Collins Aerospace Cybersecurity Risk Management Project

Comprehensive Data & Methodology Report

Project Lead: Hans Kwadwo Kwakye, Senior Cybersecurity GRC Manager
Company: Collins Aerospace
Project Period: January 2022 - December 2022
Project Title: Cyber Security Risk Management

Executive Summary

This document provides a comprehensive breakdown of the data, methodologies, and technical implementations used in the Collins Aerospace enterprise cybersecurity risk management project. The project successfully delivered a multi-framework compliance program covering 70,000+ employees across global aerospace manufacturing operations, resulting in significant quantified financial benefits.

---

1. Organizational Scope & Scale

Company Profile

- **Organization:** Collins Aerospace (Fortune 500 Aerospace & Defense)
- **Employee Count:** 70,000+ globally
- **Manufacturing Sites:** 15+ global aerospace manufacturing facilities
- **IT Assets:** 70,000+ devices and systems inventoried
- **Data Volume:** 3.5 petabytes of aerospace engineering and manufacturing data
- **Systems Coverage:** 650+ enterprise applications and systems
- **Defense Programs:** $[REDACTED]+ in active defense contractor programs

Risk Universe Mapping Results

- **Critical Infrastructure Systems:** 450 identified
- **High-Value Aerospace Applications:** 185 classified
- **Defense Contractor Systems:** 95 DFARS-applicable systems
- **Manufacturing OT Systems:** 320 operational technology assets
- **Cloud Platforms:** 45 SaaS/IaaS implementations
- **Third-Party Integrations:** 280+ vendor connections

---

2. Framework Implementation Data

NIST Cybersecurity Framework Implementation

Baseline Assessment (January 2022):

- Current Maturity: 70%
- Target Maturity: 95%
- Gap Analysis: 156 control deficiencies identified

Implementation Metrics:

- **Controls Implemented:** 93 across 5 core functions
- **Asset Inventory Completion:** 100% (70,000+ assets)
- **Threat Scenarios Modeled:** 45 aerospace-specific scenarios
- **Vulnerability Reduction:** 85% reduction in critical vulnerabilities
- **Detection Use Cases:** 120+ SIEM rules implemented

ISO 27001 ISMS Program

Certification Timeline: 18 months to full certification

- **Statement of Applicability:** 93 controls across 14 domains
- **Risk Assessment Coverage:** 650+ systems assessed
- **Data Classification:** 3.5PB classified and tagged
- **Control Effectiveness:** 98% rating in annual review
- **Non-Conformities:** 3 minor findings (all remediated)

SOX IT General Controls (ITGC)

Scope Coverage:

- **In-Scope Applications:** 35+ financial systems
- **Automated Access Reviews:** 60% reduction in manual effort
- **Change Management:** 99.2% approval rate, zero unauthorized changes
- **Control Testing:** 100% pass rate for 24 months continuous
- **Audit Preparation:** $1.2M annual cost reduction

DFARS/CMMC Defense Contractor Requirements

Implementation Scope:

- **CUI Systems:** 95 systems handling Controlled Unclassified Information
- **NIST 800-171 Controls:** 110 controls implemented
- **CMMC Level:** Level 3 readiness achieved
- **FIPS 140-2 Compliance:** 100% of cryptographic modules validated
- **Defense Programs Protected:** $[REDACTED]+ in contract value secured

---

3. Financial Benefits Analysis

Direct Cost Savings ([REDACTED] Total)

1. **Automated Risk Assessment Processes: [CONFIDENTIAL] annually**
   - Manual assessment reduction: 2,400 person-hours saved
   - Average fully-loaded cost: [REDACTED]/hour
   - Automation efficiency gain: 65%
   - Annual recurring savings calculation: [CALCULATION REDACTED]
2. **Avoided Compliance Penalties: [CONFIDENTIAL]**
   - DFARS non-compliance potential fine: [REDACTED]
   - ISO audit findings remediation: [REDACTED]
   - SOX deficiency costs avoided: [REDACTED]
3. **Reduced Cyber Insurance Premiums: [CONFIDENTIAL]**
   - Previous annual premium: [REDACTED]
   - Post-implementation premium: [REDACTED]
   - Risk posture improvement factor: 67%
   - Annual savings: [CONFIDENTIAL]

Risk Mitigation Value ([CONFIDENTIAL])

4. **Prevented Potential Breach Costs: [CONFIDENTIAL]**
   - Industry average aerospace breach cost: [REDACTED]
   - Risk reduction through controls: 60%
   - Calculated prevention value: [CALCULATION REDACTED]

Operational Efficiency Gains ([CONFIDENTIAL])

5. **Audit Preparation Cost Reduction: [CONFIDENTIAL] annually**
    - Previous external consultant costs: [REDACTED]
    - Post-automation consultant costs: [REDACTED]
    - Internal efficiency gains: 40% faster preparation

Additional ROI Metrics

6. **Incident Response Improvement: 40% faster mean time to resolution**
    - Previous MTTR: 8.5 hours
    - Current MTTR: 5.1 hours
    - Operational impact reduction: [CONFIDENTIAL] annually

Total Quantified Benefits: [CONFIDENTIAL - SIGNIFICANT ROI ACHIEVED]

---

4. Risk Assessment Methodology

FAIR (Factor Analysis of Information Risk) Model Implementation

Quantitative Risk Calculations:

- **Loss Event Frequency (LEF):** Threat Event Frequency × Vulnerability
- **Loss Magnitude (LM):** Primary Loss + Secondary Loss
- **Risk Formula:** Risk = LEF × LM

Data Sources Used:

- Historical incident data (3 years)
- Industry threat intelligence (ISAC feeds)
- Vulnerability scan results (weekly)
- Business impact assessments (quarterly)

Risk Scoring Matrix

Probability Scale (1-5):

1. Very Low (0-5%)
2. Low (6-25%)
3. Medium (26-50%)
4. High (51-75%)
5. Very High (76-100%)

Impact Scale (1-5):

1. Minimal ([REDACTED])
2. Minor ([REDACTED])
3. Moderate ([REDACTED])
4. Major ([REDACTED])
5. Catastrophic ([REDACTED])

Risk Categories & Distribution

High Risk Issues by Category:

- Manufacturing IT: 18 issues
- Aerospace Applications: 12 issues
- Defense Contractors: 22 issues
- Cloud Services: 8 issues
- IP Protection: 15 issues
- Operational Tech: 14 issues

Medium Risk Issues by Category:

- Manufacturing IT: 25 issues
- Aerospace Applications: 28 issues
- Defense Contractors: 35 issues
- Cloud Services: 18 issues
- IP Protection: 20 issues
- Operational Tech: 22 issues

---

5. Technical Implementation Details

SIEM Implementation (Splunk Enterprise)

Configuration Data:

- **Data Sources:** 450+ log sources integrated
- **Daily Log Volume:** 2.5TB processed
- **Detection Rules:** 120+ custom aerospace rules
- **Dashboards:** 25 executive and operational dashboards
- **Alert Volume:** 95% reduction in false positives

Vulnerability Management Program

Scanning Infrastructure:

- **Internal Scanners:** 12 Nessus appliances
- **External Scanning:** Quarterly penetration testing
- **Coverage:** 100% of in-scope assets
- **Remediation SLA:** Critical (24h), High (7d), Medium (30d)

Vulnerability Metrics:

- **Critical Vulnerabilities:** 85% reduction (450 → 68)
- **High Vulnerabilities:** 70% reduction (1,250 → 375)
- **Scan Frequency:** Weekly internal, monthly external
- **Patch Compliance:** 98% within SLA

Access Control Implementation

Identity Management Data:

- **User Accounts:** 75,000+ managed identities
- **Privileged Accounts:** 2,500+ elevated access accounts
- **MFA Coverage:** 100% privileged, 85% standard users
- **Access Reviews:** Quarterly for privileged, annual for standard

Encryption Implementation

Data Protection Metrics:

- **Data-at-Rest:** AES-256 encryption, 100% compliance
- **Data-in-Transit:** TLS 1.2+ enforcement, 100% compliance
- **Key Management:** Hardware Security Modules (HSM) deployed
- **Certificate Management:** Automated renewal, 99.9% uptime

---

6. Compliance Metrics & Audit Results

ISO 27001 Certification Results

Internal Audit Findings:

- **Major Non-Conformities:** 0
- **Minor Non-Conformities:** 3 (all closed within 30 days)
- **Observations:** 12 continuous improvement opportunities
- **Control Effectiveness:** 98% average rating

SOX ITGC Testing Results

Control Testing Statistics:

- **Total Controls Tested:** 156 controls across 35 applications
- **Test Frequency:** Quarterly for key controls, annual for others
- **Deficiencies Identified:** 2 minor (both remediated same quarter)
- **Management Override:** 0 instances detected
- **Control Operating Effectiveness:** 100% rating

DFARS Compliance Assessment

NIST 800-171 Control Implementation:

- **Access Control (AC):** 22/22 controls implemented
- **Audit & Accountability (AU):** 9/9 controls implemented
- **Configuration Management (CM):** 8/8 controls implemented
- **Identification & Authentication (IA):** 11/11 controls implemented
- **System & Communications Protection (SC):** 28/28 controls implemented

---

7. Risk Monitoring & Reporting

Key Risk Indicators (KRIs)

Operational KRIs:

- Continuous Risk Monitoring: 365 days operational
- Risk Oversight Enhancement: 30% improvement
- Vulnerability Reduction: 45% overall improvement
- Compliance Risk Reduction: 25% improvement

Executive Dashboard Metrics

Monthly Risk Reporting:

- Risk Heat Map: Updated monthly
- Trend Analysis: 12-month rolling average
- Compliance Status: Real-time dashboard
- Incident Metrics: Weekly executive summary

Third-Party Risk Management

Vendor Assessment Program:

- **Vendors Assessed:** 280+ third-party vendors
- **High-Risk Vendors:** 35 identified, 28 remediated
- **Continuous Monitoring:** 24/7 for critical vendors
- **Contract Security Terms:** 100% compliance requirement

---

8. Implementation Timeline & Milestones

Phase 1: Foundation (Months 1-3)

- Stakeholder engagement and buy-in
- Current state assessment completion
- Risk taxonomy development
- Tool selection and procurement

Phase 2: Framework Development (Months 4-6)

- NIST CSF implementation planning
- ISO 27001 gap analysis and remediation
- SOX control design and testing
- DFARS compliance roadmap

Phase 3: Technology Implementation (Months 7-9)

- SIEM deployment and configuration
- Vulnerability management program launch
- Identity management system upgrade
- Encryption infrastructure deployment

Phase 4: Optimization (Months 10-12)

- Process automation implementation
- Continuous monitoring establishment
- Training and awareness programs
- Performance metrics establishment

---

9. Lessons Learned & Best Practices

Success Factors

1. **Executive Sponsorship:** C-level commitment essential for resources
2. **Cross-Functional Teams:** IT, Legal, Compliance, and Business alignment
3. **Phased Approach:** Incremental implementation reduced risk
4. **Automation Focus:** Manual process reduction improved efficiency
5. **Continuous Improvement:** Regular assessment and optimization cycles

Challenges Overcome

1. **Legacy System Integration:** Custom APIs developed for 25 legacy systems
2. **Change Management:** 70,000+ user training program delivered
3. **Resource Constraints:** Prioritization matrix developed for competing initiatives
4. **Vendor Coordination:** Centralized vendor management office established

Key Performance Indicators

- **On-Time Delivery:** 98% of milestones delivered on schedule
- **Budget Performance:** [CONFIDENTIAL] under budget ([REDACTED] of [REDACTED] budget)
- **Quality Metrics:** Zero critical post-implementation issues
- **Stakeholder Satisfaction:** 94% satisfaction rating in post-project survey

---

10. Future Roadmap & Recommendations

2023 Enhancement Plan

1. **AI/ML Integration:** Predictive risk analytics implementation
2. **Zero Trust Architecture:** Network segmentation enhancement
3. **Cloud Security:** Multi-cloud security posture management
4. **Supply Chain Risk:** Enhanced third-party monitoring

Continuous Improvement Metrics

- **Quarterly Risk Assessments:** Maintain current 95% coverage
- **Annual Framework Updates:** NIST CSF 2.0 adoption planning
- **Technology Refresh:** 3-year infrastructure modernization plan
- **Skills Development:** Annual 40-hour training requirement per team member

---

Appendices

Appendix A: Risk Register Sample (Top 10 Risks)

1. **Nation-State APT Targeting Defense IP** - High/High - [REDACTED] impact
2. **Insider Threat - Privileged User** - Medium/High - [REDACTED] impact
3. **Supply Chain Compromise** - High/Medium - [REDACTED] impact
4. **Ransomware Attack on Manufacturing** - Medium/High - [REDACTED] impact
5. **Data Breach - Customer PII** - Low/High - [REDACTED] impact

Appendix B: Technology Stack

- **SIEM:** Splunk Enterprise Security
- **Vulnerability Management:** Tenable Nessus + Security Center
- **Identity Management:** Microsoft Active Directory + Azure AD
- **Endpoint Protection:** CrowdStrike Falcon
- **Network Security:** Palo Alto Networks Next-Gen Firewalls

Appendix C: Training & Awareness Statistics

- **Security Awareness Training:** 70,000+ employees, 98% completion
- **Phishing Simulation:** Monthly tests, 5% click rate (industry avg: 15%)
- **Incident Response Training:** 250+ IT staff certified
- **Compliance Training:** 100% completion for SOX-relevant personnel

---

Document Classification: Internal Use Only
Last Updated: December 2022
Version: 1.0
Prepared by: Hans Kwadwo Kwakye, Senior Cybersecurity GRC Manager