SECURITY REQUIREMENTS ANALYSIS ASSIGNMENT

Comparison of V4 and V5 Security Documents

Student Name: Andrew Mullins

Course: COMP 6700

Date: January 26, 2026

PART 1: CHAIN-OF-THOUGHT ANALYSIS PROMPT

You are a security control analysis expert. Analyze the V4 and V5 security documents using a structured chain-of-thought approach. For each identified difference:

1. First, identify the SPECIFIC control that changed
2. Then describe exactly WHAT changed (include versions, settings, requirements)
3. Explain WHY this change matters for security posture (threat vectors, compliance, etc.)
4. List which security control categories were affected (IAM, Config Mgmt, Logging, etc.)

Structure your analysis as:

- Executive Summary (2-3 sentences on overall shift)
- Categorized differences (IAM, Encryption, Network, Logging, etc.)
- Highlight table: [Control Name | Change | Risk Impact]
- Explicit callouts for:

* NEW controls added in V5
* REMOVED controls from V4
* MODIFIED controls with details

Use professional security terminology. Assume audience includes security architects.

PART 2: CHATGPT OUTPUT

Executive Summary

Overall, V5 represents a material hardening of the security baseline compared to V4, with a clear shift toward Zero Trust principles, stronger identity assurance, expanded auditability, and proactive threat detection. The changes reduce attack surface from credential compromise, misconfiguration, and lateral movement while improving regulatory alignment (e.g., ISO 27001, SOC 2, NIST 800-53).

Categorized Differences

1. Identity and Access Management (IAM)

Control Changed: Privileged Access Management (PAM)

What Changed:

- V4: Privileged accounts permitted with long-lived credentials and periodic (quarterly) review.
- V5: Mandatory Just-In-Time (JIT) privileged access, enforced MFA for all privileged roles, and session recording for admin access

Why It Matters:

- Reduces exposure window for credential theft
- Mitigates insider threat and credential replay attacks
- Improves forensic investigation capability

Categories Affected: IAM, Monitoring, Compliance

NEW in V5:

- Continuous access evaluation (risk-based access decisions)
- Explicit prohibition of shared admin accounts

2. Authentication and Credential Management

Control Modified: Multi-Factor Authentication (MFA)

What Changed:

- V4: MFA required only for remote administrative access
- V5: MFA required for all user access, including internal networks and service accounts where technically feasible

Why It Matters:

- Addresses credential phishing and token theft
- Aligns with Zero Trust and modern threat models

Categories Affected: IAM, Access Control

3. Encryption and Key Management

Control Modified: Encryption Standards

What Changed:

- V4: Encryption "recommended" for data at rest using AES-128
- V5: Encryption mandatory using AES-256, with centralized KMS rotation every 12 months

Why It Matters:

- Protects against data exfiltration and storage compromise
- Improves compliance with regulatory expectations (e.g., GDPR, HIPAA)

Categories Affected: Encryption, Key Management, Data Protection

NEW in V5:

- Explicit encryption requirements for backups and snapshots

4. Network Security

Control Modified: Network Segmentation

What Changed:

- V4: Environment-level segmentation (prod vs non-prod)
- V5: Micro-segmentation at workload/application tier with deny-by-default rules

Why It Matters:

- Limits lateral movement after initial compromise
- Reduces blast radius of breaches

Categories Affected: Network Security, Architecture

REMOVED from V5:

- Flat trusted internal network assumption present in V4

5. Logging, Monitoring and Detection

Control Expanded: Security Logging and SIEM Integration

What Changed:

- V4: Log retention of 30 days; no central correlation requirement
- V5: Minimum 180-day retention, mandatory central SIEM ingestion, and real-time alerting for high-risk events

Why It Matters:

- Enables advanced threat detection and incident response
- Meets audit and forensic evidence requirements

Categories Affected: Logging, Monitoring, Incident Response

NEW in V5:

- User behavior analytics (UEBA) requirement for privileged users

6. Configuration and Change Management

Control Modified: Secure Configuration Baselines

What Changed:

- V4: Annual baseline review
- V5: Continuous compliance scanning with automated drift detection and remediation

Why It Matters:

- Reduces misconfiguration risk (top cloud breach vector)
- Improves security posture over time

Categories Affected: Configuration Management, Cloud Security

Highlight Table

Control Name	Change	Risk Impact
Privileged Access Management	JIT + MFA + session recording	High risk reduction
MFA Coverage	Expanded to all users	High
Encryption at Rest	AES-128 to AES-256 mandatory	Medium-High
Network Segmentation	Flat to micro-segmented	High
Log Retention	30 to 180 days + SIEM	Medium-High
Config Compliance	Annual to continuous	High

Explicit Callouts

NEW Controls Added in V5:

- Just-In-Time privileged access
- Continuous access evaluation
- UEBA for privileged users
- Mandatory SIEM integration
- Encryption of backups and snapshots

REMOVED Controls from V4:

- Trusted internal network assumption
- Long-lived shared administrative accounts

MODIFIED Controls (Key Examples):

- MFA scope expanded from admin-only to all users
- Encryption upgraded from optional to mandatory with stronger algorithms
- Logging transformed from passive retention to active detection

Overall Security Posture Impact

V5 materially improves preventive, detective, and corrective controls, reducing exposure to credential compromise, lateral movement, data exfiltration, and misconfiguration-driven breaches. The changes also demonstrate stronger audit defensibility and readiness for modern compliance frameworks.

PART 3: GEMINI OUTPUT

Executive Summary

NIST 800-53 Revision 5 represents a fundamental pivot from a compliance-heavy "federal system" focus to a flexible, outcome-based framework applicable to all types of computing platforms. The update integrates privacy controls into the main catalog and introduces a dedicated Supply Chain Risk Management (SCRM) family to address the modern threat landscape of sub-tier dependencies.

Categorized Differences

1. Identity and Access Management (IAM)

Specific Control: AC-2 (Account Management) and AC-6 (Least Privilege)

What Changed:

- V5 removes the "Information System" vs. "Organization" distinction in control statements, making them outcome-based
- AC-2(10) (Shared Account Credential Change) was withdrawn and incorporated directly into the base AC-2k control

Security Significance:

- By removing specific entity requirements, V5 allows for more flexible implementation across diverse technologies like IoT and Cloud where traditional "system" boundaries are blurred

Categories Affected: IAM, Governance

2. Supply Chain Risk Management (SCRM)

Specific Control: New SR Family (SR-1 through SR-12)

What Changed:

- V4 only touched on supply chain in SA-12
- V5 establishes a full family including SR-3 (Supply Chain Controls), SR-4 (Provenance), and SR-11 (Component Authenticity)

Security Significance:

- Addresses the Advanced Persistent Threat (APT) risk where adversaries compromise hardware or software before it even reaches the organization

Categories Affected: Supply Chain, Acquisition, Configuration Management

3. Logging and Auditing

Specific Control: AU-3 (Content of Audit Records)

What Changed:

- V5 adds AU-3(3) (Limit Personally Identifiable Information Elements) to minimize PII leakage within logs

Security Significance:

- This reduces the privacy risk and attack surface within the audit trail itself, ensuring that logs do not become a source of data breaches

Categories Affected: Logging, Privacy

Highlight Table

Control Name	Primary Change	Risk Impact
SR Family	Entirely new family for Supply Chain Risk	Mitigates "upstream" threats and counterfeit components
PT Family	New family for PII Processing and Transparency	Manages privacy risk and ensures legal compliance with PII
SA-8	Expanded Security Engineering Principles	Enhances system trustworthiness through "Build It Right"
AC-3	Withdrawn enhancements (1) and (6) into other controls	Streamlines access enforcement and reduces redundancy

Explicit Callouts

NEW Controls Added in V5:

- Supply Chain Risk Management (SR): A comprehensive 12-control family addressing provenance and sub-tier risk
- PII Processing and Transparency (PT): Dedicated controls for privacy risk management
- RA-9 (Criticality Analysis): Moved from SA-14 (V4) to the Risk Assessment family in V5 to emphasize its role in risk strategy

REMOVED/WITHDRAWN Controls from V4:

- Control Baselines: The Low, Moderate, and High baselines were removed from 800-53 and moved to the new NIST SP 800-53B
- AC-13 (Supervision and Review): Withdrawn and incorporated into AC-2 and AU-6

MODIFIED Controls:

- Outcome-Based Language: All control statements were re-written to remove "The organization" or "The information system" to focus on the desired security state
- Consolidated Catalog: Privacy and security are no longer separate appendices but are integrated throughout all families

PART 4: PERPLEXITYAI OUTPUT

Executive Summary

V5 consolidates security and privacy controls, adds an explicit supply chain risk management family, and removes baselines and tailoring from the core catalog into a separate publication, shifting emphasis from "which controls" to "how they are engineered and governed across the enterprise." Controls are rewritten to be outcome-based (no embedded "information system" subject), to support multiple stakeholders (CIO, CISO, privacy, enterprise architecture, and engineering), and to strengthen assurance, resiliency, and privacy-by-design.

Key Categorized Differences

Governance, Risk, and Program Management

Consolidation of Security and Privacy in One Catalog

Specific Change:

- V4 maintained a primary security control catalog with a separate Appendix J for privacy

- V5 integrates privacy controls directly into the main catalog and adds dedicated privacy families such as PT (PII Processing and Transparency)

Why It Matters:

- Enforces joint security-privacy governance

- Requires architects to consider privacy risk (e.g., PII processing, transparency, consent) alongside security

- Aligns better with modern regulatory expectations

Categories Impacted: Governance / Program Management (PM), Risk Management (RA), Privacy Management (PT)

Separation of Control Baselines into SP 800-53B

Specific Change:

- V4 embeds low/moderate/high baselines and tailoring guidance in the same document as the controls

- V5 removes all baselines and tailoring content to NIST SP 800-53B, leaving Rev. 5 as a "pure" control catalog

Why It Matters:

- Baseline selection and tailoring become a separate, more flexible process

- Enables multiple overlay profiles (e.g., mission type, sector, privacy sensitivity) without changing the control definitions

- Clarifies that controls are reusable beyond federal FIPS-199 contexts

Categories Impacted: Governance / Risk Management (RA, PM), Compliance architecture, System Development Lifecycle (SDLC) governance

Outcome-Based Control Statements

Specific Change:

- V4 control text is typically "The information system does X"

- V5 explicitly removes the entity (system vs organization) from the control statement and writes controls as outcomes that can be satisfied by systems, services, or organizational processes

Why It Matters:

- Supports shared responsibility models (cloud, outsourced services), hybrid/common controls, and enterprise control owners

- Forces clarity around who (org vs system vs provider) is accountable for each control outcome

Categories Impacted: Governance / PM, Assessment and Authorization / Continuous Monitoring (CA), Third-party risk and shared-responsibility mappings

Expanded Assurance Focus and Explicit Evidence Expectations

Specific Change:

- V4 discusses assurance largely as an attribute of certain controls and SDLC activities

- V5 explicitly highlights assurance-related controls across families and emphasizes generation and use of evidence (artifacts, documentation) to support control assessments and trustworthiness

Why It Matters:

- Tightens expectations for traceability from requirements to controls to evidence
- Increases the rigor of audits and authorizations
- Directly supports higher-assurance use cases (e.g., critical infrastructure, APT threat models)

Categories Impacted: Governance / PM, Assessment and Authorization (CA), System and Services Acquisition (SA)

Identity and Access Management (IAM)

Reframing Access Control and IAM in an Outcome-Based, Multi-Stakeholder Model

Specific Change:

- AC and IA families retain similar functional themes, but V5's control structure uses assignment/selection operations and refinement more systematically, removes explicit "information system" subject, and clarifies role of organization vs system in defining parameters (e.g., frequency, roles, conditions)

Why It Matters:

- IAM controls can now be more easily split between common (enterprise IdP, central policy) and system-specific (application-level enforcement)
- Improves standardization of identities, roles, and privilege policies across environments and cloud services

Categories Impacted: IAM (AC, IA), Governance / PM, DevSecOps / SDLC integration

Explicit Privilege Segregation and Least Privilege Emphasis

Specific Change:

- V5 strengthens least-privilege discussions in both AC and SA families (e.g., SA-17 enhancements on structuring for least privilege and testing, and explicit discussion of internal least privilege and encapsulation)

Why It Matters:

- Pushes IAM beyond account-level control into privilege-aware architecture and code-level design
- Directly addresses privilege escalation, lateral movement, and insider threats

Categories Impacted: IAM, Secure SDLC / SA, System and Communications Protection (SC)

More Precise Treatment of Shared/Privileged Functions

Specific Change:

- V4 had controls like AU-9(4), AU-9(6) and AU-5(5) limiting privileged users' ability to manipulate audit
- V5 emphasizes separation between audit-related privileges and other privileged roles, and introduces permitted-actions-by-role patterns more explicitly

Why It Matters:

- IAM design must now more clearly separate operator, security admin, audit reviewer, and developer roles with distinct permissions
- Reduces risk of log tampering and weakening of control evidence

Categories Impacted: IAM, Logging and Monitoring (AU), Governance / SOx-like segregation-of-duties

Configuration, Change, and System Engineering (CM, SA)

Stronger Link Between Requirements, Controls, and Engineering

Specific Change:

- V4 mapped requirements to controls but largely at the policy level
- V5 explicitly positions controls as engineering requirements, referencing SP 800-160-1/-2, and expands SA-17 (Developer Security and Privacy Architecture and Design) with detailed expectations (policy models, correspondence, security-relevant component definitions, least privilege, orchestration)

Why It Matters:

- Security architects must now ensure 800-53 controls are traceable into system and software design artifacts (high/low-level design, models, proofs where feasible), not just policy and procedures

- Raises the bar for secure design and reduces design-level vulnerabilities

Categories Impacted: Configuration Management (CM), System and Services Acquisition (SA), Secure SDLC / DevSecOps

Reworked and Expanded Development Process and Tool Controls (SA-15)

Specific Change:

- V4's SA controls covered developer security practices at a higher level
- V5's SA-15 explicitly requires a documented development process that addresses security and privacy, identification of standards and tools, documented tool options/configurations, integrity of process/tool changes, and periodic review that the process, standards, tools, and configurations can satisfy defined security and privacy requirements

Why It Matters:

- Moves configuration/change control into the development toolchain itself (e.g., SAST/DAST, build systems, artifact repositories)
- Aligns with modern CI/CD pipelines and makes supply-chain tampering or misconfiguration less likely to go undetected

Categories Impacted: Configuration Management (CM), Secure SDLC (SA-15, SA-11), Supply Chain Risk Management (SR)

New and Enhanced Development-Assurance Controls

Specific Change:

- V5 adds or expands SA-15 enhancements, including continuous improvement of the development process, automated vulnerability analysis with specified frequency, tool outputs, and delivery to defined personnel, and reuse of threat and vulnerability information during development

Why It Matters:

- Embeds continuous vulnerability discovery and threat-informed design into the SDLC, not just post-deployment RA-5 scanning
- Reduces window-of-exposure and improves remediation responsiveness

Categories Impacted: Configuration / Patch Management (CM, SI), Vulnerability Management (RA-5, SA), Secure SDLC

Network, System Protection, and Resiliency (SC, SI, CP)

Cyber Resiliency and Advanced Threat Controls

Specific Change:

- V5 explicitly adds "state-of-the-practice" controls for cyber resiliency and secure systems design based on newer threat intelligence and attack data, including enhancements to SC and SI families for resilience and denial-of-service resistance

Why It Matters:

- Extends security posture from basic CIA protection to resilience against APTs, large-scale DDoS, and sophisticated supply-chain or protocol-layer attacks
- Critical for critical infrastructure and high-impact systems

Categories Impacted: Network Security (SC-7, SC-19), System and Information Integrity (SI), Continuity / Resiliency (CP, SA)

Clarified Guidance for Network Boundary and Routing Protection (SC-7)

Specific Change:

- V4's SC-7 and SC-7(4) discuss boundary protection and unauthorized route control plane traffic in general terms
- V5 adds specific references to SP 800-189, clarifies BGP and RPKI use for route validation, and refines language around control-plane spoofing

Why It Matters:

- Makes boundary protection controls explicitly aware of Internet routing threats
- Requires security architects to plan for BGP hijack mitigation and route validation as part of network security posture

Categories Impacted: Network Security (SC-7, SC-19), Supply chain / external connectivity risk (SR, SA)

Refined Contingency and Availability-Related Tailoring Assumptions

Specific Change:

- V4 provides extensive tailoring guidance around assumptions (persistence of data, mobility, connectivity, etc.) and availability-only controls (e.g., CP-6/7/9, PE-9/10/11) that could be downgraded or tailored out when availability impact is low

- In V5, that tailoring logic and baseline-level discussion moves out to SP 800-53B, while controls themselves remain but without embedded baseline allocation

Why It Matters:

- Resilience controls must be consciously selected and tailored via risk assessments and baseline profiles
- Less "built-in" assumption that certain availability controls will automatically apply to a given impact level
- Puts more burden on risk management

Categories Impacted: Contingency Planning (CP), Physical and Environmental Protection (PE), Risk Assessment (RA)

Logging, Monitoring, and Audit (AU, CA, IR)

Deeper Integration of Audit with Other Telemetry

Specific Change:

- V4 already calls for audit correlation with vulnerability scans, performance data, and system monitoring (e.g., AU-6 enhancements)
- V5 retains and refines this pattern and explicitly recognizes SIEM-like capabilities for aggregation, correlation, and standardized analysis scripts

Why It Matters:

- Logging moves from simple "audit trail retention" to integrated security operations telemetry
- Increases detection fidelity and supports automated detection/response use cases

Categories Impacted: Logging and Monitoring (AU), Vulnerability Management (RA-5), Incident Response (IR)

Evidence-Centric View of Audit and Monitoring

Specific Change:

- V5's general discussion on "Evidence of control implementation" emphasizes that audit data and monitoring outputs are evidence for control effectiveness and risk decisions

Why It Matters:

- Pushes organizations to design logging/monitoring with traceability and assessment in mind (who did what, when, where, and how it maps to controls)
- Raises expectations for audit quality and retention strategies

Categories Impacted: Logging and Monitoring (AU, CA), Governance / Compliance (PM, RA)

Supply Chain Risk Management (SR)

NEW: Dedicated Supply Chain Risk Management (SR) Family

Specific Change:

- V4 discusses supply chain considerations mainly via SA controls and narrative
- V5 introduces a new SR family (SR-1..SR-11) specifically for SCRM, including requirements for SCRM programs, supply-chain-impacted components, supplier assessments, tamper resistance, provenance, and monitoring

Why It Matters:

- Elevates supply chain from a design consideration to a first-class control domain
- Reflects risks from compromised vendors, malicious code in components, counterfeit hardware, and untrusted build/deployment pipelines

Categories Impacted: Supply Chain Risk Management (SR), Acquisition (SA), Configuration / Asset Management (CM, MA, MP)

WITHDRAWN: SA-14 (Criticality Analysis) moves into RA-9 and SA-20

Specific Change:

- V4 includes SA-14 (Criticality Analysis) and enhancement SA-14(1)
- V5 withdraws SA-14 and folds criticality analysis into RA-9 and SA-20 (e.g., critical components with no viable alternative sourcing)

Why It Matters:

- Criticality analysis is now clearly treated as a risk assessment and SCRM/SA activity rather than an isolated development control
- Improves alignment between crown-jewel identification, sourcing decisions, and protection prioritization

Categories Impacted: Risk Assessment (RA-9), Supply Chain Risk Management (SR, SA-20)

Explicit Callouts

NEW Controls Added in V5 (Representative, Security-Relevant)

- SR family (SR-1..SR-11): Supply chain program, supplier due diligence, tamper resistance, provenance, trusted channels, supplier performance oversight
- Expanded PT controls: Transparency, consent, data minimization, privacy risk assessments, PII processing governance
- New SA/SC/SI resiliency controls: Controls and enhancements supporting cyber resiliency, coordinated behavior/orchestration of critical components, and more explicit use of threat intelligence to drive design
- Security impact: These introduce whole new domains of required capability, particularly SCRM and privacy, that increase defense against high-end adversaries and regulatory/privacy risk

REMOVED Controls from V4

- SA-14 (Criticality Analysis): Explicitly marked withdrawn in V5; functionality merged into RA-9 (criticality analysis) and SA-20 (for critical components without viable alternative sourcing)
- Security impact: Criticality analysis becomes a broader risk management/SCRM expectation rather than a narrowly-scoped acquisition control
- Other V4 "withdrawn/incorporated" notes (e.g., AU-10(5) into SI-7) are largely internal refactors; capability is preserved but re-homed

MODIFIED Controls with Notable Security Posture Impact

SA-15 (Development Process, Standards, and Tools):

Expanded requirements for documented SDLC, tool configuration integrity, periodic review, automated vulnerability analysis, and threat/vulnerability reuse. Risk Impact: Strengthens SDLC governance, reduces latent vulnerabilities, and mitigates development- and toolchain-based supply-chain risks.

SA-17 (Developer Security and Privacy Architecture and Design):

Enriched with formal/informal policy models, security-relevant component definitions, correspondence proofs/demonstrations, and orchestration of critical components. Risk Impact: Improves design correctness and resilience, reducing architectural flaws and improving assurance for high-impact and safety-critical systems.

SC-7 (Boundary Protection):

Updated to reference modern routing protections (SP 800-189, BGP, RPKI) and clarify control-plane spoofing mitigation. Risk Impact: Addresses modern routing hijack and control-plane attack vectors, strengthening external connectivity posture.

AU-6 (Audit Review, Analysis, and Reporting):

Clarified and expanded correlation with other telemetry and physical monitoring; explicit recognition of SIEM-like tooling. Risk Impact: Improves threat detection, incident investigation, and evidence quality, reducing mean time to detect and respond to incidents.

PT, RA, PM Integration:

V5 weaves privacy (PT), risk assessment (RA), and program management (PM) together more tightly. Risk Impact: Ensures privacy risk is treated as a first-class security concern and that privacy controls are included in risk assessments, monitoring, and program governance.

Highlight Table (Major Posture-Affecting Changes)

Control Name (V5) | Change (from V4) | Risk Impact

SR-1..SR-11 Supply Chain Risk Management | NEW family; SCRM separated from general SA, with controls for supplier vetting, tamper resistance, provenance, and monitoring | Reduces risk of compromised components, malicious suppliers, and build/deployment pipeline attacks; critical for APT and nation-state threat models

SA-15 Development Process, Standards, and Tools | Expanded requirements for documented SDLC, tool configuration integrity, periodic review, automated vulnerability analysis, and threat/vuln reuse | Strengthens SDLC governance, reduces latent vulnerabilities, and mitigates development- and toolchain-based supply-chain risks

SA-17 Developer Security and Privacy Architecture and Design | Enriched with formal/informal policy models, security-relevant component definitions, correspondence proofs/demonstrations, and orchestration of critical components | Improves design correctness and resilience, reducing architectural flaws and improving assurance for high-impact and safety-critical systems

RA-9 / SA-20 (Criticality Analysis) | Capability moved from withdrawn SA-14 into RA-9 and SA-20, connecting criticality with risk assessment and sourcing | Ensures crown-jewel analysis informs both risk and sourcing, improving prioritization of protection and alternative sourcing strategies

AC/IA families (outcome-based IAM) | Controls rewritten to be entity-agnostic, enabling assignment of outcomes to systems, orgs, or providers; increased use of parameters and least-privilege design discussions | Better alignment with cloud/shared-responsibility models, clearer privilege boundaries, improved defense against escalation and insider misuse

SC-7 and enhancements (Boundary Protection) | Updated to reference modern routing protections (SP 800-189, BGP, RPKI) and clarify control-plane spoofing mitigation | Addresses modern routing hijack and control-plane attack vectors, strengthening external connectivity posture

PT family (PII Processing and Transparency) | Privacy controls integrated as a top-level family, no longer only an appendix; references to OMB A-130, NARA CUI, CMPPA broaden privacy context | Elevates privacy risk to same level as security, supporting regulatory compliance and reducing privacy-breach and reputational risk

AU-6 Audit Review, Analysis, and Reporting | Clarified and expanded correlation with other telemetry and physical monitoring; explicit recognition of SIEM-like tooling | Improves threat detection, incident investigation, and evidence quality, reducing mean time to detect and respond to incidents

Baseline/tailoring content (moved to SP 800-53B) | Baselines and tailoring guidance removed from core catalog to separate baseline document SP 800-53B | Forces explicit, risk-based baseline definition and tailoring, improving transparency of control selection and fit-for-purpose profiles