



Opsfolio

Lead Magnets Tour

Table of Contents

- Opsfolio Lead Magnets Tour2
 - Overview.....2
- 1. Customer Journey Overview3
 - Typical Lead Journey3
- 2. Landing Pages & Campaign Experience3
 - Example Public Landing Pages3
 - Landing Page Goals4
- 3. Sign-Up & User Inputs4
 - Initial Sign-Up Information4
- 4. Assessment Experience5
 - CMMC Assessments5
 - SOC 2 Readiness Assessments6
 - HIPAA Self-Assessment6
- 5. Automated Emails & Customer Touchpoints7
 - Automated Customer Experience7
- 6. Reports & Outputs Generated9
 - CMMC Level 1 Reports9
 - CMMC Level 2 Reports 10
 - SOC 2 Readiness Reports 11
 - HIPAA Self-Assessment Reports 12
- 7. How Channel Partners Can Use the System 13
 - Partner-Driven Campaigns 13
 - Why This Matters for Partners 13
- 8. CMMC Customer Journey 14
 - Customer Workflow 14
 - Phase 1: Level Determination and Routing 15
 - Phase 2: CMMC Level 1 Assessment..... 15
 - Phase 3: CMMC Level 2 Assessment..... 15
- 9. Current Capabilities 16
- 10. Business Value..... 16
- Final Summary..... 17

Opsfolio Lead Magnets Tour

This document is intended for marketing agencies, channel partners, prospective partners, sales enablement teams, and external GTM collaborators. It covers what currently works: the customer-facing assessment journey, landing pages, reports users receive, email touchpoints, and how partners can use the system. For internal operational details, automation architecture, and roadmap planning, refer to the companion internal document.

Overview

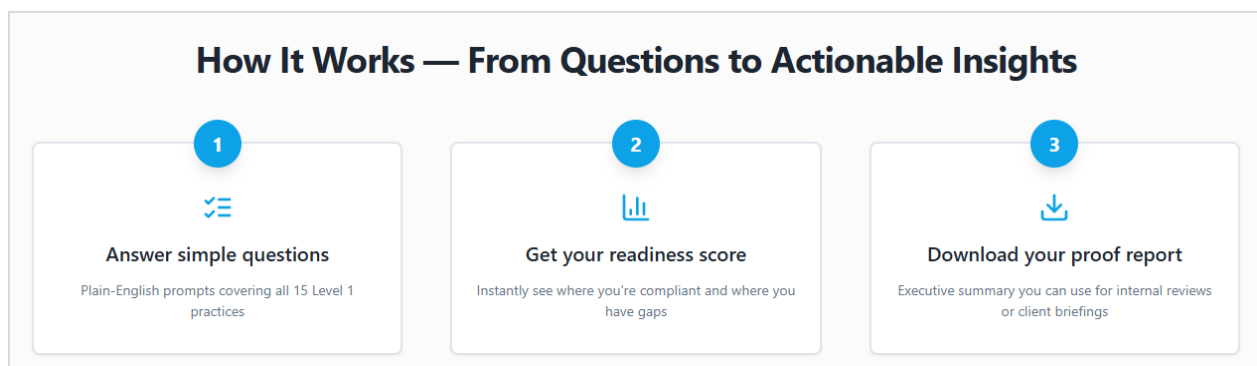
Opsfolio's **CMMC** and **SOC 2** compliance readiness tools are designed to reduce friction and enable self-assessment, helping organizations evaluate their cybersecurity and compliance posture through guided Readiness Assessments and Self-Assessments.

These workflows are intentionally designed to:

- Reduce friction during initial engagement and enable self-service assessment
- Help prospects understand their current readiness position
- Generate immediate value through automated self-assessment reports
- Enable channel partners to engage prospects at scale
- Create structured follow-up opportunities for consulting and remediation services

These tools function as a customer-facing compliance engagement experience, currently focused on Readiness Assessments and Self-Assessments, combining:

- Landing pages
- Guided assessments
- Automated report generation
- Email touchpoints
- Readiness scoring
- Partner-branded engagement workflows



1. Customer Journey Overview

Typical Lead Journey

1. Prospect receives a campaign link or visits a landing page
2. Prospect signs up using a simple form
3. Prospect starts the compliance readiness assessment
4. Assessment questions guide the user through their current compliance posture
5. Readiness calculations are performed automatically
6. A report or readiness summary is generated
7. Follow-up conversations can be initiated by the partner
8. Customer progresses toward remediation and compliance engagement

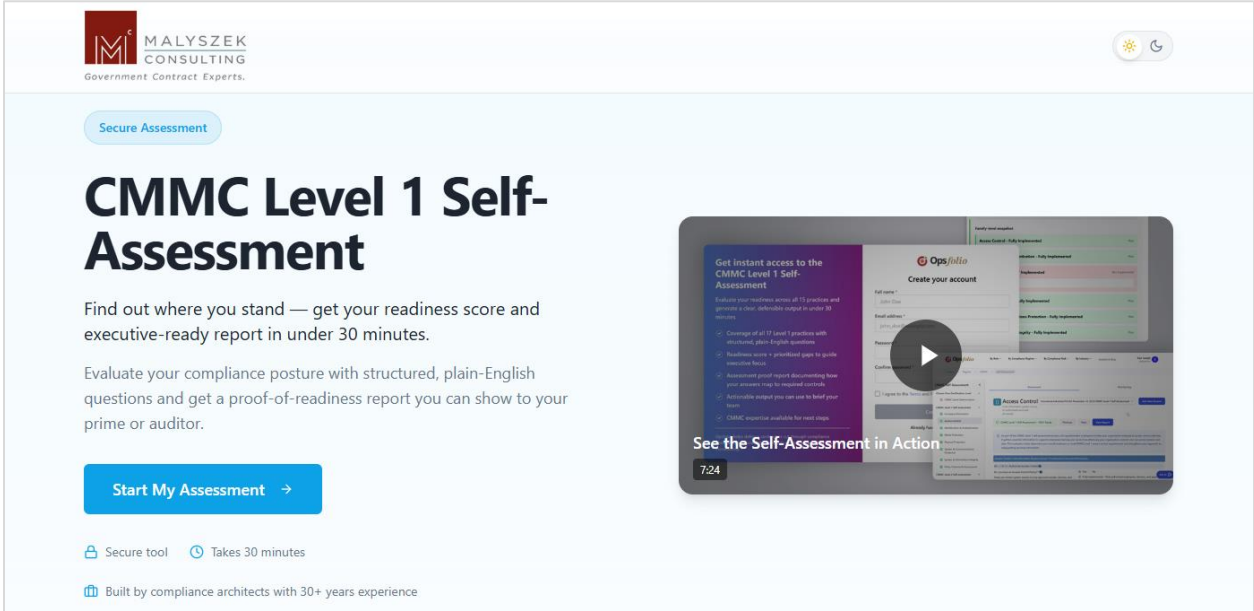
The process is designed to feel lightweight, guided, and self-service.

2. Landing Pages & Campaign Experience

Example Public Landing Pages

Opsfolio – CMMC Level 1 Self-Assessment
<https://opsfolio.com/regime/cmmc/self-assessment-landing/>

Opsfolio – Self-Assessment Malyszek
<https://opsfolio.com/lp/cmmc/self-assess-malyszek/>
<https://opsfolio.com/lp/cmmc/self-assess-malscmmc/>



Landing Page Goals

The landing pages are designed to:

- Introduce compliance-readiness assessments
- Explain the business value of self-assessment
- Encourage immediate engagement
- Capture prospect information
- Guide users toward assessment completion

Typical landing page elements include:

- Compliance overview
- Business-risk positioning
- Readiness messaging
- Assessment entry points
- Call-to-action buttons
- Lead capture forms
- Partner branding

3. Sign-Up & User Inputs

Get instant access to the CMMC Level 1 Self-Assessment

Evaluate your readiness across all 15 practices and generate a clear, defensible output in under 30 minutes.

- ✓ Coverage of all 17 Level 1 practices with structured, plain-English questions
- ✓ Readiness score + prioritized gaps to guide executive focus
- ✓ Assessment proof report documenting how your answers map to required controls
- ✓ Actionable output you can use to brief your team
- ✓ CMMC expertise available for next steps

Opsfolio helps defense contractors cut through compliance uncertainty with credible, standards-aligned outputs you can act on immediately.

Opsfolio

Create your account

Full name *
John Doe

Email address *
john.doe@example.com

Password *
.....

Confirm password *
.....

I agree to the [Terms](#) and [Privacy Policy](#).

Create account

Already have an account? [Sign in](#)

Initial Sign-Up Information

The current workflows typically collect:

- First Name
- Last Name
- Email Address

Additional information may be collected throughout the assessment process depending on the workflow.

4. Assessment Experience

CMMC Assessments

The CMMC Self-Assessment walks users through a structured series of questions covering their current security practices. The experience is guided and self-service, covering areas such as:

- Questions to determine the applicable CMMC level
- Current security practices and controls
- Existing policies and documented processes
- How access to systems and data is managed
- Incident response and recovery preparedness
- Risk management and vendor oversight practices
- Documentation and day-to-day operational practices

A screenshot of the Opsfolio CMMC Self-Assessment web application. The interface shows a navigation menu on the left with 'CMMC Level Determination' selected. The main content area is titled 'CMMC Level Determination' and includes a 'Resume an existing session' dropdown and a 'Start New Session' button. A message states: 'No session is selected. Choose one from the dropdown to resume, or use Start New Session and save this first step to create a new assessment session.' Below this is a blue box with the text: 'This questionnaire helps organizations determine the appropriate CMMC certification level based on their handling of FCI and CUI.' The questionnaire is divided into sections: 'Section 1: Organization and Contract Information' and 'Section 2: Type of Information Handled'. Section 1 includes questions about organization name, DoD contracts, and CMMC level requirements. Section 2 includes questions about the types of information handled (Public, CUI, FCI, etc.) and technical data handling.

At the end of the assessment, users receive a clear picture of:

- Where they likely stand against CMMC requirements
- Specific areas that need attention before certification
- A starting point for remediation conversations

SOC 2 Readiness Assessments

The SOC 2 Self-Assessment guides users through a structured review of their operational and security practices. It covers areas such as:

- How security governance and oversight is structured
- Operational controls currently in place
- Readiness for an external SOC 2 audit
- Availability of evidence and supporting documentation
- User access management and identity practices
- Monitoring, logging, and operational procedures



The completed assessment gives organizations a practical, directional view of where they stand and what to address before pursuing a SOC 2 audit.

The screenshot displays the Opsfolio SOC 2 Readiness Assessment interface. The top navigation bar includes the Opsfolio logo, 'Explore Solutions', 'Operational Truth™', 'Insights & Blog', and user information for 'Ajay'. The breadcrumb trail shows 'Home > Regime > SOC2 > Readiness Assessment'. The left sidebar lists assessment categories: 'SOC 2 Readiness Assessment' (expanded), 'SOC 2 Type 1 Readiness Assessment' (expanded), and 'SOC 2 Type 2 Readiness Assessment'. Under 'SOC 2 Type 1 Readiness Assessment', 'General Information' is selected. The main content area shows 'General Information' as 'Step 1 of the SOC 2 Type 1 readiness assessment'. A progress indicator shows 'SOC 2 Type 1 Readiness Assessment – 0% Ready'. A 'Start New Session' button is present. A message states: 'No session is selected. Choose one from the dropdown to resume, or use Start New Session and save this first step to create a new assessment session.' Below this is a blue box with a link: 'Collect organizational context, contact information, product details, and the baseline audit details needed to start the SOC 2 Type 1 readiness review.' The 'General Information Evidence Collection Form' includes fields for: Organization Name, Organization Address, Product Name, Website, Point of Contact, Contact Email, and Date of Submission. Navigation buttons 'Previous' and 'Next' are visible at the bottom of the form area.

HIPAA Self-Assessment

The HIPAA Self-Assessment guides users through a structured, four-step review of their organization's current safeguard implementation. The experience is guided and self-service, covering:

- Company and contact information

- **Administrative Safeguards:** security management, workforce access, training, incident response, and contingency planning (164.308)
- **Physical Safeguards:** facility access, workstation controls, and device and media handling (164.310)
- **Technical Safeguards:** access controls, audit controls, data integrity, authentication, and transmission security (164.312)



At the end of the assessment, users can view their report immediately via the View Report button, which is available throughout the workflow once the session is saved.

The screenshot displays the Opsfolio HIPAA Self-Assessment interface. The top navigation bar includes the Opsfolio logo and user information (Netspective, Ajay). The breadcrumb trail shows 'Home > Regime > HIPAA > Self Assessment'. The left sidebar lists assessment categories: Company Information, Administrative Safeguards (selected), Physical Safeguards, and Technical Safeguards. The main content area is titled 'Administrative Safeguards' and shows 'Step 2 of HIPAA Self-Assessment'. A progress indicator indicates 'HIPAA Self-Assessment - 100% Ready'. Below this, there are navigation buttons for 'Previous', 'Next', and 'View Report'. The assessment questions are listed as follows:

- 164.308 Administrative Safeguards
- 164.308(a) Internal Policies & Procedures
- 164.308(a)(1) Security management process
- 164.308(a)(1)(i) Have you implemented policies and procedures to prevent, detect, contain, and correct security violations? Yes No Not Applicable
- 164.308(a)(1)(ii)(A) Has a risk analysis been completed using IAW NIST Guidelines? * Yes No Not Applicable
- 164.308(a)(1)(ii)(B) Has the risk management process been completed using IAW NIST Guidelines? * Yes No Not Applicable
- 164.308(a)(1)(ii)(C) Do you have formal sanctions against employees who fail to comply with security policies and procedures? * Yes No Not Applicable
- 164.308(a)(1)(ii)(D) Have you implemented procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking? * Yes No Not Applicable
- 164.308(a)(2) Assigned security responsibility
- 164.308(a)(2)(i) Have you identify the security official who is responsible for the Yes No Not Applicable

5. Automated Emails & Customer Touchpoints

Automated Customer Experience

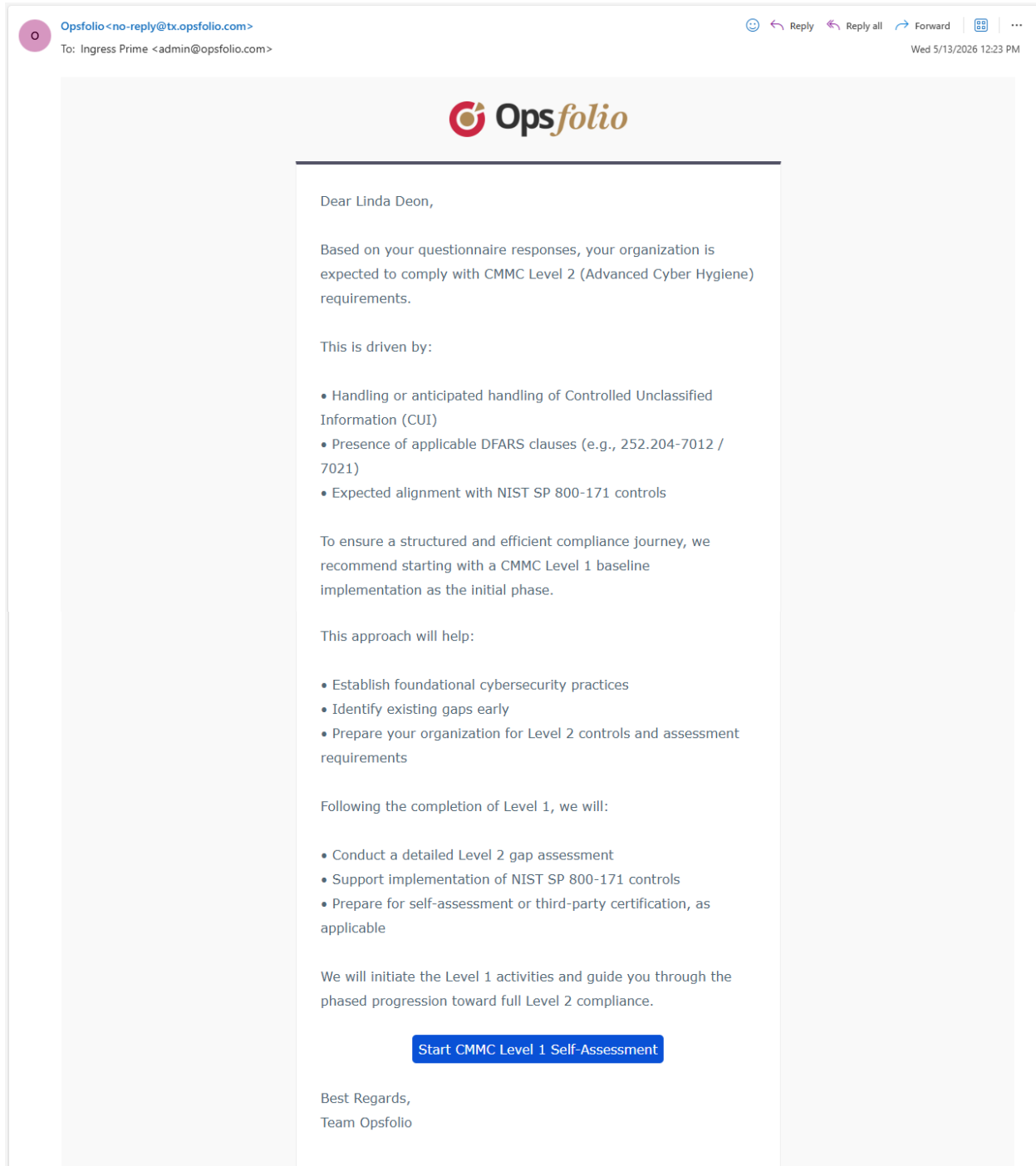
Several workflows currently trigger automated customer-facing emails.

Examples include:

- Assessment initiation notifications
- Workflow-based email responses

- Level determination follow-up emails
- Report delivery emails

These touchpoints help maintain engagement during the assessment journey.



The screenshot shows an email interface. At the top left, the sender is 'Opsfolio <no-reply@tx.opsfolio.com>' and the recipient is 'Ingress Prime <admin@opsfolio.com>'. The top right shows email actions: 'Reply', 'Reply all', 'Forward', and a date 'Wed 5/13/2026 12:23 PM'. The main content area features the Opsfolio logo at the top. The email body is as follows:

Dear Linda Deon,

Based on your questionnaire responses, your organization is expected to comply with CMMC Level 2 (Advanced Cyber Hygiene) requirements.

This is driven by:

- Handling or anticipated handling of Controlled Unclassified Information (CUI)
- Presence of applicable DFARS clauses (e.g., 252.204-7012 / 7021)
- Expected alignment with NIST SP 800-171 controls

To ensure a structured and efficient compliance journey, we recommend starting with a CMMC Level 1 baseline implementation as the initial phase.

This approach will help:

- Establish foundational cybersecurity practices
- Identify existing gaps early
- Prepare your organization for Level 2 controls and assessment requirements

Following the completion of Level 1, we will:

- Conduct a detailed Level 2 gap assessment
- Support implementation of NIST SP 800-171 controls
- Prepare for self-assessment or third-party certification, as applicable

We will initiate the Level 1 activities and guide you through the phased progression toward full Level 2 compliance.

[Start CMMC Level 1 Self-Assessment](#)

Best Regards,
Team Opsfolio

6. Reports & Outputs Generated

CMMC Level 1 Reports

Upon successful completion of the CMMC Level 1 Self-Assessment:

- A self-assessment report is automatically generated
- A report link is delivered to the user

CMMC Level 1 - Self-Assessment Report
Generated from submitted forms

Executive Summary

Session Name: CMMC Level 1 Assessment. January 05, 2026 CMMC Level 1 Self-Assessment
Scope: Responses from submitted CMMC Level 1 questionnaires.
Assessment Date: Thu May 14 2026

≈ 100%
Overall readiness (by families submitted)
(partial / demonstrable controls - see notes)

Compliance Note: CMMC Level 1 requires **all 17 practices** to be fully implemented. Any score less than **100%** means you are **not yet compliant**.

Family-level snapshot

Access Control - Fully Implemented	<i>Pass</i>
Identification & Authentication - Fully Implemented	<i>Pass</i>

The self-assessment reports help organizations understand:

- Current readiness status
- Compliance gaps
- Areas requiring additional work
- Suggested improvement focus areas

CMMC Level 2 Reports

Upon successful completion of the CMMC Level 2 Self-Assessment:

- A self-assessment report is automatically generated
- A report link is delivered to the user

Assessment Status report for CMMC Level 2
Generated from submitted forms

Executive Summary

Session Name: CMMC Level 2 Assessment January 05, 2026 CMMC Level 2 Self-Assessment
Organization: CMMC Level 2 Assessment
Completed By: Ann
Email: ann-jose@netspective.in
Scope: Responses from submitted CMMC Level 2 questionnaires.
Assessment Date: Thu May 14 2026

≈ 92%

Overall readiness (by domains submitted)

94 fully implemented, 15 partially implemented, 1 not implemented

Assessment Note: This report is a readiness summary based on submitted answers. A formal CMMC Level 2 outcome still depends on complete implementation, supporting evidence, and assessor review where applicable.

Domain-level snapshot

Access Control - Needs Work91% readiness

The report helps organizations understand:

- Current readiness status across all 14 CMMC Level 2 practice domains
- Practice-level compliance gaps and areas of partial implementation
- Which of the 110 required practices are met, partially met, or not yet addressed
- Recommended focus areas before engaging a C3PAO for formal assessment
- An overall readiness posture summary

The Level 2 self-assessment report gives organizations a structured, practice-level view of their current compliance posture and a concrete starting point for remediation planning.

SOC 2 Readiness Reports

SOC 2 readiness workflows generate:

- Self-assessment report summarizing readiness findings
- Gap-oriented observations
- Operational maturity indicators
- Directional compliance insights

These self-assessment reports are intended to serve as starting points for deeper readiness discussions.

SOC 2 READINESS REPORT
Print Assessment

SOC 2 Type 1 Readiness Assessment

CERTIFICATE OF READINESS

BlueWave Defense Systems LLC

Foundational controls are forming, though consistency and evidence quality still need work before you can claim strong readiness.

READINESS SCORE

61%

In Progress

ASSESSMENT SESSION

BlueWave Defense Systems LLC April 20, 2026 SOC 2 Type 1 Readiness Assessment

2026-04-20

ISSUED TO

BlueWave Defense Systems LLC

Scope: SOC 2 Type 1 Readiness Assessment

Product: akon

Contact: test • akon.2021@mail.com

Website: https://www.akon111.com

Evidence artifacts noted: 2

This readiness certificate summarizes submitted assessment responses and evidence references. It is not a SOC 2 audit opinion or formal certification.

COMPLETED DOMAINS

11/11

OVERALL READINESS

In Progress

EVIDENCE LINKS

2

SUBMISSION DATE

2026-04-20

DOMAIN SNAPSHOT

Control-by-control readiness

General Information 69% • In Progress

7 answered items • 2 evidence-rich responses

QUESTION	YOUR ANSWER	OBSERVATION
Organization Name	BlueWave Defense Systems LLC	Detailed narrative provided.
Organization Address	Alton	Response captured.
Product Name	akon	Response captured.
Website	https://www.akon111.com	Evidence link provided.
Point of Contact	test	Response captured.

STRENGTHS

What already looks strong

Logical and Physical Access: Are information security policies and procedures in place to communicate managements requirements with regards to user account security, appropriate handling of information systems data, privacy standards, etc.?: Yes

Control Environment: Are core values are communicated from executive management to personnel through policies and the employee handbook?: Yes

Risk Assessment: Please describe your annual risk assessment process in regards to your service under review. (i.e., Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.): Yes

HIPAA Self-Assessment Reports

Upon successful completion of the HIPAA Self-Assessment:

- A self-assessment report is automatically generated
- A report link is delivered to the user



The report helps organizations understand:

- Overall safeguards readiness score across all HIPAA Security Rule controls
- Section-level scores for Administrative, Physical, and Technical Safeguards
- A breakdown of controls reviewed with Yes, No, and Not Applicable counts
- Specific priority gaps tied to individual 164.308, 164.310, and 164.312 regulation references

- The user's own responses and explanations captured against each gap item

The HIPAA Self-Assessment report gives healthcare organizations and their business associates a structured, regulation-referenced view of their current safeguard posture and a prioritized starting point for remediation.

7. How Channel Partners Can Use the System

Partner-Driven Campaigns

These Readiness Assessment and Self-Assessment tools are designed to support partner-led engagement models.

Channel partners can:

- Share branded campaign links
- Run outreach campaigns
- Use custom landing pages
- Receive customer engagement visibility
- Use generated reports for follow-up conversations
- Position remediation and consulting services

The [Malyszek](#) implementation is an example of this partner-driven model.

Why This Matters for Partners

The workflows help partners:

- Start conversations faster
- Reduce manual discovery effort
- Generate compliance discussions earlier
- Create consulting opportunities
- Scale outreach without large technical teams

Instead of beginning with generic cybersecurity conversations, partners can immediately discuss:

- Readiness findings
- Gap areas
- Business risks
- Improvement opportunities

8. CMMC Customer Journey

The diagram below maps the full CMMC customer journey from initial awareness through to Level 1 or Level 2 compliance completion. It shows three distinct phases across two swim lanes: the customer's actions and Netspective's supporting workflow at each stage.

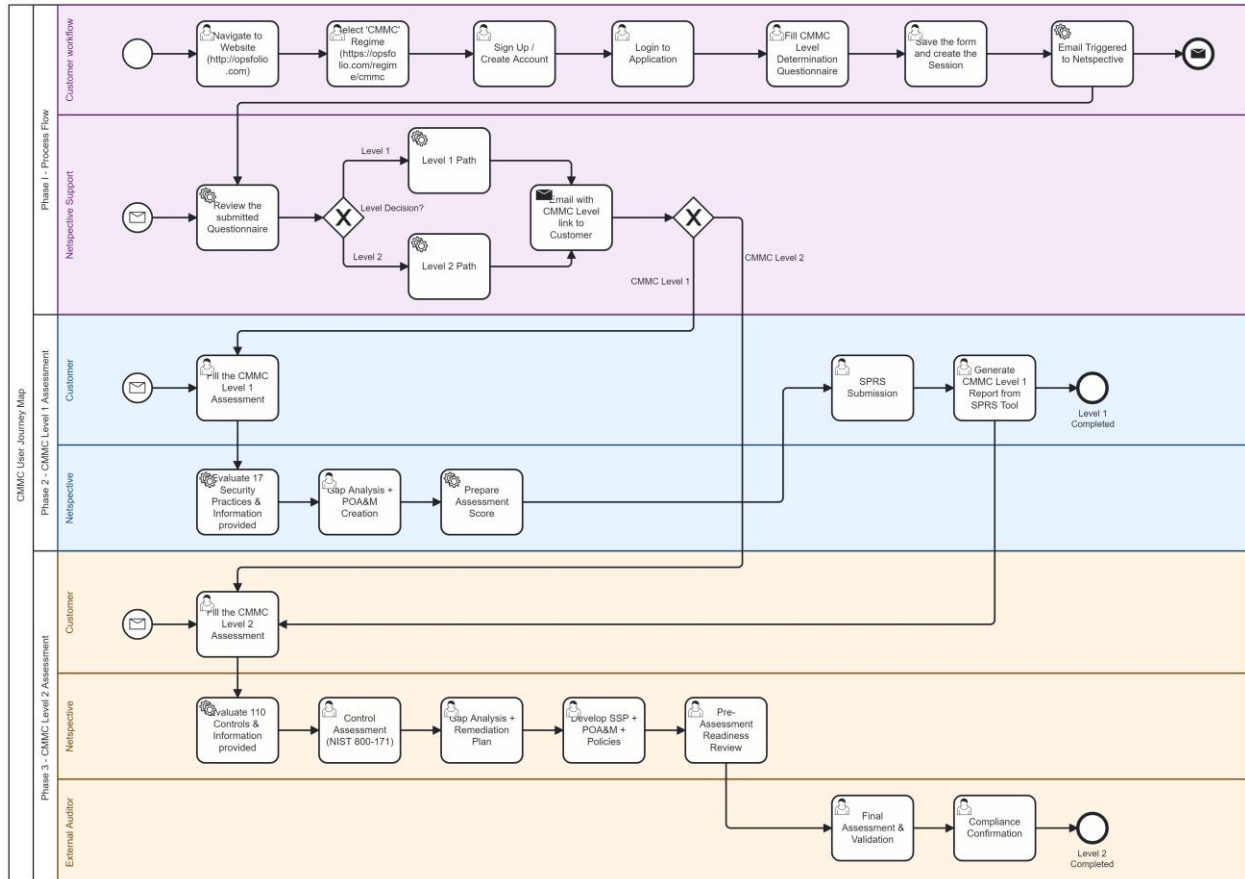


Figure: CMMC Customer Journey Map - from initial website visit through Level 1 or Level 2 completion

Customer Workflow

This is the top swim lane and shows the actions taken by the customer from the very start of their journey. The customer:

- Navigates to the Opsfolio website (opsfolio.com)
- Selects the CMMC Regime (opsfolio.com/regime/cmmc)
- Signs up or creates an account
- Logs in to the application
- Fills in the CMMC Level Determination Questionnaire
- Saves the form and creates the session, triggering an automated email to Netspective

Phase 1: Level Determination and Routing

Once the customer's questionnaire is submitted, Netspective reviews the session and determines the appropriate CMMC level. This is a short routing phase:

- Netspective reviews the submitted questionnaire
- A level decision is made: Level 1 or Level 2
- An email is sent to the customer with a link to their appropriate CMMC level assessment
- Customer follows the Level 1 or Level 2 path depending on the outcome

Phase 2: CMMC Level 1 Assessment

For customers routed to Level 1, the journey follows a self-assessment path supported by Netspective's evaluation workflow.

Customer actions:

- Fills in the CMMC Level 1 Assessment in the Opsfolio Web App
- Completes SPRS submission
- Generates the CMMC Level 1 Self-Assessment Report from the SPRS tool
- Level 1 journey is complete

Netspective supporting workflow:

- Evaluates the 17 security practices and information provided by the customer
- Performs gap analysis and creates a POA&M
- Prepares the assessment score

Phase 3: CMMC Level 2 Assessment

For customers routed to Level 2, or who progress from Level 1, the journey continues into a more rigorous assessment supported by both Netspective and an External Auditor.

Customer actions:

- Fills in the CMMC Level 2 Assessment in the Opsfolio Web App

Netspective supporting workflow:

- Evaluates all 110 controls and the information provided, against NIST 800-171
- Performs a Control Assessment (NIST 800-171)
- Produces a Gap Analysis and Remediation Plan
- Develops SSP, POA&M, and supporting Policies

- Conducts a Pre-Assessment Readiness Review

External Auditor (C3PAO):

- Conducts the Final Assessment and Validation
- Issues Compliance Confirmation, completing the Level 2 journey

9. Current Capabilities

Partners and external collaborators can count on the following being available and working today:

- Live public landing pages with campaign and partner-branded variants
- Guided CMMC and SOC 2 Self-Assessments that prospects can complete independently
- Automated self-assessment reports delivered to prospects upon completion
- Automated assessment-triggered emails keeping prospects informed at each stage
- Partner visibility into prospect engagement and assessment completion
- A self-service experience prospects can complete in under 30 minutes

Self-assessment reports available today:

- CMMC Level 1 Self-Assessment report
- SOC 2 Readiness Self-Assessment report
- CMMC Level 2 Self-Assessment report

10. Business Value

These tools help transform compliance engagement from:

Traditional Manual Discovery → Guided Automated Readiness Engagement

This creates value for:

- Customers seeking quick readiness visibility
- Channel partners needing scalable outreach
- GTM teams looking for engagement acceleration
- Consulting organizations seeking qualified compliance leads

Final Summary

Opsfolio's Readiness Assessment and Self-Assessment tools provide a structured, customer-friendly compliance engagement experience that combines:

- Readiness assessments
- Automated reporting
- Partner-led engagement
- Customer education
- Compliance awareness
- Funnel acceleration

The workflows help prospects quickly understand where they stand while giving partners and GTM teams a scalable way to initiate meaningful compliance-readiness conversations.