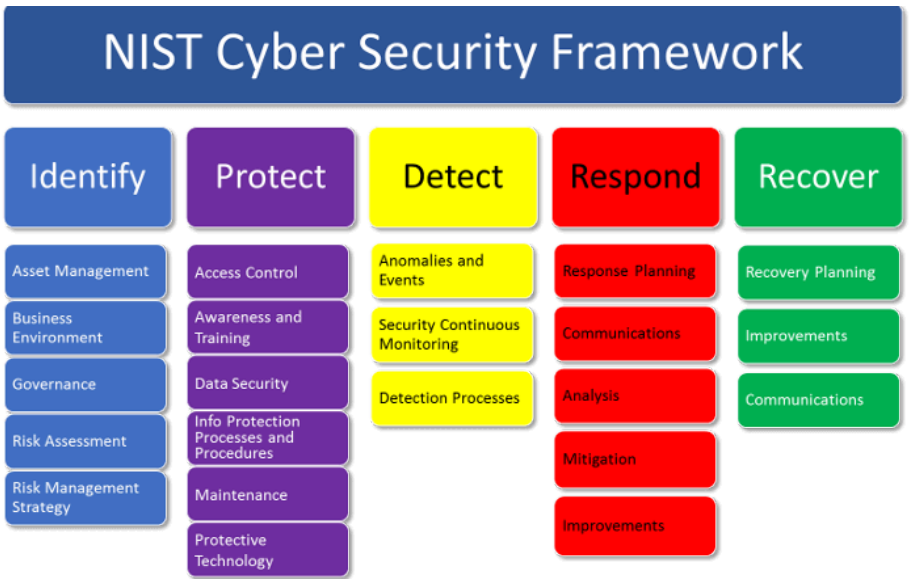
Essay Question (Theory of Vulnerability)

Explain how the NIST Risk Management Framework (SP 800-30) can be applied to mitigate vulnerabilities in a cloud computing environment. Provide examples

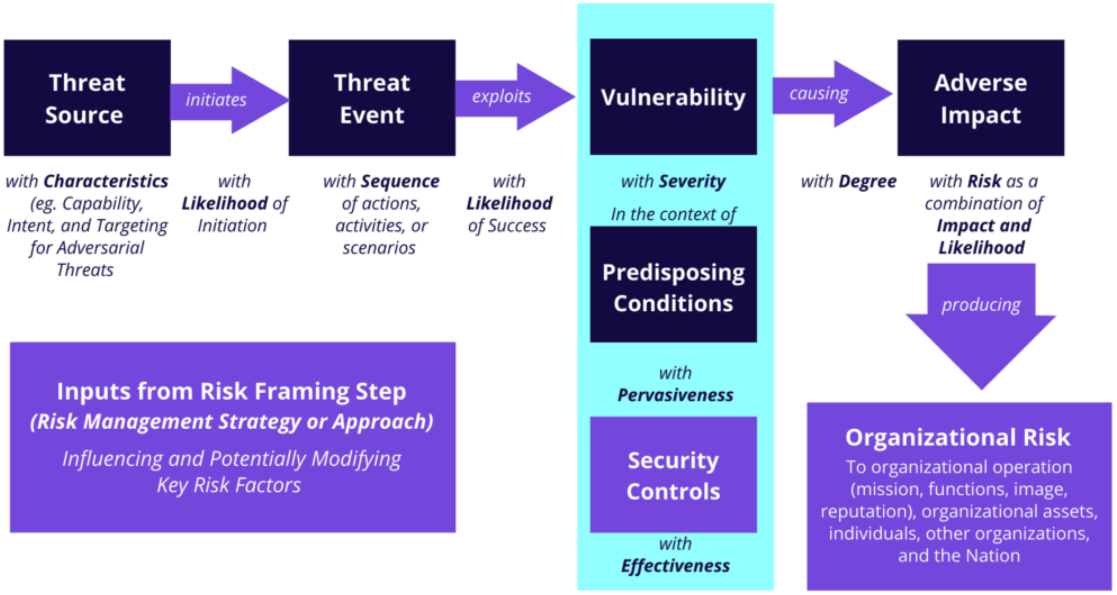
Source: Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Pearson.

Analysis:



Gambar 1. NIST Cybersecurity Framework

The *Theory of Vulnerability* dalam keamanan siber menyatakan bahwa kelemahan sistem tidak dapat dihindari tetapi dapat dikelola melalui kerangka kerja yang terstruktur. The **NIST SP 800-30** (Risk Management Guide) dan **CVSS** (Common Vulnerability Scoring System) adalah dua model utama yang mengoperasionalkan teori ini dengan mengkuantifikasi dan memprioritaskan kerentanan. Essay ini menganalisis peran mereka dalam vulnerability management, didukung oleh contoh-contoh dunia nyata.

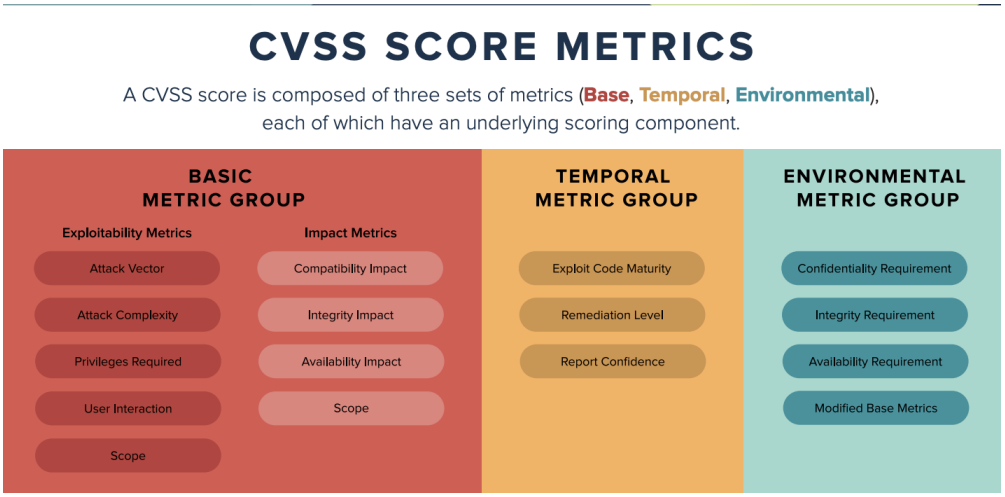


Gambar 2. NIST SP 800-30 (NIST Special Publication)

Lingkungan cloud computing yang dinamis dan berbasis model tanggung jawab bersama (shared responsibility) menghadirkan tantangan unik dalam hal keamanan siber, sehingga memerlukan pendekatan sistematis untuk mengelola vulnerabilities. Kerangka Manajemen Risiko (Risk Management Framework/RMF) dari NIST yang diuraikan dalam SP 800-30 menyediakan metodologi yang kuat untuk mengidentifikasi, menilai, dan memitigasi vulnerabilities tersebut melalui enam langkah berulang. Pada fase persiapan (preparation), organisasi harus menetapkan ruang lingkup strategi manajemen risiko cloud mereka, dengan mempertimbangkan shared responsibility model di mana penyedia cloud mengamankan infrastruktur sementara pelanggan bertanggung jawab atas data dan kontrol akses. Misalnya, insiden kebocoran data Capital One pada 2019, yang terjadi karena misconfigured AWS web application firewall yang memaparkan data sensitif di S3 bucket, menunjukkan pentingnya inventaris aset dan pemetaan akses yang komprehensif sebelum deployment.

Langkah penting selanjutnya adalah mengkategorikan cloud-specific vulnerabilities, membedakan antara kelemahan teknis seperti API yang tidak aman (contoh: insiden Tesla 2018 akibat Kubernetes console yang terbuka) dan kelemahan operasional seperti kebijakan IAM (Identity and Access Management) yang lemah (contoh: kasus Uber 2022 akibat kompromi kredensial kontraktor). Alat seperti AWS Inspector atau Azure Security Center dapat digunakan untuk melakukan pemindaian vulnerabilities secara otomatis. Setelah diidentifikasi, pemilihan kontrol yang tepat sangat penting untuk memitigasi risiko. Enkripsi data (menggunakan AES-256 untuk data saat diam/at rest), arsitektur Zero Trust (contoh: BeyondCorp dari Google), dan manajemen patch otomatis untuk layanan cloud-native adalah beberapa langkah kunci. Serangan SolarWinds pada 2020, yang mengeksploitasi pembaruan perangkat lunak berbasis cloud, menegaskan pentingnya kontrol seperti code-signing dan verifikasi integritas dalam pipeline CI/CD.

Penilaian risiko (risk assessment) di lingkungan cloud memerlukan kuantifikasi vulnerabilities menggunakan alat seperti Common Vulnerability Scoring System (CVSS) bersamaan dengan evaluasi kualitatif. Misalnya, database MongoDB yang terbuka mungkin mendapat skor CVSS 9.8 karena mudah dieksploitasi dari jarak jauh, sehingga memerlukan remediasi segera. Strategi respons harus memprioritaskan vulnerabilities berisiko tinggi, seperti mencabut API key yang terbuka atau menggunakan alat Cloud Security Posture Management (CSPM) seperti Prisma Cloud untuk mendeteksi misconfigurations. Contohnya, Microsoft berhasil memitigasi vulnerability PowerShell JEA pada 2023 di Azure melalui pembaruan patch dan baseline keamanan tepat waktu.



Gambar 3. CVSS Score Metrics

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Gambar 4. CVSS Score Rating

Terakhir, continuous monitoring melalui solusi SIEM (contoh: AWS GuardDuty, Azure Sentinel) dan pencatatan log yang kuat (contoh: AWS CloudTrail) memastikan threat detection yang berkelanjutan di lingkungan cloud. Insiden Twilio 2022, yang terjadi akibat serangan phishing via SMS, bisa terdeteksi lebih awal jika analisis log lebih komprehensif. Dengan mengikuti NIST RMF, organisasi dapat secara sistematis mengatasi vulnerabilities di cloud, menyeimbangkan otomatisasi dengan pengawasan manusia. Kasus nyata seperti kebocoran data Capital One dan supply chain attack SolarWinds tidak hanya menunjukkan konsekuensi dari kelalaian dalam manajemen risiko terstruktur, tetapi juga membuktikan efektivitas strategi yang selaras dengan NIST dalam memitigasi ancaman spesifik cloud.