**ASM Playbook: Vulnerability Reporting & Advisory**

**Focus: Turn raw scan data from CDC/third party into actionable insights**

**📌 Purpose**

To ensure Account Security Managers act as trusted advisors by transforming vulnerability scan results into business-relevant risk reports, supporting remediation planning, and driving stakeholder engagement.

**🧭 Process Overview**

1. **Initiate & Scope Engagement**
2. **Coordinate with CDC/Third Party for Scan Execution**
3. **Enrich Vulnerability Data (CVSS, Exploitability, Business Context)**
4. **Prepare Standardized Report**
5. **Present Results to Stakeholders & Drive Action**
6. **Track Remediation & Lessons Learned**

**✅ 1. Initiate & Scope Engagement**

**ASM Actions:**

* Use intake form to collect:
  + Business owner and technical contact
  + Asset list / system names / environment
  + Business criticality (e.g., customer-facing, internal ops)
* Agree on scan frequency and follow-up cadence (monthly, quarterly)

**🤝 2. Coordinate with CDC/Third Party**

**ASM Actions:**

* Submit request or confirm scan plan with CDC/partner
* Track when scans are scheduled and completed
* Ensure proper asset tagging or grouping for meaningful reporting
* Validate that critical systems are in scope and credentials are valid (if authenticated scans are planned)

**🧠 3. Enrich Vulnerability Data**

**ASM Enrichment Areas:**

* **CVSS Base Score**
* **Known exploits** (e.g., Exploit-DB, CISA KEV list)
* **Business impact** of vulnerable assets
* **Repeat findings** or long-standing issues
* **Patch availability or workarounds**

**Tools & Data Sources:**

* NIST NVD
* Vulners or ThreatConnect API
* MITRE ATT&CK mapping
* Previous scan reports for comparison

**📄 4. Prepare the Report**

**Use the Standard Format:**

* **Executive Summary:**
  + Top 5 risks (based on impact + exploitability)
  + Trends since last scan
  + Risk to business operations
* **Risk Categorization:**
  + Based on CVSS + asset criticality + threat context
  + E.g., "High risk: Unpatched RCE on payment system server"
* **Remediation Guidance:**
  + Practical, prioritized actions (patch, config change, compensating control)
  + Suggested owner and remediation timeline
* **Appendices:**
  + Full list of findings
  + False positive notes (if applicable)

**🎤 5. Present & Advise**

**ASM Actions:**

* Schedule a walkthrough meeting with key stakeholders
* Focus discussion on:
  + Top business risks
  + What needs to happen in next 7/14/30 days
  + Dependencies on IT, cloud, or other teams
* Document action items and ownership

**📊 6. Track & Improve**

**ASM Actions:**

* Follow up on remediation timelines
* Track metrics like:
  + Open critical vulnerabilities over time
  + Avg. remediation time
  + Number of repeat findings
  + Stakeholder feedback
* Log lessons learned or process issues (e.g., scan missed hosts, false positives)

**✨ Extra Value Add (Optional for Maturity Growth)**

* Create dashboards for business units with top risks
* Offer comparative reports ("you vs. similar BU X")
* Trend analysis across multiple quarters
* Map vulnerabilities to compliance gaps (e.g., NIS2, ISO 27001 controls)

## Your Key Concept: ****Risk-Weighted Exposure Score (RWES)****

Instead of counting all findings equally, assign a **weighted score** to each based on:

| **Factor** | **Weight** |
| --- | --- |
| CVSS score (v3) | Base (0–10) |
| Exploitability (known public exploit?) | +5 |
| Asset criticality (e.g., customer-facing) | ×1.5 |
| Repeat finding (not fixed over 2+ scans) | +3 |

### 🧮 Sample RWES formula per finding:

### RWES = (CVSS + Exploitability bonus + Repeat bonus) × Asset Criticality Weight

### Then sum it up across all findings in the scan/report for a total **exposure score**. This is your **risk temperature** for that unit/system.

**What You Can Show to Management**

**1. Risk-Weighted Trend Over Time**

"While the total number of vulnerabilities has dropped, risk exposure is flat—most fixes were low severity."

A simple bar or line chart like:

### RWES Over Time:

### Q1: 420

### Q2: 390

### Q3: 405

### Q4: 320

### Shows if they’re fixing the right vulnerabilities

**Investment**

| **Investment** | **RWES Drop** | **Cost per Point** |
| --- | --- | --- |
| Patching automation | $15,000 | -100 |
| Endpoint EDR upgrade | $40,000 | -250 |
| MFA rollout | $10,000 | -80 |

Now they can start thinking like: *“Where should we invest to get the most risk reduction?”*

**Efficiency View**

Plot **Control Investment vs. Risk Reduction**:

“You spent $15K on patching tools this quarter. RWES dropped by 100 points. That’s $150 per point. Want to double down or shift focus?”

Could be shown as a simple ROI-style chart or even a table:

### 3. ****Forecasting: What If We Fix X?****

Build a "control impact simulation" dashboard:

* “If you remediate all criticals next quarter, RWES would drop from 320 → 190”
* “If you fix all exploitable vulns with patch available, RWES → 120”

**🔧 1. Foundation: Set Clear Expectations & Build Core Services**

Before earning trust externally, the team needs clarity and structure internally. This means defining what the team **does well**, **can own**, and **can scale**.

**Actions:**

* **Define Core Security Services** (starting point of your catalog):
  + 🔍 **Security Risk Analysis (IT risk assessment)** — using structured risk matrices and business impact analysis.
  + 🛠 **Vulnerability Scanning** — with clear SLAs for report turnaround and actionable prioritization.
  + 📊 **Technical Security Reports** — consistent structure (executive summary, technical detail, remediation guidance).
  + 🧪 **Penetration Testing Coordination/Support** — leverage internal or external testers, but ensure ASMs add value in scoping, interpretation, and follow-up.
  + 📅 **Compliance Readiness Reviews** — map current controls against regulatory requirements (ISO 27001, NIS2, etc.).
  + 🧩 **3rd Party Risk Reviews** — repeatable methodology to assess vendors' security postures.

These are services the business needs and likely tries to handle ad hoc or poorly themselves today.

**📐 2. Standardization: Deliver Consistently and Professionally**

Consistency = credibility. Every customer touchpoint must reinforce trust and clarity.

**Actions:**

* **Create Templates & Playbooks:**
  + Report templates (with executive summary, risk rating, business relevance).
  + Standard service descriptions with scope, inputs, timeline, and outcomes.
  + Clear definitions of what’s “in scope” and what’s a handover to other teams.
* **Implement a “Security Delivery Process”:**
  + Intake form or request system for services.
  + Pre-defined timeline expectations (e.g., "vulnerability scan results delivered within 3 working days").
  + Use Kanban or light project management tools to track engagements transparently.

**⚙️ 3. Delivery: Use Automation & Tools to Be Fast and Relevant**

You mentioned automation and ML—great! If you're faster *and* easier to work with, you become indispensable.

**Actions:**

* **Adopt Security Tools for Delivery Efficiency:**
  + Automate vulnerability scanning (e.g., Nessus, Qualys) and enrich with CVSS, threat intel.
  + Use scripting or platforms to auto-generate reports (Markdown + Pandoc, or reporting plugins).
  + Leverage platforms like Tenable.io, SecurityScorecard, or OpenVAS + custom dashboards for internal visibility.
* **Data-Driven Reporting:**
  + Every report should include:
    - Risk reduction potential
    - Comparison against past results (trendlines)
    - Metrics like “time to resolution,” “critical findings open,” etc.
* **Feedback Loops:**
  + Post-delivery satisfaction surveys.
  + Stakeholder reviews after major assessments.

**🌟 4. Differentiation: Show Strategic Value, Not Just Findings**

Don’t just deliver scans and findings—connect security to the business.

**Actions:**

* **Translate Technical to Business Impact:**
  + For every risk finding, include: “Business impact if exploited” (downtime, reputation, data loss).
  + Add remediation path and timeline (aligned with ownership and reality).
* **Align Services with Business Objectives:**
  + Offer “Security Roadmapping” workshops — where ASMs sit with IT and business leaders to align priorities.
  + Show how proactive security services reduce future incidents and enable business initiatives (e.g., entering regulated markets, supporting cloud migrations).

**🎯 Suggested Strategic Goals for the Next 3–6 Months**

| **Goal** | **Description** |
| --- | --- |
| Define and publish a core catalog of services | Standardized offerings are available for internal stakeholders |
| Train ASMs on delivery standards and business impact communication | Use workshops, shadowing, and QA reviews |
| Launch an internal “pilot” program with key stakeholders | Deliver 2–3 well-run security services to teams who gave negative feedback |
| Implement 1–2 automation tools to support delivery | Start with vulnerability management and report generation |
| Introduce monthly delivery metrics | Time to deliver, stakeholder satisfaction, number of services run |