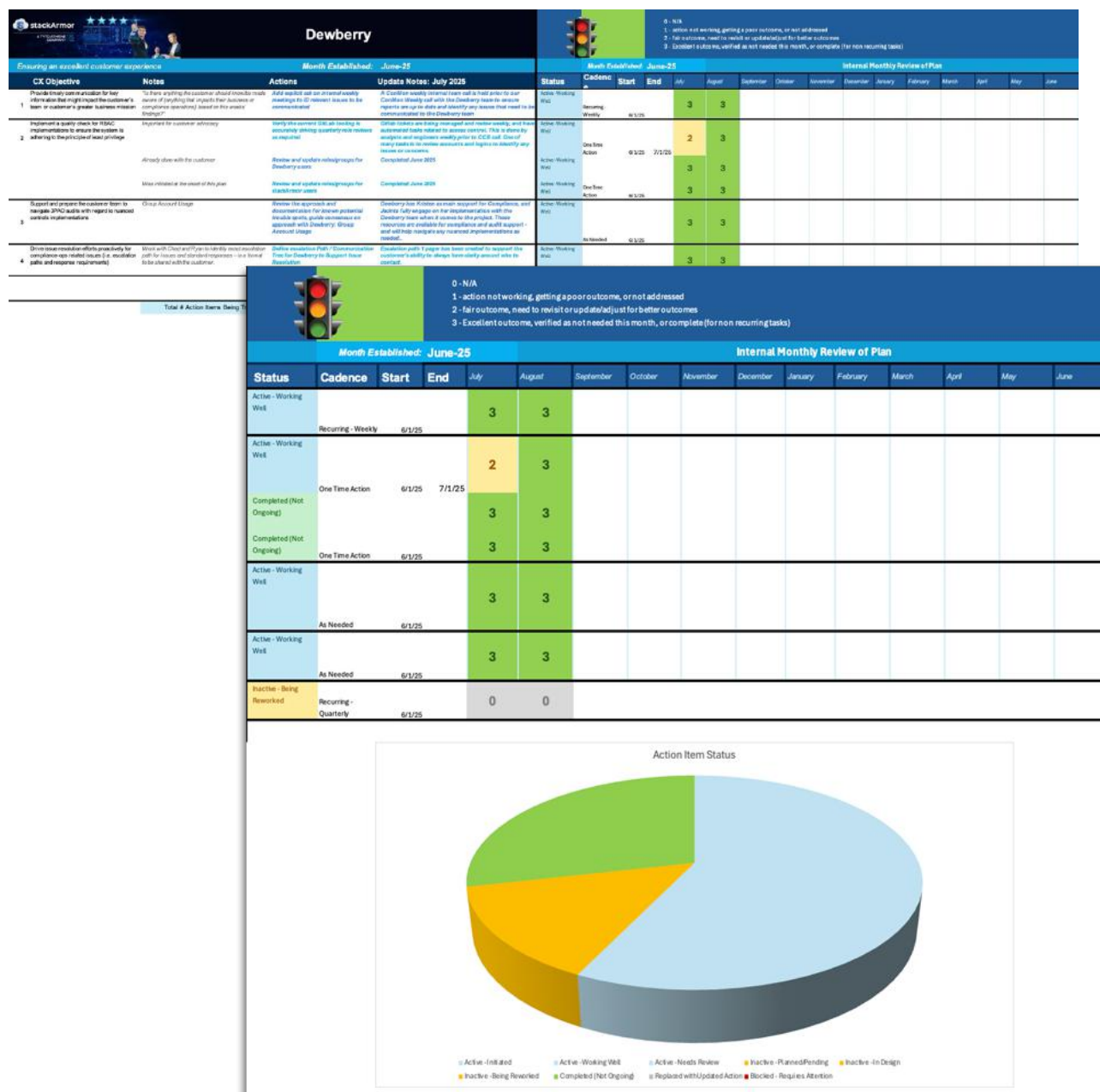
Operational Risk Reduction Micro Project Overview: Plans to Health												
Issue / Risk	Issue 1	Status	Issue 2	Status	Issue 3	Status	Issue 4	Status	Issue 5	Status	Issue 6	Status
Dependencies <div>1. Communication Quality: Ensuring all stakeholders are informed and aligned on project goals and progress. 2. Resource Availability: Ensuring all team members have the necessary skills and capacity to complete their assigned tasks. 3. Information Accessibility: Ensuring all relevant data and documents are easily accessible to the project team.</div>	1. Clear project communication and stakeholder engagement. 2. Lack of project communication and stakeholder engagement. 3. Lack of project communication and stakeholder engagement.		1. Lack of project communication and stakeholder engagement. 2. Lack of project communication and stakeholder engagement. 3. Lack of project communication and stakeholder engagement.		1. Lack of project communication and stakeholder engagement. 2. Lack of project communication and stakeholder engagement. 3. Lack of project communication and stakeholder engagement.		1. Lack of project communication and stakeholder engagement. 2. Lack of project communication and stakeholder engagement. 3. Lack of project communication and stakeholder engagement.		1. Lack of project communication and stakeholder engagement. 2. Lack of project communication and stakeholder engagement. 3. Lack of project communication and stakeholder engagement.		1. Lack of project communication and stakeholder engagement. 2. Lack of project communication and stakeholder engagement. 3. Lack of project communication and stakeholder engagement.	
Micro Projects <div>1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.</div>	1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.	Planned	1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.	Planned	1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.	Planned	1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.	In Progress	1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.	In Progress	1. Establish a project team and assign roles and responsibilities. 2. Develop a project plan and timeline. 3. Identify potential risks and develop mitigation strategies.	In Progress

Micro Project-Plan Tracker (Rolls up Action Items & Status for Each Plan)

Customer CX Action Plan Program | “Plan to Green”

Designed and built templates to record and track specific action items as part of an issue resolution or root cause analysis that results in action items. This shows our commitment to the customer experience and holds us accountable to commitments we’ve made to the customer. This is **intentional relationship management**.

- Executed with both **Dewberry** and **Checkmarx**, both of whom are now happy with us (returned them to green!)
- Original plan is shared with the customer to address issues
- Issue status and “stoplight” (red-yellow-green) can be tracked monthly until all issues are green
- At 4-6 weeks a follow up report is presented to the customer led by myself to address our response (the internal tracking isn’t shared)
- Meetings will continue until issues are “resolved”, relationship is “green” – at which time the normal retention plan remains
- CX-Excellence-Delivery-Plans-v2-Dewberry-Aug25-2025.xlsx



Customer CX Action Plan Program | Plan to Green cont...

- The updates on plan progress are shared on video call with the customer in presentation format. (The example below is **Dewberry**, but also have one of these for **Checkmarx**...)



Dewberry Dewberry CX Review

Aug 5, 2025

Dewberry			
Ensuring an excellent customer experience		Month Established: June-25	
CX Objective	Notes	Actions	Update Notes: Aug 2025
1 Provide timely communication for key information that might impact the customer's team or customer's greater business mission	"Is there anything the customer should know/be made aware of (anything that impacts their business or compliance operations) based on this weeks' findings?"	Add explicit ask on internal weekly meetings to ID relevant issues to be communicated	A ConMon weekly internal team call is held prior to our ConMon Weekly call with the Dewberry team to ensure reports are up to date and identify any issues that need to be communicated to the Dewberry team
2 Implement a quality check for RBAC implementations to ensure the system is adhering to the principle of least privilege	Important for customer role management Already done with the customer Was initiated at the onset of this plan	Verify the current GitLab tooling is accurately driving quarterly role reviews as required Review and update roles/groups for Dewberry users Review and update roles/groups for stackArmor users	GitLab tickets are being managed and review weekly, and have automated tasks related to access control. This is done by analysts and engineers weekly prior to CCB call. One of many tasks is to review accounts and logins to identify any issues or concerns. Completed June 2025 Completed June 2025
3 Support and prepare the customer team to navigate 3PAO audits with regard to nuanced controls implementations	Group Account Usage	Review the approach and documentation for known potential trouble spots, guide consensus on approach with Dewberry: Group Account Usage	Dewberry has Kristen as main support for Compliance, and Jacinta fully engage on her implementation with the Dewberry team when it comes to the project. These resources are available for compliance and audit support - and will help navigate any nuanced implementations as needed.
4 Drive issue resolution efforts proactively for compliance-ops related issues (i.e. escalation path for issues and standard responses - in a format to analyze and measure performance)	Work with Chad and Ryan to identify exact escalation path for issues and standard responses - in a format to analyze and measure performance	Define escalation Path / Communication Tree for Dewberry to Support Issue Resolution	Escalation path 1 pager has been created to support the customer's ability to always have clarity around who to contact.

Escalation Paths

stackArmor			
Issue Escalation Process for ConMon Engagements			
<p>Figure 1 - General Escalation Path</p>			
Dewberry Specific Escalation Path:			
Escalation	Role/Title	Team Member	Email
1 Project Team	Security Engineer Lead	Jacinta Bailey	jbail@stackarmor.com
	Security Analyst Lead	Jacinta Bailey	jbail@stackarmor.com
	Compliance Consultant	Kristen Page	kpage@stackarmor.com
	Backup Engineer	Karen Hines	khines@stackarmor.com
2 Engagement Management Team	Engagement Manager (EM)	Orly Noyan	onoyan@stackarmor.com
	EM Backup (i.e. PTO coverage)	Orly Noyan	onoyan@stackarmor.com
3 Director/Str. Director Team	Str Director of Cloud Ops - Oversees analysis & engineering or - Director of Cloud Ops	Chad Busha	cbusha@stackarmor.com
	Str Director of Cloud Ops - Oversees ERM	Ryan Mahan	rmahan@stackarmor.com
	Str Director of Cloud Ops - Oversees ERM	David Hines	dhines@stackarmor.com
	Str Director of Cybersecurity & Compliance	Rene Clarke	rclarke@stackarmor.com
	Str Director of Compliance	Tracy Bomer	tbomer@stackarmor.com
4 Chief Team	Chief Delivery Officer (CDO) - Oversees all Customer Engagements	John DeBorja	jdeb@stackarmor.com
	Chief Information Security Officer (CISO) - Oversees Risk and Compliance Efforts	Martin Rieger	mrieger@stackarmor.com
	Chief Solutions Officer (CSO) - Oversees Solution Offerings	Martin Rieger	mrieger@stackarmor.com

Aug 5, 2025



Established stackAcademy for Role Based Training

Established a role based training template with built-in participant attestation that is now in use in multiple use cases at stackArmor.

- Role based training template contains key elements that matter for compliance (identifying roles, identifying NIST family impacted, including a participant attestation page/certificate of completion).
- Created the first training on Change Control to address specific issues with our folks not complying (*below is a few of those slides... not all*)
- SecOps also uses this template/approach for training on TSW releases (new SOP as of spring/summer 2025)

stackArmor Cloud Migration | Compliance | Cybersecurity | Managed Services

Compliance Role-Based Training

Cybersecurity Compliance

Change Management for Regulated Systems

Last Updated Oct 3, 2024

Proprietary and Confidential Information of stackArmor

Target Roles:

- System Owner, Engineering Lead, ISSM, Configuration Manager, Compliance Lead, Senior Manager, Change Control Board Members
Any company roles who act as change ticket creators and/or approvers
- ISSO or Lead SOC Engineer
Any company roles who act as change ticket creators or implementors
- SOC Engineers, Security Analysts, Security Technical Admin
Any company roles who act as change/ticket implementors

August 7, 2025

Proprietary and confidential information of stackArmor

Training Objectives

- Understand controls and constraints associated with making changes to a highly regulated production environment (NIST 800-53 CM-3)
- Identify the processes for making changes to the organization's production environment (minor, major and significant)

August 7, 2025

Proprietary and confidential information of stackArmor

This training is focused on FedRAMP Moderate Systems

Guiding NIST 800-53 Controls

Primary:

- CM-3 – Configuration Change Control – Requires a change management and control process, with part d focused specifically on implementing changes to a production environment.

Secondary (related):

- CM-5 (5) – Access Restrictions for Change – Privilege Limitation for Production and Operation related to those allowed to make system changes (must be reviewed quarterly).
- CM-9 – Configuration Management Plan, which describes how system components or configuration items (CI) are brought under control (updated annually or as needed).
- SA-10 – Developer Configuration Management – Requires the developer of the system or its components to follow similar change control guidelines.

Thursday, August 7, 2025

SSP Requirements for FedRAMP

stackArmor

Training Agenda

- Control Review - NIST 800-53 guidance
- Review of System Specific Implementation Details (from System SSP)
- Managing change for:
 - Minor changes
 - Major changes
 - Significant changes
- Next steps

Thursday, August 7, 2025

SSP Requirements for FedRAMP

stackArmor

NIST 800-53 Review: CM-3 – Configuration Change Control

- Determine and document the types of changes to the system that are configuration-controlled;
- Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
- Document configuration change decisions associated with the system;
- Implement approved configuration-controlled changes to the system;
- Retain records of configuration-controlled changes to the system at least 1 year (we retain in GitLab for the life of the system);
- Monitor and review activities associated with configuration-controlled changes to the system;
- Coordinate and provide oversight for configuration change control activities through Change Control Board (CCB) (equivalent to a configuration control board) that convenes at least monthly but may convene Emergency Change Control Board meetings as often as deemed necessary to maintain appropriate security risk posture and Service Level Agreements (SLA).

Thursday, August 7, 2025

SSP Requirements for FedRAMP

stackArmor

Creating Role-Based Tickets

Click to the ISSM or System Owner

Through Automated Technologies

Team

at GitLab Change Request Issue

Thursday, August 7, 2025

SSP Requirements for FedRAMP

stackArmor

Change Management Role-Base Training: Certificate of Completion

This certificate serves as attestation that I have completed the Change Management role-based training course – and that I understand and will incorporate the change management information presented in the training as I perform my job duties.

Name: _____

Title/Role: _____

Date: _____

Signature: _____

stackArmor

CX/EX – Designed & Built Company Portal/Intranet

Designed and built a company Intranet that is currently ready to be shared with all and serve as a single point from which employees can access resources either directly or through links and interfaces.

- Identified the need and took the initiative to improve the employee experience by designing an “Intranet”
- While only partially implemented, using this type of Intranet as a single starting point for employees to find resources they need is critical to our ability to grow effectively
- Site is designed to hold general stackArmor information, elicit feedback from employees (the fully functional Idea Tank), point to SOPs for all practice areas, hold role-based training modules, provide HR support materials, etc.
- Part of this was a proof of concept in how a SharePoint site can be designed for intuitive and delightful user experience (UX)

CX/EX Intranet Home Page



The screenshot displays the CX/EX Intranet Home Page. The top navigation bar includes the stackArmor logo and a search bar. The main content area features a large banner with the text "Your Employee | Customer Experience journey starts here!" and a call to action "Idea Tank". Below this, a section titled "Employee and Customer End-to-End Journey Maps (Click to Hide/Show)" displays a detailed "Sales & Work Initiation Life Cycle Phases" diagram. The diagram is organized into a grid with columns for various stages: 1. Offering Establishment & Validation, 2. BD, Sales & Marketing Campaigning, 3. Customer Pipeline Establishment, 4. Prospect Qualification & Sales Navigation, 5. SOW/Contract Negotiations, 6. Signed SOW, and 7. Handshake with Delivery, Prep Work. Each column contains a list of tasks and responsibilities. The "Idea Tank" section is highlighted with a blue dashed line and a large lightbulb icon.

Established an Idea Tank – a link that opens an employee idea/feedback form, tracked in a SmartSheet dashboard...

CX/EX Intranet H

SharePoint | Customer Experience | Employee Experience (CX/EX)

stackArmor

Your Employee | Customer Experience journey here!

Welcome to the stackArmor CX/EX site - purpose built to support a better employee experience. Like Amazon, we share our job roles and check to make the evolution in the experience. Feel free to use the idea tool for any thoughts, ideas, issues, or suggestions aimed at improving the customer employee experience on board!

stackArmor is committed to being the company our employees never want to be without!

Employee and Customer End-to-End Journey

Customer and Employee Journey

Sales & Work Instructions

Employee Resource Center

Info & Onboarding Docs

Document Templates

Establish Professional Goals

Journey-Driven Job Taskings

SOPs for Common Tasks

Job Role Playbooks

Quick Reference Guides

LEADERSHIP & COMPANY CULTURE

"We are committed to being the company our employees and customers never want to be without!"

Employee Resource Center

Let's Grow!

Info & Onboarding Docs

Document Templates

Establish Professional Goals

Journey-Driven Job Taskings

SOPs for Common Tasks

Role-Based Training

Job Role Playbooks

SOPs

Role Based Training

Quick Reference Guides

Quick Reference Guides

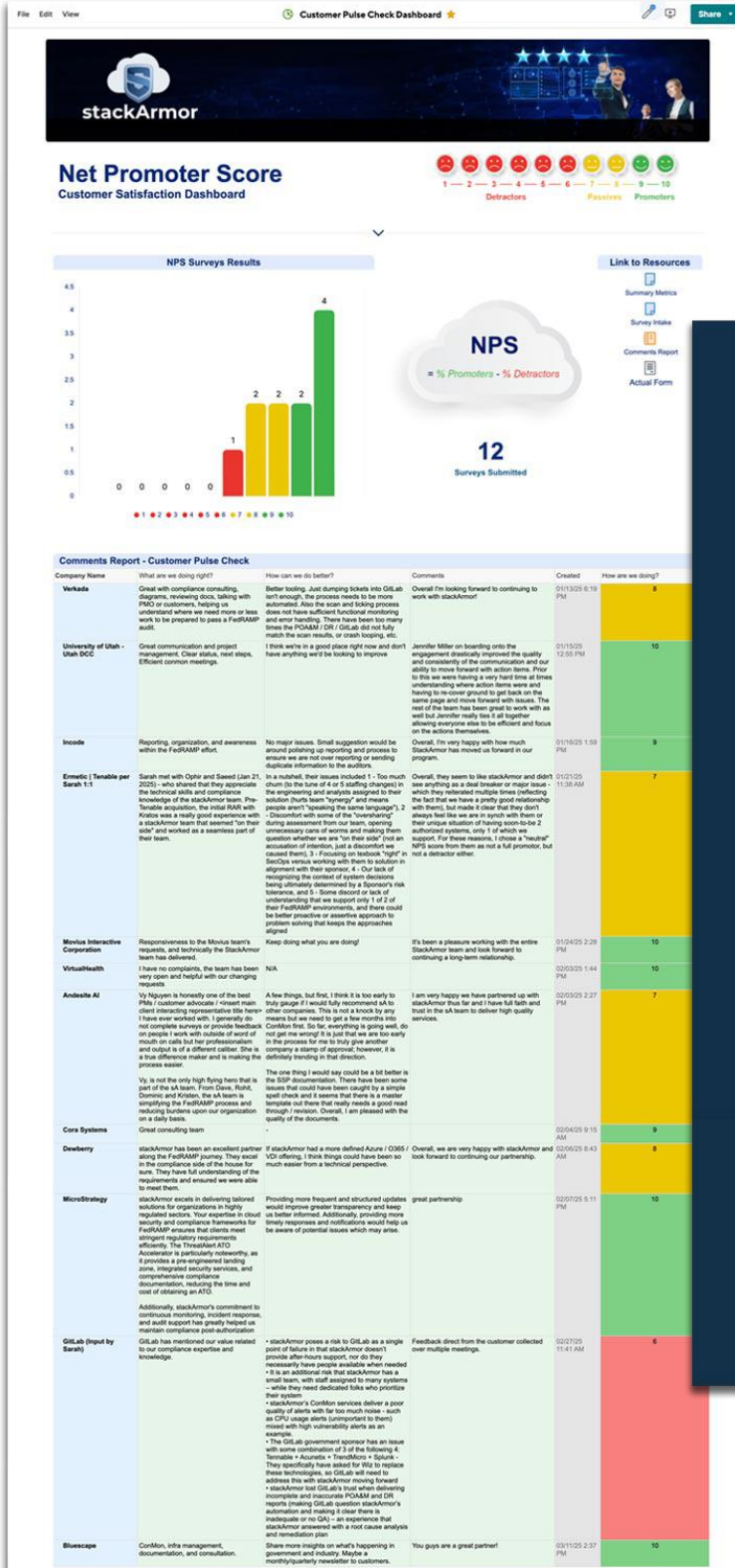
LEADERSHIP & COMPANY CULTURE

"We are committed to being the company our employees and customers never want to be without!"

MVP Customer Advisory Board – NPS-Based Customer Satisfaction Tracking

Established an MVP “Customer Advisory Board” to guide intentional feedback elicitation from our customer base to help inform our delivery and improve CX.

- Took the initiative to create this, expand my SmartSheet skills
- Ongoing coordination with the EM team to encourage participation
- Designed a tracking dashboard
- Program has resulted in a handful of new feature request tickets and product roadmap considerations (e.g. Wiz incorporation)



stackArmor Survey

stackArmor looks forward to collecting real customer feedback to help us improve our service delivery!

Company Name
Please provide your company name.

1 - How are we doing? *
How likely are you to recommend stackArmor to someone with cloud service compliance consulting needs? (1 - Not at all likely | 10 - Extremely likely)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

2 - What are we doing right? *
What does stackArmor do really well that we should continue?

3 - What can we do better? *
What changes would stackArmor have to make for you to grant a higher rating?

Comments
Please feel free to share any additional comments or feedback.

Thank you for your input!

We appreciate your time in and help with this survey and the opportunity to improve our service.

☐ Send me a copy of my responses

Submit

[Privacy Notice](#) | [Report Abuse](#)

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Marketing & Content Development

Created a stackArmor Brand Guide

Established a stackArmor Brand Guide, and updated post Tyto acquisition.

- Took the initiative to create this as it was non-existent
- Defined our competitive differentiators, identity, core values, target customer (not just look and feel, imagery guidance and color palettes, but deeper corporate identity)
- Did all the same for Armory (competitive differentiators, core benefits, core capabilities, competitors, and a full page of core product messaging)
- [stackArmor-Style-Guide-content-DRAFT3.pdf](#)





A TYTO ATHENE
COMPANY

stackArmor Brand Strategy

Built to Align with & Augment the Tyto Brand



stackArmor Brand Positioning

Competitive Differentiators:

- Founder Experience (Since Day 1)
- "GRC" Automation Leadership (product)
- Proven Track Record of ATOs (services)
- Commitment to Continuous Improvement (CX Program)
- Key Partnerships

Target Customer Profiles:

- SaaS CSPs wanting to serve federal/DOD agencies and looking for a path to cybersecurity & compliance
- Federal agencies without skills or resources needing to secure and meet regulatory compliance requirements for their cloud solutions
- State, local and educational institutions that require a secure, hardened, compliant environment

stackArmor Identity - We are:

- Competent Technologists
- Trusted Advisors
- Industry Thought Leaders
- Creative Solutioners
- Reliable Partners

Core Personality:

Future-Embracing, Future-Defining

stackArmor is a future-defining organization, that both embraces the cutting-edge technologies available today and innovates/invents the technologies that will solve real problems tomorrow.

Core Values - We believe in:

- Courage in Digital Innovation
- Leadership in Cybersecurity Compliance
- Trustworthiness in Service Delivery
- Dedication to Customer Mission
- Excellence in Customer Experience
- Integrity in all Interactions

Imagery and Visual Aesthetic:

- Crisp & Clean** - concise and to the point images
- Digital Energy/Movement** - images that reflect movement, advancement, excitement
- Futuristic** - images that reflect AI & "Machine Driven"
- Connectedness** - images that say "connected"
- Secure** - images that reflect security & trustworthiness
- Accomplishment** - images that reflect human wins

Images with Digital Energy



Web Navigation Icon styles that say strong, machine, etc.

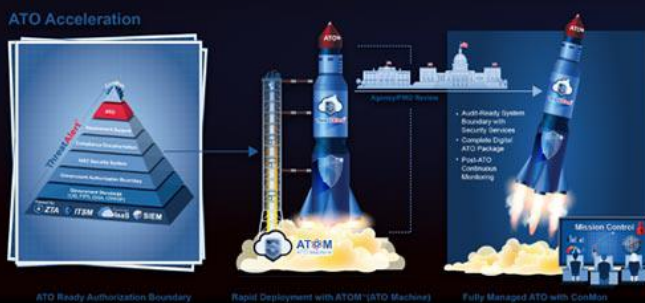


Illustration

2D shadowed Icon Example:



Multi-dimensional Illustration Example:



Logo Usage

What to do...



Full color for white/light background



All black for white/light background
(for uses that require black/white logo)



Full color for black/dark background



White for black/dark background
(for uses that require black/white logo)

Font Usage

Avenir Next - Corporate Font Family

Avenir Next Bold

Avenir Next Medium

Avenir Next Regular

Avenir Light

Avenir Next Italic

Arial - Backup Font

If Avenir or Avenir Next is not available, an acceptable secondary font choice would be Arial - which is generally universally available.

OTHER FONTS

Other (creative impact) fonts may be used within marketing and sales literature, but should be used strategically, in a very limited basis, and largely for titles or one-time headings. Other fonts should also reflect the mood and messaging of the artifact for which it is being used, and should align with stackArmor's broader imagery guidelines.

stackArmor.com QR Code

Logo Usage

What not to do...



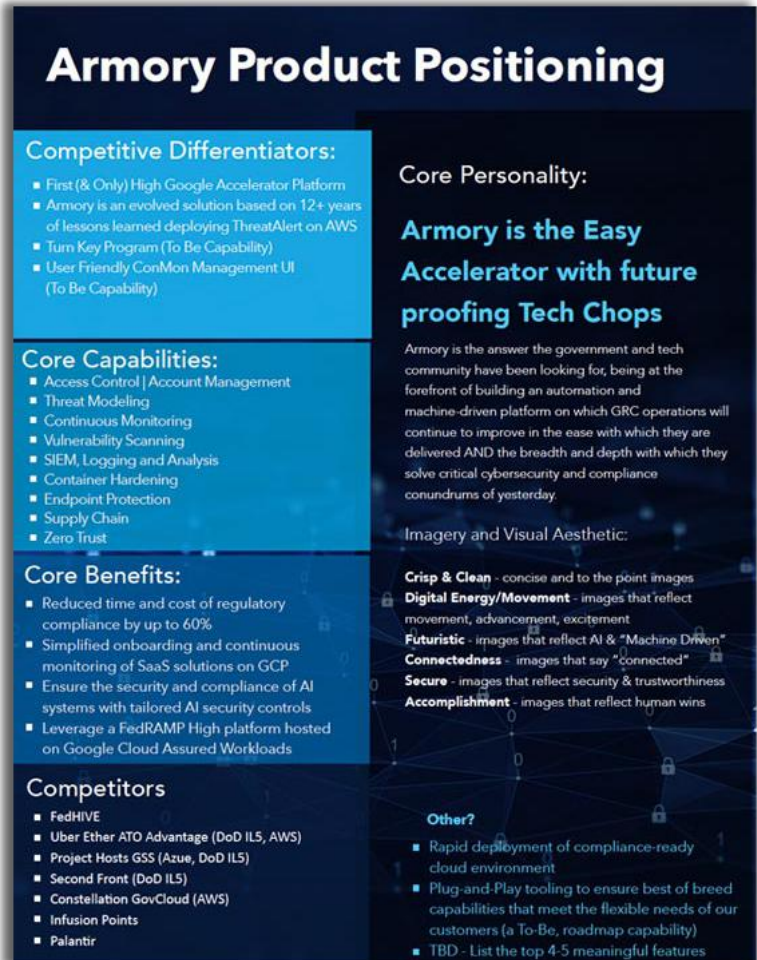
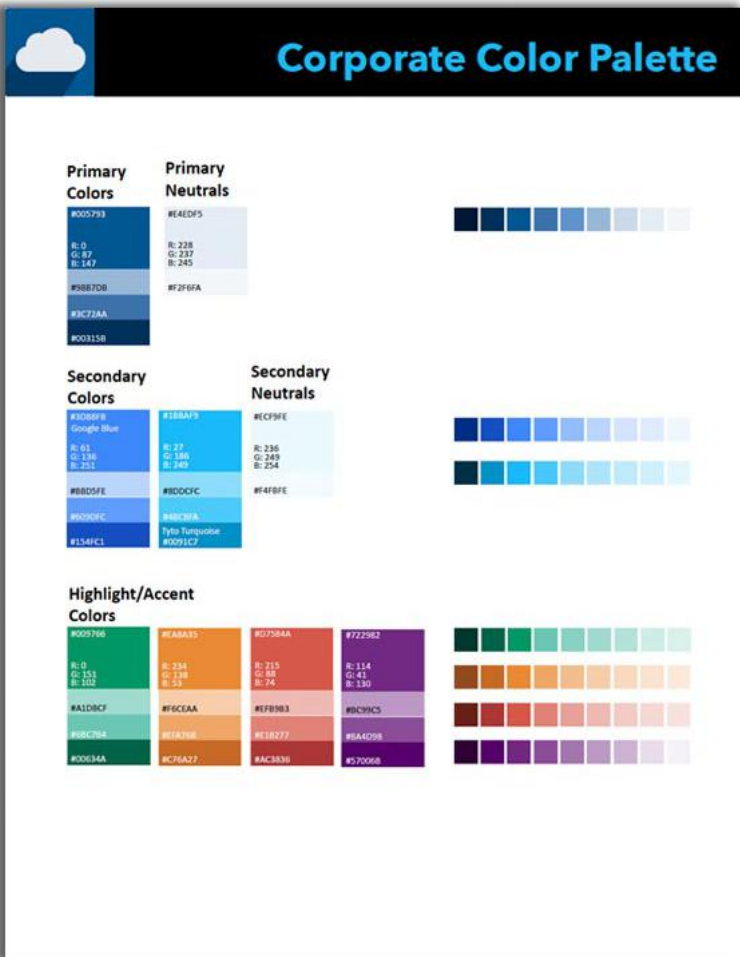
DO NOT change or vary the logo colors. Instead use an approved version that is appropriate for the use case.



DO NOT place the logo on a busy or competing background. Instead choose a logo style or placement that makes the logo clear and easy to recognize.



DO NOT skew or distort the logo.



Product Logo Usage

What to do...



Full color for white/light background



All black for white/light background
(for uses that require black/white logo)



Full color for black/dark background



White for black/dark background
(for uses that require black/white logo)

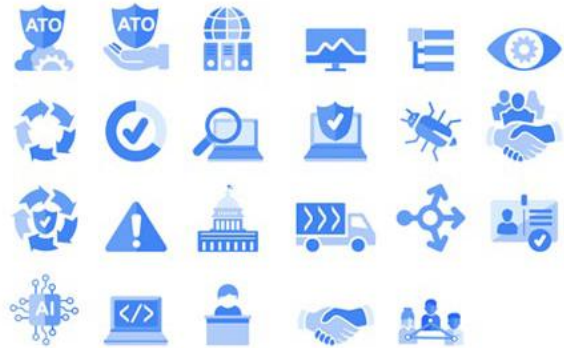


Armory Illustration

Armory Offering Illustration | for Explainer Decks



Armory Icon Set | Google Blues



Armory Illustration

Armory High-Tech, Photo-realistic Illustration Styles



Designed Logos for the Armory and Armory 20x

Created original illustrations and logo design for Armory (multiple versions) as well as a separate logo for our Armory 20x pilot offering.

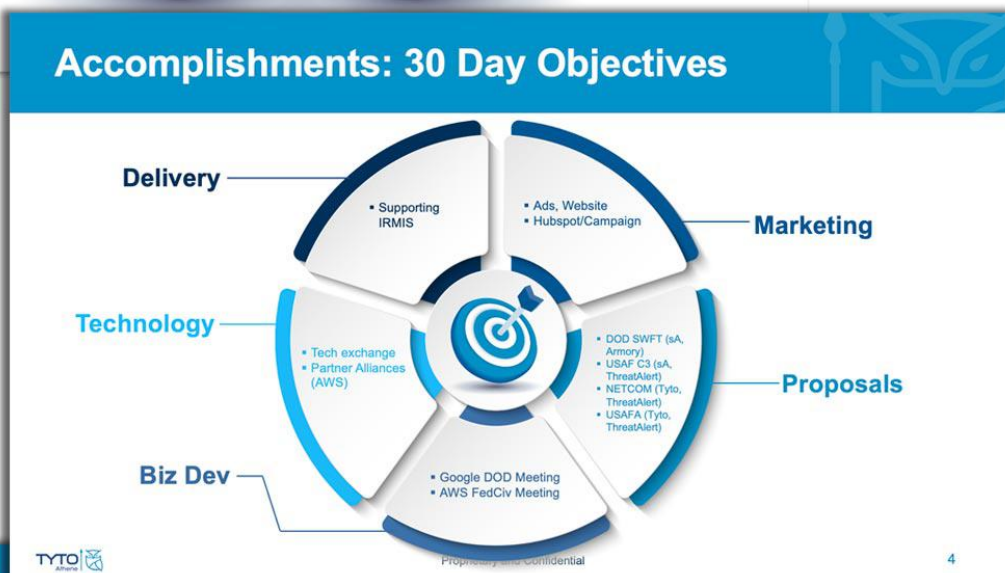
- Drove the creative iteration process with the leadership team.
- Logos are original vector illustrations (infinitely scalable)



Created Tyto Board Presentation Infographics

Created some original infographics for GP for a Tyto Board Presentation.

- VENN diagram, 30 Day Objectives Circle, Target Icon and Calendar Icon are all original illustrations
- Also helped format the other slide content in this deck to have a consistent, professional, Tyto look and feel



Upcoming Meetings

	Name	Role	Objective
1	Christian Hoff	AWS – FedCiv Leader	Connect on specific leaders within specific accounts of alignment and interest. VMWare Migration.
2	Keith Brooks	AWS – DOD Leader	Connect on specific opportunities within the DOD Estates and Services Account as well as JWCC; Marketplace
3	Rebecca Weatherly / Jane Lacy	AWS – Partner Leader	Credits, training, enablement, initiatives, funding.
4	Jim Kelly	Google – Federal Leader	Strategic conversation with discussion on large opportunities together e.g., SCIF, GDC
5	Troy Bertram	Google – Partner Team Leader	Discuss growth and training opportunities for Tyto
6	Chuck Greene	WWT - Public Sector Cloud Advisor	Strategic teaming opportunities on areas of interest. Broad capability briefing discussion including Marketplace
7	Craig Abod	Carahsoft -	Broad capabilities discussion; Opportunities to streamline purchases from Carahsoft e.g., MSFT licenses? Opportunities to list "products" on Carahsoft vehicles?
8	Broadcom Executives	Clarity, Rally	Deployed at multiple agencies including DAU, CPB, NCI, USPTO and others.

TYTO

Proprietary and Confidential

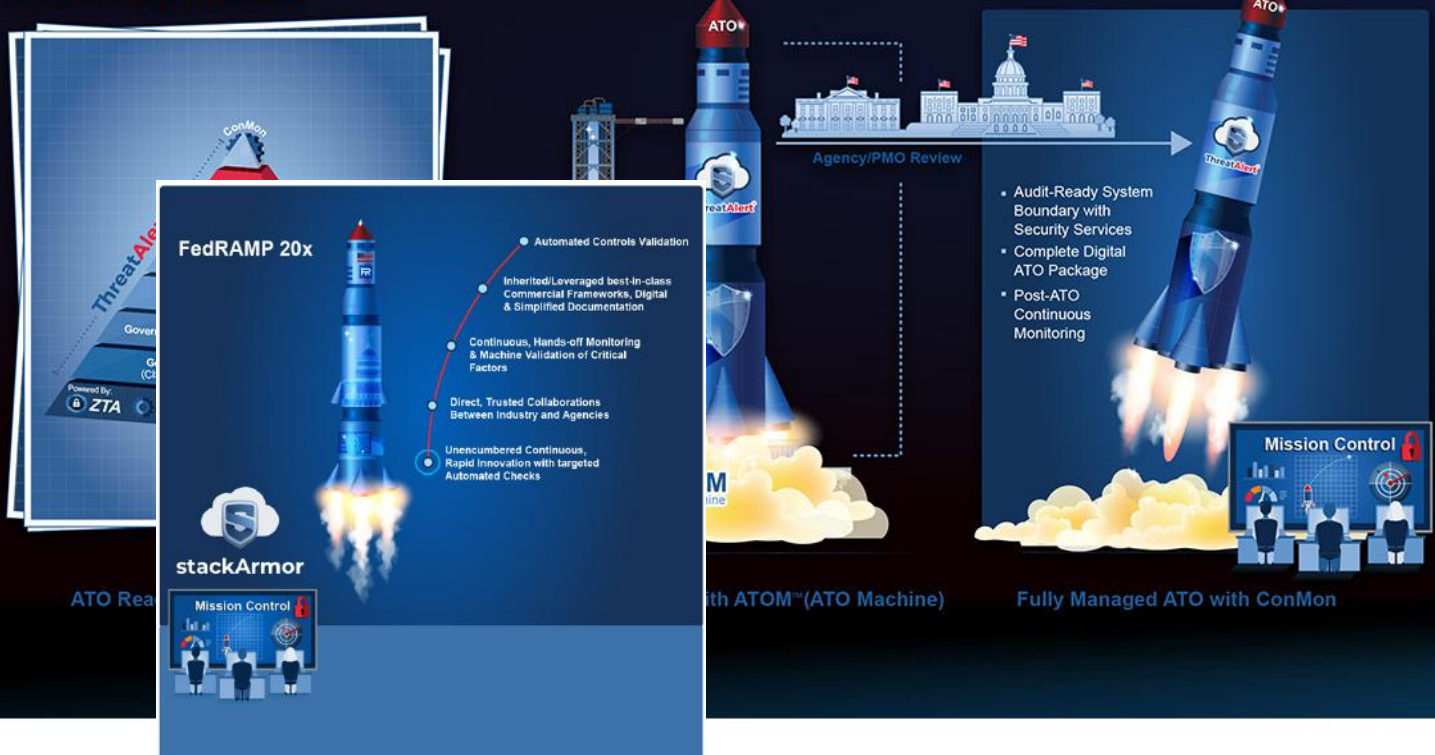
5

Created FedRAMP 20x Launch Infographics (GP)

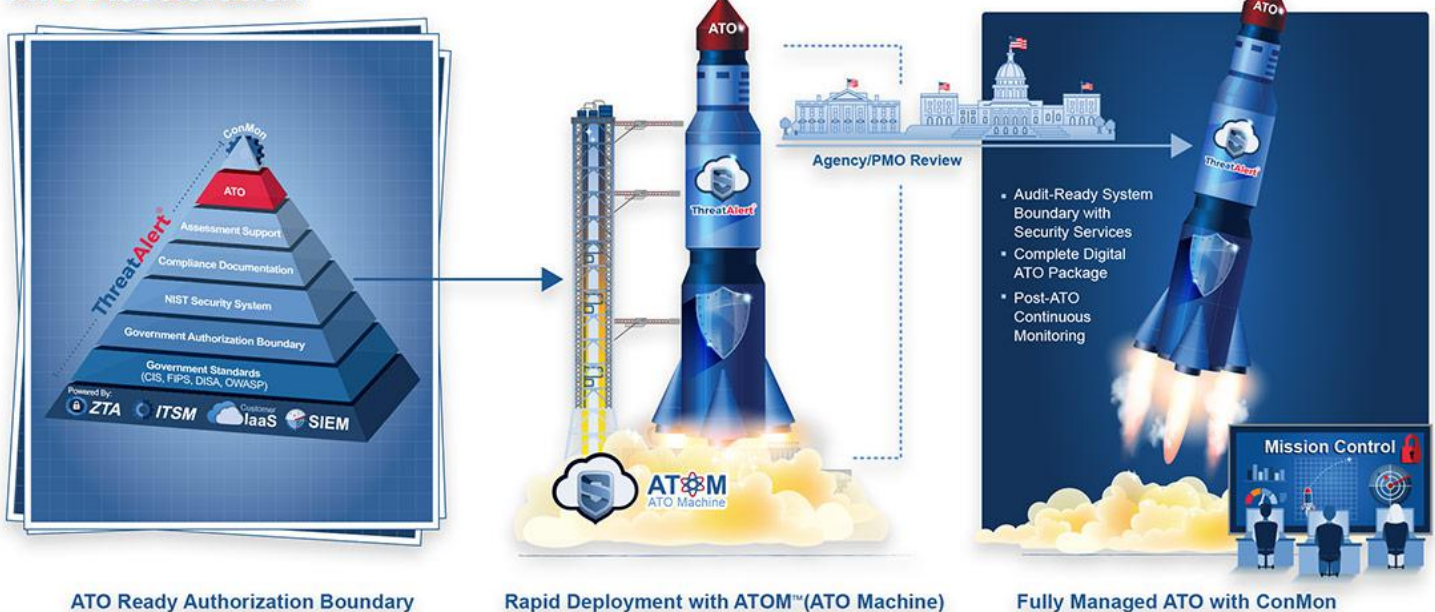
Created multiple original and updated infographics in support of FedRAMP 20x messaging for GP.

- Previously created ThreatAlert pyramid was updated, and the rocket and associated imagery created as vector illustrations
- Versions were used for various deliverables and marketing artifacts
- There was unique work required for various backgrounds

ATO Acceleration



ATO Acceleration



Created Component Definition Paper Infographic

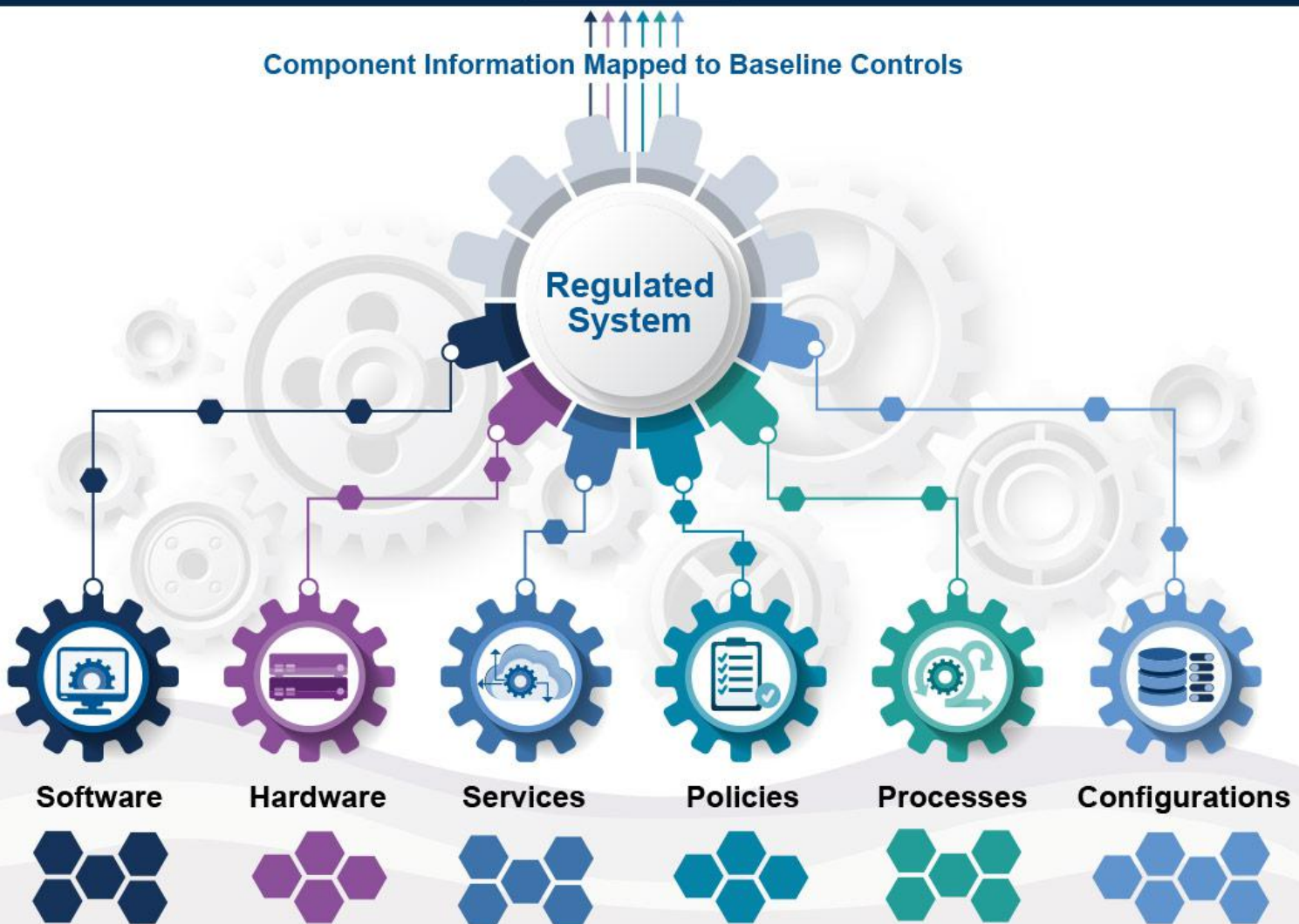
Envisioned and created original illustrations to tell a story of component-based SSP generation visually, based on written content from Johann.

- Read Johann's paper, and came up with the infographic below to tell his story visually
- All images are vector illustrations and fully scalable and editable



- Accurate Data-Driven System Representations
- Increased Assessment Speed and Efficiency
- Automated Validation of Control Implementations
- Efficient Updates

Component Information Mapped to Baseline Controls



CDEF - Component Definition Approach to SSP Management

Created a New Armory 2 Pager

Created a new 2 page glossy for trade shows and sales/marketing highlighting the Armory offering.

- All illustrations in the infographics on both pages are original vector images that I drew.
- I introduced a couple background photo files to align better with the Tyto branding norms.
- Most of the written content I also created (for this and the website)



The Armory™ | Accelerating FedRAMP ATOs on Google

Do you have a cloud solution that solves critical mission needs, provides a path of least resistance to FedRAMP and Google Cloud, offering the ability to accelerate the process, all the compliance, documentation, audit, and architecture? If your Government needs your solution, you need an ATO.

The Armory is a purpose-built, General Support System (GSS) to empower ISVs and Enterprises to conquer compliance (GCP) by delivering fully compliant architecture, engineering, along with continuous monitoring and a range of infrastructure and account management, all within a FedRAMP authorized environment managed to CMMC, ITAR, FedRAMP High, and DoD.



- Reduces time and cost of regulatory compliance
- Simplified onboarding and continuous monitoring
- Ensures the security and compliance of AI/ML
- Leverages a FedRAMP High compliant platform



www.stackarmor.com

Serving Government Agencies



- Reduced sponsorship burden and cyber risk
- Cybersecurity controls tailored for automated risk management
- Faster access to new SaaS capabilities to support mission needs



Connecting Agency Teams to Authorized, Mission Critical SaaS Solutions



Secure and Compliant SaaS Solutions



Google Cloud Platform

Modernized Cyber PMO



- ✓ StateRAMP
- ✓ FedRAMP
- ✓ CJIS
- ✓ CMMC
- ✓ HIPAA
- ✓ FISMA


- Subject Matter Expertise led advisory services
- Accreditation services & assessment support
- Machine-enabled continuous monitoring and Findings Lifecycle Management (FLM) for team member force multiplication
- Machine-enabled compliance monitoring and risk mitigation
- Automation-enabled monthly reporting

www.stackarmor.com/armory

Created a Revised ThreatAlert 2 Pager

Created an updated version of a ThreatAlert 2 page glossy (that I originally designed) to align with the most recent 2025 messaging.

- Again, all images in the infographics on both pages are original vector images that I drew.
- Some version of this 2-page has been used at trade shows for a couple years at least, this is just the latest!




ThreatAlert® ATO Accelerator


ThreatAlert ATO Accelerator reduces the time and cost of ATOs by 40%

ThreatAlert ATO Accelerator brings together innovative automation and compliant cybersecurity solutions to help organizations reduce the time and cost of FedRAMP, DOD, FISMA, CMMC and StateRAMP compliance by 40%. Our fully vetted ATO Acceleration solution is deployed "in-boundary" and meets Agency, DISA as well as ATO requirements for Moderate and High baselines.

ATO Acceleration

- Expert Advisory Services
- Audit-Ready System Boundary with Security Services
- Complete Digital ATO Package and SecOps Automation
- Post-ATO Continuous Monitoring
- Support for 100% of Compliance Baseline Controls





ATOM
ATO Machine


stackArmor's experienced cloud engineers are constantly innovating with technologies like Cloud Development and DevOps. Our approach leverages several key components:

ATOM is a faster, consistent, repeatable way to deploy FedRAMP compliant environments using compliance-ready cloud IaaS Security Platform. Global ISVs and customers looking to accelerate their ATO process can easily do so with ATOM.

Accelerating the Path to ATO


1. Build a Compliant, "In Boundary" Cloud Landing Zone for SaaS
2. Deploy SaaS in the Cloud, Inheriting IaaS & PaaS Compliant Controls
3. Tailor, Harden & Establish Readiness for All Required Controls: Scan, Test & Comply
4. Fully Assess End-to-end System & Address any Findings
5. Authorize Agency AO & PMO Review & Authorize
6. Continuously Monitor and Support Authorized SaaS
7. Post ATO Marketplace Listing

Documentation & Implementation of Policies, Procedures, Plans




ThreatAlert

stackArmor ThreatAlert® ATO Accelerator reduces time and cost of FedRAMP, FISMA/RMF, StateRAMP and CMMC ATOs by 40%




Automated SecOps

Machine-driven SecOps with integrated compliance control implementation component definitions answers the industry's growing demand for automation and machine-managed content



SIEM+

SIEM analytics with findings life-cycle management work together to quickly detect, triage and automate compliance and monitoring of security incidents/events







Customer IaaS

Compliant customer IaaS (e.g. Govcloud instances of AWS, GCP, Azure, etc.) delivers control inheritance capabilities

Meeting government security requirements is a strenuous, costly, and time-consuming obligation for enterprises providing mission-critical solutions to defense and government agencies - as well as customers in other highly regulated industries.

stackArmor's **ThreatAlert ATO Accelerator** is a proven method for meeting FedRAMP, CMMC 2.0 or FISMA requirements that is both fast and efficient without costing millions of dollars.



www.stackarmor.com

Delivered Brown Bag Session - Armory

Took the initiative and created and delivered a brown bag presentation introducing and explaining the Armory for stackArmor.

- Included a decent overview of the ThreatAlert product suite, which is also something most people don't have clarity on. 😊
- Created a visual metaphor of a factory/machine showing ATOM, the IaaS, TSW, TST, TCS, TSR, the GSS tools, and the application.
- Also created a self-paced video version that is available on the CX/CE Intranet site.




Also created a self-timed video for folks to watch...

Agenda:

- Quick review of the standard stackArmor offering
- Discussion of how The Armory is the same, and how it is different from stackArmor's historical offerings
- Review of The Armory deployment architecture
- A look at the value proposition of The Armory



For the video version of this presentation, just pause  to read the more content-rich slides!

July 22, 2025

Video Intro:



To understand Armory, we'll start with the standard stackArmor Offering:

stackArmor Customer

ISV SaaS

GSS

ATOM

TSM | Security Workbench

- The standard stackArmor customer engages ATOM automation to deploy GSS
- This initial establishment of the environment

Multiple “build” slides bridged these 2, basically showing the relationship between ThreatAlert elements and ISV applications...

TSW | Security Workbench

stackArmor Customer

Expert Services

Cloud Tools & Services

Secure Environment | SaaS VPC

ThreatAlert®

11

A story of 3 Authorized ISVs: Traditional stackArmor Model

The diagram illustrates the Traditional stackArmor Model architecture. It shows three separate ISV authentication boundaries (ISV 1, 2, and 3) each with its own ATO. Each ISV's architecture includes a ThreatArmor Workbench (TAW) connected to a ThreatArmor Connector (TAC), which in turn connects to a ThreatArmor Gateway (TAG). The TACs connect to a central ThreatArmor Management Console (TAMC). The TAMC is connected to a ThreatArmor Gateway (TAG) which connects to a ThreatArmor Gateway (TAG) which connects to a ThreatArmor Gateway (TAG).

The diagram illustrates the ISV 3 Auth Boundary: ISV 3's ATO. It shows a single ISV authentication boundary (ISV 3) with its own ATO. The architecture includes a ThreatArmor Workbench (TAW) connected to a ThreatArmor Connector (TAC), which in turn connects to a ThreatArmor Gateway (TAG). The TAC connects to a central ThreatArmor Management Console (TAMC). The TAMC is connected to a ThreatArmor Gateway (TAG) which connects to a ThreatArmor Gateway (TAG) which connects to a ThreatArmor Gateway (TAG).

- Each ISV has their own instance of the ThreatArmor GSS
- Each ISV has their own policies, procedures, SSP
- Each ISV has their own ATO and logo in the FedRAMP marketplace
- ISVs can be deployed on AWS, Azure or GCP

July 22, 2025

14

**Then I covered
3 deployment
models, the
traditional, then
Armory Hosted
and Armory
Managed...**

A story of 3 Authorized ISVs: Hosted Armory Model

3 Armory Hosted ISVs: Under a single Armory ATO

The diagram illustrates the Hosted Armory Model architecture. On the left, the **TSW Security Workbench** (Google Cloud) is connected to the **GSS** (Google Security Service) via a **Secure Environment / Host VPC**. The GSS is a central hub that manages various security services, including:

- TSM / CCB
- IMA / IAM / IAM
- Secure Logging
- Application Quarantining
- Endpoint Protection
- Host Security
- Host Patching

On the right, three **ISVs** (ISV 1, ISV 2, ISV 3) are shown, each with its own **Armory Container** and **Armory Container**. These ISVs are connected to the GSS and the Secure Environment / Host VPC. The ISVs are also connected to the **Armory Container** and **Armory Container**.

Below the diagram, the text reads: **Secure Environment / Host VPC**.

- Hosted ISVs are deployed and operated within the authorization boundary—ISV teams. (We don't directly operate their apps.)
- Each Hosted ISV is securely monitored using a single ThreatAlert GSS.
- Each ISV is represented by a team that adheres to the Armory policies, procedures, SRR, stack armor is the entity the ATO and logo in the FedRAMP marketplace (currently in the marketplace FedRAMP Ready).
- All Hosted ISVs are basic Armory "services", even if each is sold and licensed independently by that ISV to their distributors.

July 22, 2025

Processes and controls are under development

A story of 3 Authorized ISVs: Managed Armory Model

Armory Authorized GSS*

Armory Authorized GSS Architecture Diagram

3 Armory Managed ISVs: Each with their own ATO**

3 Armory Managed ISVs: Each with their own ATO**

- Managed Security/ComSec Services
- Armory Customer
- Armory Customer

*For simplicity, any hosted ISV, are not represented in this depiction of Armory, even though there would be hosted ISVs within the boundary... beginning with Qeios.

**This is not an architecturally accurate representation. Managed ISVs are assessed and monitored largely as some as hosted ISVs, but there is a significant difference in who is ultimately accountable for controls implementation and maintenance.

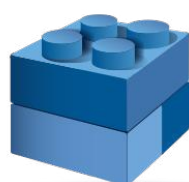
July 22, 2025

16

SWFTAlert New Offering Infographics

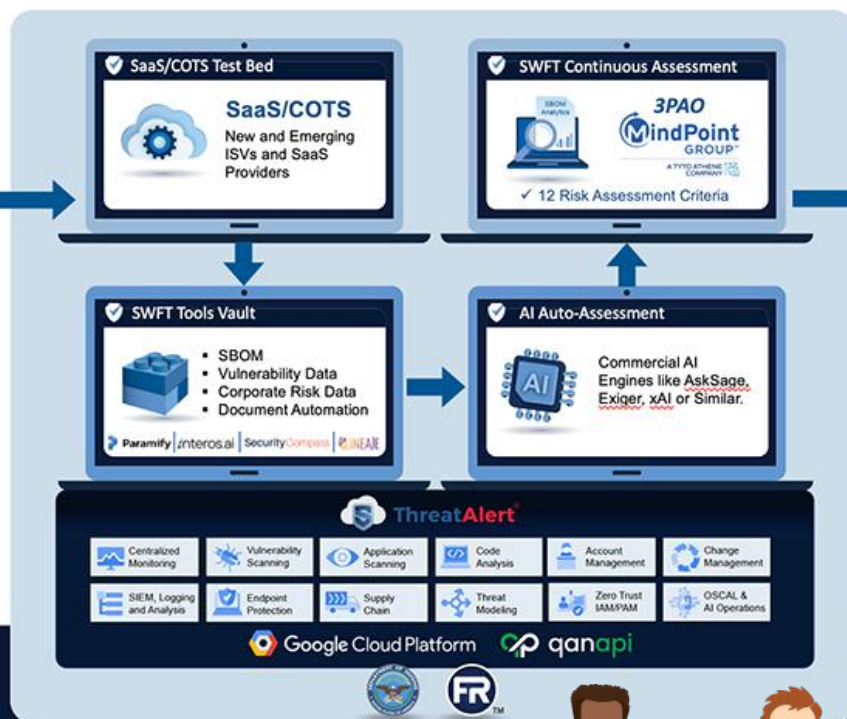
Created original infographics for GP to visually communicate the SWFTAlert Platform which is a proposed Continuous Assessment offering in cooperation with MindPoint Group.

- *Memorial Day Weekend Work*
- *Evolved the visual story telling approach from original concepts.*
- *Logos are original vector illustrations (infinitely scalable)*
- *All iconography is custom illustrated by me ☺*



stackArmor's SWFTAlert | Leading the charge to better manage and mitigate cloud computing risks

SWFTAlert Platform



Risk Mitigation Insights



5.26.2025

1



Built Robust TechTrend Slide Deck

Created a new “vibrant” PowerPoint template and used it for an Agentic AI and Modernized RMF presentation for Johann and Fawad.

- *Created animated GIFs to have movement in dotted lines/arrows.*
- *Helped craft the story and guide a meaningful flow*
- *Illustrated multiple new infographics to visually tell various stories.*
- *Lots of editing of stock photography throughout to get the right look.*
- *Lots of interesting use of pptx animations as well!*
- *Note: **Peter O'Donoghue** (Tyto CTO) asked who did the graphics, and commented that they were **better than “his guy’s”** 😊*

Challenges with AI in Today's Cybersecurity & Compliance Landscape

Modernizing Cybersecurity Operations for the Army and Enhancing RMF Compliance with Agentic AI

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Challenges with AI in Today's Cybersecurity & Compliance Landscape

Topics:

- Today's cybersecurity challenges (including AI-enabled adversaries)
- General challenges with using AI as part of today's systems
- Agentic AI-Driven Processes and Automations
- Agentic AI and Modernizing the RMF - Use case for cybersecurity and compliance solutions
- Governance and oversight considerations
- Benefits of AI and automation

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Today's Cybersecurity Challenge

- Adversaries are evolving their use of AI in their kill chain at warp speed
- The scale and frequency of attacks continues to rise exponentially
- 600 million cyber attacks are detected daily
- 12k cyber incidents have been recorded by DOD
- DOD's cyber workload remains intense with thousands of incidents requiring response and a budget to match
- Teams have to cover more cyber activities with lower budgets

The RMF of yesterday must be re-imagined and modernized -- leveraging the power of machine automation and Agentic AI to stay a step ahead of the adversaries in protecting our mission critical systems and the data it processes!

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Timeline of Major Cybersecurity Breaches

In spite of the Government's investment in cybersecurity and risk management, history shows we must continue improving and building on lessons learned.

- 2015 OPM Breach: 21.5M federal personnel records stolen
- 2018 DOD Travel Breach: PII and travel data of 30,000 DOD employees compromised
- 2020 Satellite Probe: Foreign actors attempted to infiltrate military satellite systems
- 2023 Microsoft Cloud Breach: Chinese hackers accessed DOD emails via token exploit
- Persistent theft of data from defense contractors
- Ongoing DIB Compromises

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Challenges of Integrating AI into Today's Systems

- Clearly Defining the Role(s) AI Can and Should Play in Modern Systems, and Choosing the Right Kind of AI (e.g. Agentic vs Generative)
- Trusting AI - Ensuring Integrity in AI Outputs and Actions
 - Addressing Risk and Security Issues Introduced by AI
 - Managing the Quality and Integrity of Data used to Inform AI Models
- Integration of AI with Legacy Systems
- Governance and Oversight

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

The Role of AI for Today's Cybersecurity Operations: Agentic AI Plus a Modernized RMF

Thinking beyond "Shift Left" to Re-imagining What's Possible.

- **Agentic AI** - The focus of this presentation, Agentic AI is used to address well-defined use cases and implemented with appropriate training models and guard rails. AI is an increasingly invaluable force multiplier for Cybersecurity Teams. AI is already in the hands of adversaries and permeates the threat landscape - so making AI a part of the solution is no longer revolutionary, but necessary.
- **Agentic AI as a Part of A Modernized RMF** - Shifting from a traditional RMF implementation to a more modern and integrated "data and machine-driven" approach turns things on their head - better addressing the intent of the original RMF for today's technologies. In today's systems, continuous monitoring and risk-posture information, controls compliance, and real-time system-state documentation should be derived from risk-mitigated, zero-trust, well-architected systems - not created outside of those systems.

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Trusting Agentic AI

Traceability by Design

- Unlike generative AI use cases, agents are tailored to execute precise, specific actions.
- AI agent actions are treated like privileged user actions and agents are treated like the ultimate insider threat.
- Immutable logging of prompts, model decisions, and downstream effects.
- AI agent activity is aligned with RMF workflow artifacts (e.g., audit trails, ATO evidence).

Assurance through Alignment

- MCP servers are secured as high-value/critical assets.
- Policy-as-code is used to govern AI inputs/outputs.
- NIST AI RMF is incorporated into system design to build provable trust.

Transparency for Defenders

- AI behavior is interpretable for cyber teams.
- Maintained visibility into model updates, data lineage, and system logic.
- AI-driven actions impacting security posture have explainable outcomes.

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Agentic AI Driven Process

Incorporating Agentic AI into today's systems helps automate and orchestrate complex system and cybersecurity operations in ways humans alone cannot.

- Utilize Model Context Protocol (MCP) server directed at telemetry/orchestration layer to:
 - Poll system states continuously and orchestrate AI agent actions based on operational triggers.
- Agentic approach deployed to autonomously support various aspects of SecOps and compliance.
 - Validate system changes in real-time.
 - Perform automated risk assessments.
 - Generate audit-ready evidence with minimal human input.
 - Create and update Component Definitions based on current, validated system state.

August 7, 2025 Proprietary and confidential information of stackArmor | A Tyto Athens Company

Force Multiplication Through Automation



- Reduces need to expand workforce for routine compliance tasks.
- Frees up skilled personnel to focus on mission-critical cybersecurity operations.
- Maintains continuous compliance without dedicated manual oversight.


August 7, 2025

Cyber AI Agent




August 7, 2025


The RMF Challenge



- The current process is slow, labor intensive, and not aligned to today's fast-paced, machine-driven system environments.
- Manual documentation under NIST SP 800-37 Rev. 2 is resource-intensive and error-prone.
 - Often the wrong resources with the wrong data are charged with documenting system state.
- Limited cybersecurity workforce capacity to support ongoing compliance.
 - Continuous control validation strains limited cyber resources.
- Compliance often lags behind system changes, creating audit and operational risk.
 - Instead of managing risk, RMF has become a source of risk.

August 7, 2025


Vision: A Modernized RMF Workflow



- Define via **GitOps** the desired system state using Policy-as-Code and Infrastructure-as-Code
 - Git repositories used to manage infrastructure and application configurations declaratively, where Git is the source of truth, and changes are automatically applied to environments through automation.
- Deploy via **DevSecOps** pipelines and GitOps principles.
- Embed **Continuous Validation** directly into infrastructure deployment workflows.
- Coordinate **Agentic AI** with MCP (Model Context Protocol) for intelligent, continuous monitoring and validation of assertions of system state.
- Collect Evidence by creating a "Data Lake" based on gathered assertions and gathered automated evidence.
- Automate Authorization Package generation and maintenance which is informed of the actual system state by content in the data lake.
- Continuously Monitor and update based on running system state via automation.

August 7, 2025


Define Policy and Controls Up Front



- Use Infrastructure as Code + Policy as Code to:
 - Define expected system state.
 - Establish control baselines.
 - Enforce approvals and traceability via GitOps.
- Policies drive system behavior and automation, not paperwork.
- Leverage Continuous Integration/Continuous Deployment (CI/CD) pipelines to deploy code and policy.
 - Introduce stage gates and approvals.
 - Run automated checks and validation prior to deployment.
 - Ensure consistency and accuracy of updates.

August 7, 2025

Telemetry/Orchestration Layer for Real-Time System State Validation



- Implement lightweight, plugin-based telemetry and query orchestration layer that polls live system configurations and security states using SQL-like queries across cloud and on-premises environments, providing real-time, structured data to drive automated compliance and security workflows.
- Derived Data Lake drives automation and orchestration.
- Stores:
 - Live system configurations.
 - Validation logs.
 - Control checks and outcomes.
- Generate real-time, audit-ready evidence.
- Enables transparency and continuous readiness.

August 7, 2025

Agentic AI for Automation and Orchestration




Agentic AI drives automation and orchestration of compliance and security operations, taking actions and delivering information based on system data.

- Enables continuous validation assertions of system state.
- Automates the creation of RMF artifacts, reducing manual errors.
- Reduces manual errors by automating repetitive tasks.
- Ensures that compliance workflows are up-to-date.

August 7, 2025

System Data Feeds Evidence Collection



Audit-Ready Evidence - GitOps pipelines combined with carefully designed Data Lakes provide:

- A complete audit trail with zero manual paperwork.
- Full traceability (who, what, when, why).
- Evidence of approvals and control validation.

Evidence of Cybersecurity Posture and Compliance Status are Live-State Driven:

- System Security Plans (SSPs), Implementation Statements, and Policy Docs are generated automatically from live, validated system state.
 - Powered by Authpack Automator + Component Definitions.
 - Uses modular, reusable Component Definitions for each control and capability.
- Updates are derived from changes in the running environment.

Cybersecurity Hygiene and Compliance are Aligned with DevSecOps Pipelines:

- Compliance keeps pace with mission system evolution, not something done after the fact.
- Documentation generation occurs during CI/CD deployment.

System Risk Posture and Status is Continuously Updated - As system configurations or controls change:

- Agentic AI and MCP validate new states.
- Updates are logged into the Data Lake.
- Documentation is generated continuously, ensuring alignment with system state.

August 7, 2025

System Data Powers Documentation

Using Component Definitions as Building Blocks of Control Implementation

Component Definitions:

- Are machine-readable reusable components that create a system control mappings.
- Allow the generation of an SSP in hours instead of weeks.
- Utilize the concept of a centralized location "registry" that can be leveraged by multiple systems on a network.

As the registry of components grows, the creation and management of documentation becomes exponentially faster.

06 | Automate Authorization Package

August 7, 2025

Proprietary and confidential information of stackArmor | A Tyto Athene Company

17

Modernized Systems Protect in Perpetuity

07 | Continuously Monitor and update

- Systems embracing a modern RMF model are architected to run via automation with machine-readable system state, compliance mappings, and continuous monitoring baked in.
- Agentic AI can be leveraged to deliver intelligent, continuous monitoring and validation of assertions of system state.
- SecOps teams are freed up to focus on exception handling and issues requiring human intuition and complex reasoning – with the automated system and AI capabilities serving as a significant force multiplier.
- Continuous monitoring is no longer an after thought, it's a core behavior of the designed system.

August 7, 2025

Proprietary and confidential information of stackArmor | A Tyto Athene Company

18

Governance and Oversight

Governance standards and oversight methodologies for systems leveraging AI need to evolve to align with the unique risks and challenges introduced to systems by AI features.

While this presentation won't define specific governance and oversight solutions for systems with AI capabilities, the following foundational principles hold true:

AI Functions Must be Transparent, Auditable and Traceable

- AI behavior must be interpretable for cyber teams and operations teams.
- Systems must provide visibility into model updates, data lineage, and system logic.
- AI-driven actions impacting security posture must have explainable outcomes.

August 7, 2025

Proprietary and confidential information of stackArmor | A Tyto Athene Company

Outcomes for Cybersecurity Teams

- Accelerated risk mitigation and authorization timelines.
- Scalable compliance without expanding workforce.
- Continuous monitoring and compliance maintenance that is reflective of the running state of the system.
 - The state of the system remains transparent and fully auditable in near real-time.
- Enables teams to focus on mission-critical objectives.
- Stronger security posture aligned with DoD Zero Trust Strategy.

August 7, 2025

Proprietary and confidential information of stackArmor | A Tyto Athene Company

20

Thank You

www.stackarmor.com

August 7, 2025

Proprietary and confidential information of stackArmor | A Tyto Athene Company

Illustrated and Animated stackArmor Offering Gears Infographic

Created a specific infographic at Martin's request to show stackArmor offerings working seamlessly together as an engine.

- All original vector illustrations were saved out gear by gear, icon by icon, so they could be animated in a slide-build sequence.
- Gears spun in colored clusters aligned to the story, while the icons stayed stable. In the end, the entire machine had gears moving in sync!



Illustrated and Animated stackArmor Offering Gears Infographic Cont...

This is a movie version of the animated PowerPoint slide I created.

Professional Growth

Attended UX Camp 2025

Registered for and attended a Saturday seminar focused on UX topics. I specifically signed up because this particular camp was focused on the relationship between UX and cybersecurity/risk.

- *Speaker/Author on UX and Cybersecurity – No surprise, cybersecurity tooling UX plays a huge role in risk posture and effective SecOps ☺*
- *Was introduced to some new UX tooling, and the emerging role of AI in the UX arena*
- *Intro to Web3 and the state of technology wrt UX*

UX Camps are dynamic, single-day mini-conferences designed to fuel the passion of the UX Design community. Featuring a blend of curated keynotes and community-sourced speakers, each camp offers a platform for sharing innovative ideas, practical UX methodologies, and insightful design strategies. Whether you're a seasoned UX professional or just embarking on your design journey, UX Camps provide a rich environment for learning, networking, and inspiration.



UX Camp Winter 2025

CAMP

March 1, 2025

Flex Forward at UX Camp Winter 2025 Saturday, March 1, 2025 at 10am Central! Flexing Forward: Showcasing Our Evolution Flexing Forward is an invitation for us to demonstrate how we've grown and adapted over the past year. It's time to...



Took a Harvard Mini Course on Leadership

[Back To All Lessons](#)[Sign Out](#)

Resilient Leadership

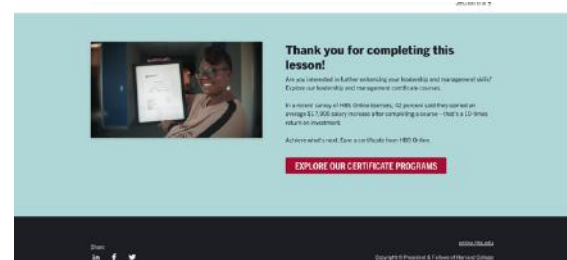


Introduction

In this two-part lesson, you'll gain insight into leading through adversity through the example of explorer Ernest Shackleton and his historic Endurance expedition.

TL;DR:

- **Attitude** trumps all when hiring (over tech skills, grit, creativity, experience, etc.)
- **Team camaraderie** is the key to success - people first (communicate, interact, “play”, let the people know they matter)
- Leaders manage their team’s individual and group **energy** – especially during uncertainty
- Leaders easily and **effortlessly shift** between hands-on tasks and visionary leadership
- Never let negativity or naysayers get in the way of the mission (keep negative influencers close, **prevent the spread of negativity**)
- **Flexibility matters** – sometimes the target has to change
- **Leaders own it** – and model this, instilling confidence and team commitment
- Leaders bring/model **positive energy**
- Leaders stay **forward thinking** always

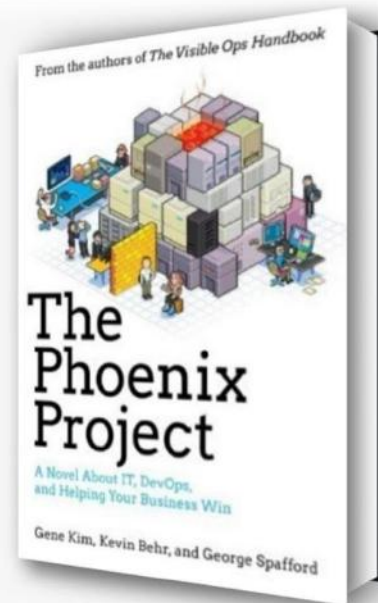


Read the Phoenix Project (per Ask from GP)

GP actually asked me to read this, and when I did, I understood why. Lots of alignment to some of the things I was talking about (and have been trying to implement). While I don't agree with everything in the book, there were some good takeaways and things I can grow from.

TL;DR:

- **There are 3 Ways (DevOps Core Principles)**
 - **Flow**: Prioritize fast delivery of work from development to operations.
 - **Feedback**: Enable quick feedback loops to detect and resolve problems.
 - **Continuous Learning**: Encourage experimentation and learning from failure.
- **Treat IT Work as a Machine/Manufacturing System**
 - **Visualize and manage the flow of work like an assembly line. (e.g. journey mapping!!!)**
 - **Limit Work-In-Progress** (WIP) and complete tasks before starting new ones.
- **Address/Control Unplanned Work!!!**
 - **Unplanned work disrupts flow** and reduces capacity for planned initiatives.
 - Visibility, prioritization, and root-cause analysis help reduce unplanned tasks.
- **Apply the Theory of Constraints**
 - Identify a system's bottlenecks and optimize those (this can be a person spread too thin).
 - Do not focus on areas that are not constraints as they don't improve throughput.
- **Break Down Silos and Align Teams**
 - **Development, QA, Security, and EMs/Operations must collaborate.**
 - Shared goals and accountability enable faster, more reliable delivery.



2024 25

Thank You!

Sarah Hensley

Annual Performance Report