Legacy Vulnerability Remediation Framework (LVRF)

Position paper for the National Institute of Standards and Technology (NIST) Virtual Workshop June 2-3, 2021.

"Secure Software Development Lifecycle Standards and Best Practices"

John Overbaugh, CISSP
Vice President, Information Security
john@overbaugh.com
https://infosec.johnoverbaugh.com
385-743-1229

With the President's executive order, the Federal Government has voiced sincere commitment to improving the security of federally-run systems, including those with third-party components. The Order includes a requirement to introduce and strengthen existing secure software development practices. These efforts are critical to ensure software changes are performed in a secure manner. Taken alone, however, the secure development practices to be introduced leave a significant source of risk unaddressed; specifically, how to identify and sequence existing security vulnerabilities which require remediation in order to secure the millions of systems in place today. The published frameworks, and the guidance anticipated in response to the Executive Order, focus on the tools, processes, and skills required to implement software securely. They do not provide a framework for addressing existing security flaws.

The topic of risk management is the subject of multiple NIST Special Publications, but no publication issued by the Institute includes guidance for prioritizing and sequencing vulnerability remediation. For consideration:

- NIST Risk Management Framework (RMF): purports to provide "a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk for organizations and systems," but places its emphasis on the evaluation and selection of security controls rather than evaluation of vulnerabilities
- NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations: documents a risk-based approach for selecting and designing security and privacy controls (including secure development practices).
- NIST SP 800-40 - Guide to Enterprise Patch Management Technologies: addresses vulnerability management not from a prioritization perspective, but from a technology and automation perspective

The need for a framework for addressing software vulnerabilities is underscored by the common thread in assessments of Federal information processing systems. In 2005 the Government Accounting Office (GAO) reported "Pervasive weaknesses in the 24 major agencies' information security policies and practices threaten the integrity, confidentiality, and availability of federal information and information systems." (https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-05-552/html/GAOREPORTS-GAO-05-552.htm retrieved 5/20/2021). And in 2018, the GAO again reported "many federal agencies were often not adequately or effectively implementing their information security policies and practices." (https://www.gao.gov/assets/gao-19-545.pdf retrieved 5/20/2021). No published statistics exist on federal software code quality, but ongoing breaches of federal system underscore the point: the United States Federal Government has a massive portfolio of legacy applications, each likely containing numerous vulnerabilities.

No amount of secure code practices can roll back time and remediate these issues - it will take a coordinated, purposeful, and prioritized effort to do so. The sheer volume of assets within the federal portfolio coupled with resource and budget constraints necessitate an approach which aims to address the highest return on investment (ie, the largest increase in security relative to cost). To implement a consistent approach to prioritizing remediation, a Legacy Vulnerability Remediation Framework (LVRF) is needed. This framework must address the following characteristics of vulnerabilities, teams, and portfolios:

- Industry-proven best practices for discovering software security vulnerabilities
- A coherent and consistent vulnerability risk score, which applies context to vulnerability ratings
- A consistent remediation treatment plan which weights 1) the vulnerability's risk score, 2) the complexity of the remediation effort, and 3) the availability of mitigating and compensating controls.

Software Vulnerability Discovery

As an answer to the President's call for improved system security, there is no doubt the numerous solutions today will shortly be joined by new and emerging technology solutions. Still, at its heart vulnerability discovery is the result of the combination of multiple best practices. Specifically:

1. Security Requirements: system design efforts must include comprehensive security requirements. These are generally driven by the risk and classification of the system, for instance as defined in NIST SP 800-53.
2. Secure Design Review: the design of proposed system architecture must undergo frequent security review to uncover flaws before they are implemented. Security Design Review is generally accomplished via the Threat Modeling process.
3. Vulnerability Scanning: the use of open source and commercial vulnerability scanning tools to identify vulnerabilities and missing patches.
4. Static Application Security Testing (SAST): static code assessment focused on security implementation flaws.

5. Software Composition Analysis (SCA): analysis of the components making up software applications. It's estimated that as much as 80% of modern software applications is comprised of third-party components. The President's Executive Order specifically calls out software supply chain as a threat and object of scrutiny.
6. Dynamic Application Testing (DAST): automated analysis of the security of an application in execution.
7. Manual penetration testing: manual, interactive, blue and red team testing to ensure applications 1) adhere to published security standards such as the Open Web Application Security Project (OWASP) Application Security Verification Standards (ASVS) and 2) are resilient to common black-hat attack techniques.

The output of these activities must be combined into a common vulnerability listing, and necessitates a consistent risk rating methodology to ensure no one source is unduly weighted in its risk evaluation.

Vulnerability Risk Scoring

The risk rating of software security vulnerabilities is generally executed in a vacuum - that is, lacking any context of the application. The truth is that a SQL injection vulnerability in an application which is not publicly addressable, contains no classified information, and has access to a small record set represents dramatically less risk than a SQL injection vulnerability in an Internet-accessible system processing public health information (PHI) with a database containing millions of records. Thus, a legacy vulnerability remediation framework must take more into consideration than a static vulnerability risk rating - the framework must introduce a risk scoring methodology which takes into consideration the context in which a vulnerability exists, prioritizing vulnerabilities which represent a truly higher risk.

Vulnerability Remediation Treatment Planning

Finally, vulnerability remediation must recognize and address the complexities and opportunities found within treatment planning. A successful framework will:

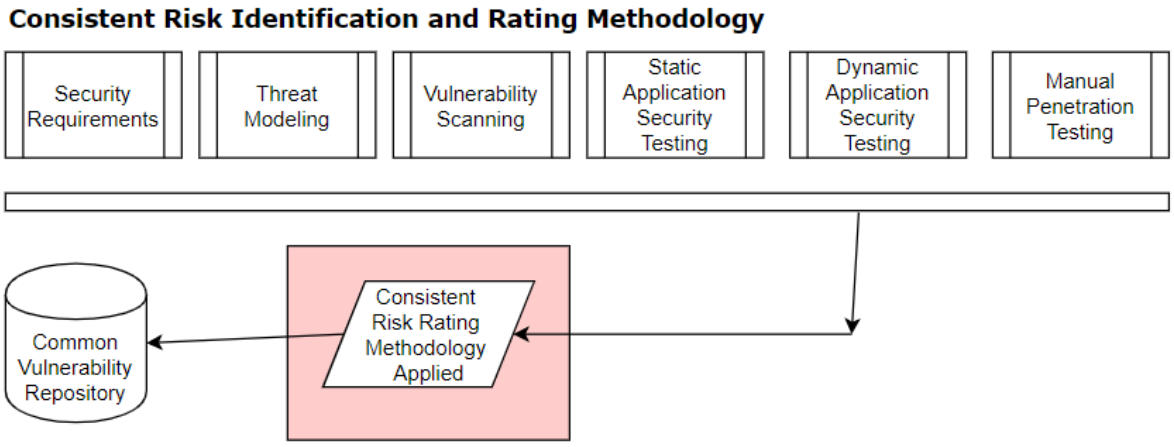
- Consider the resilience of the software under scrutiny, specifically evaluating the complexity of code and thereby the likelihood that remediation efforts will not result in further destabilizing the application. In addition, this evaluation must consider the relative cost to implement remediations; complex code represents a high cost for remediation.
- Examine and address alternative solutions. Specifically:
    - Remediation: activities which address the vulnerability's source, such as poor architecture or flawed implementation.
    - Mitigation: activities which protect the software and prevent attackers from exploiting known vulnerabilities, without actually remediating the vulnerability. For instance, a web application firewall (WAF) can be leveraged to prevent exploitation of a known SQL Injection vulnerability, without the need for a developer to update code.
    - Compensating Controls: finally, activities which implement controls to reduce the impact or likelihood of exploitation, such as detective controls which identify an ongoing exploitation effort and alert a Security Operations Center, which can then take action to block the attack or defend the application.

In a perfect world, all vulnerabilities would be remediated by being addressed in code. The reality we live in, however, dictates that the most prudent effort is to emphasize return on investment - if a mitigating control such as a WAF can be put in place at a fraction of the cost of fixing an implementation flaw, teams must give serious consideration to such a strategy in order to free themselves to address vulnerabilities which lack alternative treatment options. Furthermore, if the cost to address a specific vulnerability is high, and several similar vulnerabilities could be remediated at an equivalent cost, the team must prioritize the higher return on investment. A successful framework will quantify these values, to eliminate emotional reactions and focus teams on producing results.

Conclusion

The US Federal Government must establish and follow a consistent Legacy Vulnerability Remediation Framework to discover, prioritize, and remediate existing software flaws. This framework must be more than a simple risk rating methodology; it must be applicable to real-world applications, it must consider vulnerabilities in context, and it must consider remediation costs and alternatives. The accompanying appendix represents a proposed framework to accomplish the same. This framework represents the author's twenty-five years of experience building and maintaining software as well as their decade of experience evaluating and addressing software security vulnerabilities as a consultant and a security leader. The author volunteers this framework as a starting point for additional improvement and adaptation.

Appendix One: Risk Rating Methodology



Risk Rating Methodology

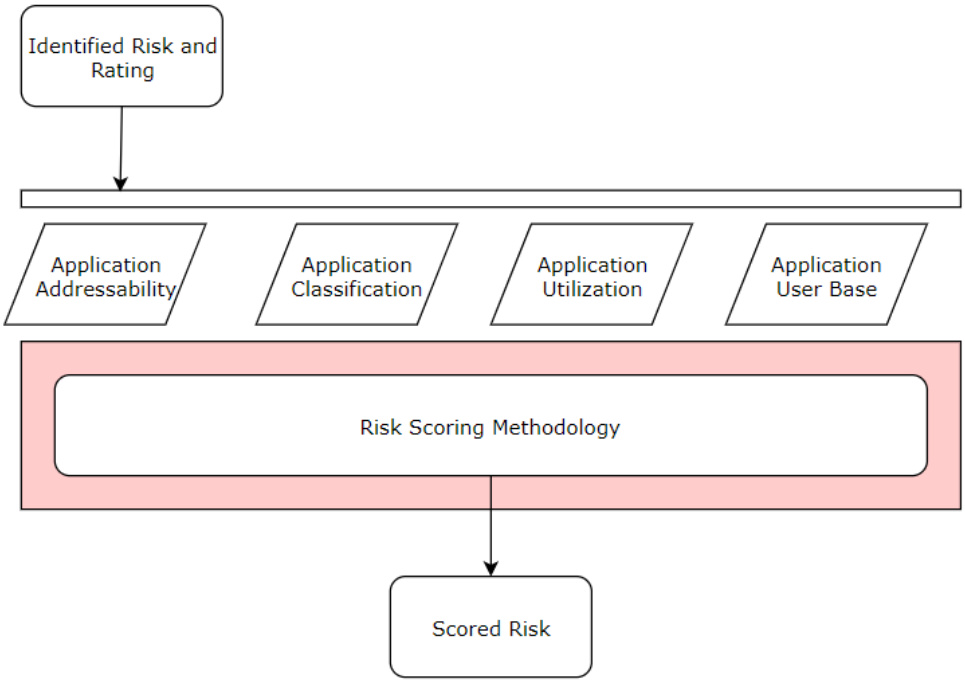
The framework requires some research into a consistent risk rating methodology. Vendor solutions and internal practices often result in widely inconsistent risk ratings for similar or identical risks. The rating methodology must also take into consideration the certainty behind a risk (for instance, a vulnerability identified during manual penetration test exploitation has a 100% certainty, whereas a Threat Modeling finding is less certain). The objective is to arrive at a common risk rating which is consistent across applications and which reflects the true risk posed by a given vulnerability.

Appendix Two: Risk Scoring Methodology

Vulnerability Risk Scoring Methodology

Once risks have been identified and consistently rated, risks must be scored. The risk scoring process aims at applying context to the identified risk. Factors considered in a risk scoring methodology must include:

- Application addressability (public internet, private network, private cloud)
- Application classification (confidential, top secret, etc.)
- Application utilization (few requests per day vs millions per day)
- Application user base (few users vs numerous users)



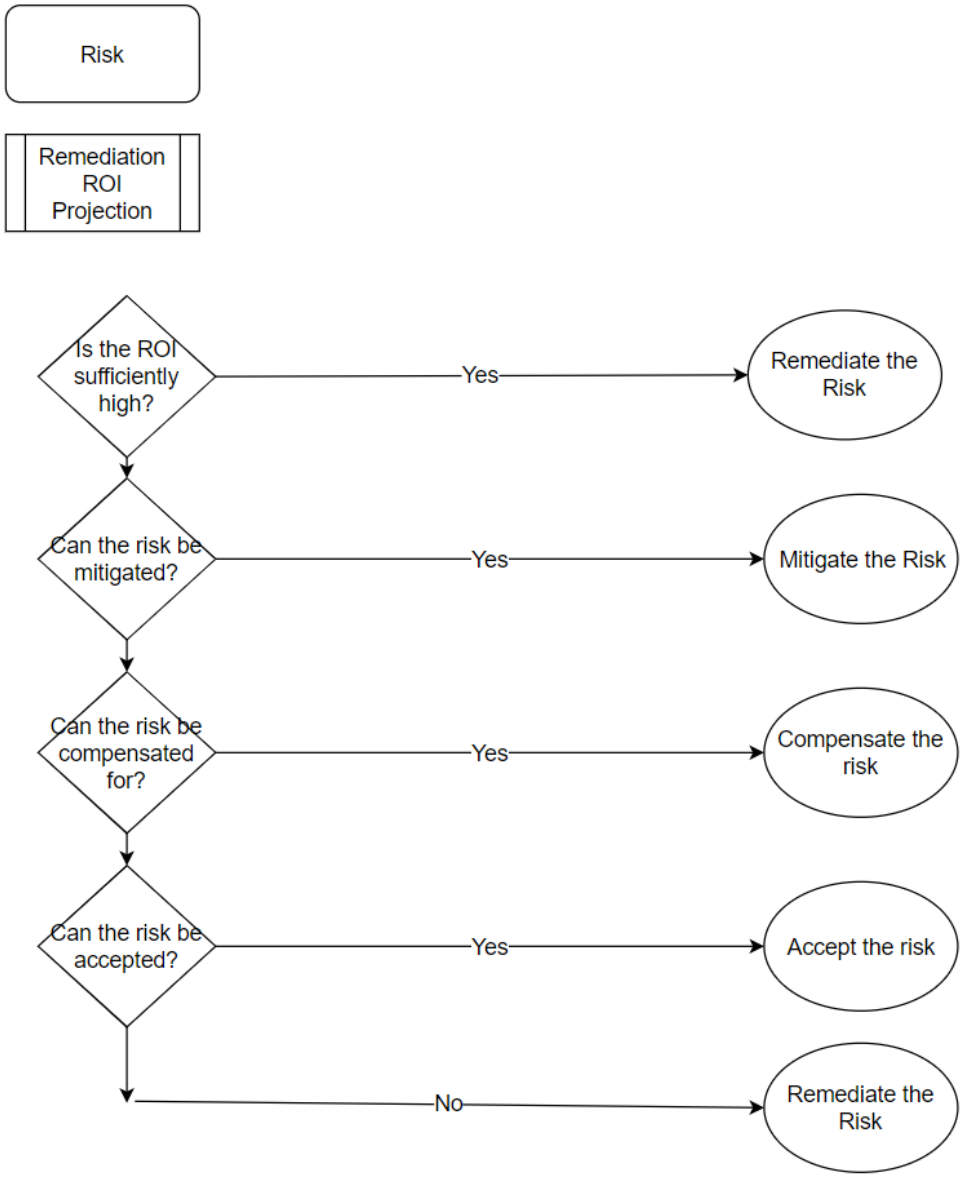
Appendix Three: Vulnerability Treatment Planning Process

Vulnerability Remediation Treatment Planning

Once a collection of vulnerabilities has been consistently rated and scored, the team will be in possession of a database of vulnerabilities, prioritized "top to bottom" against one another. Most risk frameworks advocate at this point that risks be addressed in sequence. This approach, however, does not necessarily maximize return on investment because it does not take remediation complexity and other investment factors into consideration.

For example, a risk with a scoring of 100 out of 100 seems logically to be the first risk to be remediated. However, if that risk requires 500 engineering hours to remediate due to application complexity, and if for the same investment multiple risks with a combined risk scoring of 150 could be remediated for the same investment, the appropriate strategy would to address the three smaller risks.

This remediation treatment planning process is worthy of significant investment in terms of research and estimation framework recommendations. Software applications are complex systems. Their implementation is a complex process, and the remediation of vulnerabilities represents the combined product of each - exponentially complex.



Appendix Four: About the Author

Biography

John Overbaugh
Certified Information Security Systems Professional (CISSP): 390112
GIAC Web Application Penetration Tester (GWAPT)
GIAC Security Leadership Certification (GSLC)
GIAC Certified Incident Handler (GCIH)
GIAC Mobile Device Security Analyst (GMOB)

John Overbaugh has been an information security leader since 2010 and has been involved in information security since leading one of the first product groups at Microsoft through what was then called the "Secure Windows Initiative" (SWI) and is now the Microsoft Security Development Lifecycle (SDL) in 2001. John has spoken at CES, ISC2 Security Congress, Infragard, ISACA, ISC2 and BSides conferences. As a consultant, John helped companies ranging from small startups to IPOs to Fortune 50 implement secure development and risk management methodologies.

John resides with his wife in the greater Salt Lake City, UT area. He enjoys the outdoors and loves spending time with family – especially his granddaughters.

Resume

I am an experienced, passionate, and articulate information security leader with an extensive background in leading security in healthcare IT organizations. I'm hands-on, committed to excellence, and able to work across corporate organizations to achieve common security objectives. I have led security initiatives for Fortune 50 companies as well as pre-IPO startups in healthcare and finance, across the domains of information security from standing up Governance, Risk and Compliance programs to gaining HITRUST certification to driving security remediation. I have a proven track record of results for each of my employers and clients, where each project has been a success and has led to additional success.

Skills

- Information Security management and leadership across security teams, across corporate environments, and with C-level executives
- HIPAA and Health Care Information Security leadership and expertise
- Governance, Risk and Compliance, including third-party vendor management
- Experienced in a variety of security frameworks: NIST CSF, SP800-53, HIPAA, PCI, HITRUST, Microsoft SDL, BSIMM, OWASP ASVS
- Working with cross organizational senior leadership to prioritize and execute on vulnerability management, security roadmap definition, risk and remediation prioritization, third party vendor risk management, and compliance and certification
- Budgeting, cost control, and acquisition management
- Recruiting, retention, separation and employee mentoring and engagement
- Handling significant security events and incidents, including those involving government regulation and industry compliance
- Detect, Prevent and Response strategy, solution deployment, and operationalization
- SDLC Activities: design review, threat modeling, manual code review, SAST static analysis (Checkmarx, Veracode), and DAST dynamic analysis (Burp scanner, Qualys).
- Application and network scanning, application security assessments and reporting

- C-Suite and Board-level communications. I present on the most technical subjects in a way which non-technical, highly-experience leaders can understand and can, therefore, make informed decisions
- Corporate vulnerability remediation, specifically prioritization and motivation
- Secure Cloud Principles
- Web and mobile penetration testing
- Developer mentoring in information security principles, secure architecture, and secure coding patterns

Experience

January 2018 - Present

Vice President Information Security / CareCentrix

As CareCentrix's Vice President of Information Security, I am the company's most senior security leader. My tenure began with leading a full transition of CareCentrix's information security program, from a reactive and patchwork strategy to a program based on five pillars: Identity and Access Management, Application Security, Vulnerability Management, Monitoring and Alerting, and GRC. Driving vision and implementation across each pillar, combined at times with new product selection and implementation or existing deployment optimization, I've built a program focused on complimentary controls across the detect, prevent, and recover realms of information security. Working closely with the CTO, COO and CCO and chairing CareCentrix's Security & Risk Committee, I introduced the company's risk register process, and led the company's first HITRUST certification and subsequent recertification in 2020. My responsibilities are typical of any Vice President in Information Technology, spanning budgeting and employee management to cross- team collaboration. I'm also responsible as a member of our Business Technology Leadership team for setting BT-wide priorities and supporting teammates in accomplishing organizational goals. I am responsible for nearly $2MM in annual budget ranging from full-time and contingent staff to vendor solutions to the software which powers our security program. I communicate on security status, risks, and projects to our C-Suite. My most important accomplishments are:

- My manager's feedback that, unlike most CISO's she has worked with in the past, I am committed to finding a way to get to "yes" when business needs conflict with security standards. I believe there is always a secure way to accomplish a reasonable business objective.
- Our initial and subsequent HITRUST certification
- Unifying a patchwork set of disparate security technologies into a coherent umbrella of responsive protection
- Turning the company's perception of security from a roadblock to an enabler

April 2015 – January 2018

Owner, Principle Security Engineer / infoSecure

Built profitable business focusing on web and mobile security and risk management in healthcare and financial services. Led and conducted penetration testing of web and mobile applications, conducted static code analysis and code reviews, design and support client Secure Development Lifecycle implementations, conducted HITRUST and HIPAA risk assessments, assisted in developing and presenting information security roadmaps, led and supported incident response activities. Developed corporate-owned intellectual property for penetration test engagement management as well as "DevSecure" application security policy, procedure and guidelines for .NET, Java, and mobile languages.

I am most proud of the feedback offered by one particular client. The SVP and CTO remarked “When I want a report I can share with clients, I call one of your competitors, but when I want to know what’s really wrong with my applications, I call infoSecure.”

Aug 2015 – Dec 2017 (six month break Mar – Oct 2016)

Information Security Engineer 6 / Wells Fargo (through Insight Global)

I was contracted at Wells Fargo to help lead the company’s secure coding transformation. This included maintaining and authoring secure coding guidelines for Java, .NET C#, Objective C, iOS Swift, Android Java, and Cobol. As part of the effort, I developed and socialized third party software security program in collaboration with a Wells Fargo full-time employee. I was also responsible for managing relationships with India-based groups.

Mar 2016 – Oct 2016

Chief Information Security Officer / CyberVista

Established information security policies and guidelines. Evangelized information security at CyberVista events. Conducted technology reviews, devised technology roadmaps. Authored CyberVista’s primary product, an online CISSP training course and delivered weekly “Live Online” training classes. Researched potential acquisitions.

OCT 2013 – APR 2015

Managing Director / Caliber Security Partners

Grew Caliber’s security consulting services 5x. Implemented repeatable processes to improve penetration testing estimation, accuracy, reporting and outcomes. Conducted manual penetration testing, code reviews, risk assessments in healthcare, finance, and entertainment industries. Estimated project scope, developed project proposals and statements of work, and performed other business development activities such as pre-sales consulting or presentations.

APR 2009 – OCT 2013

Director of Security / Healthagen (An Aetna Company)

Led information security strategy across multiple Healthagen subsidiaries (Medicity, ActiveHealth, NeoCare Solutions, and several incubation teams). Devise Healthagen’s cloud HIPAA compliance strategy for Amazon AWS. Collaborated with and implemented directives from Aetna’s Chief Security Architect and CISO.

SEP 2006 – APR 2009

QA Lead / Various Companies

Quality Assurance lead for Circuit City, the Church of Jesus Christ of Latter-day Saints, and Microsoft Corporation

SEP 1995 – Aug 2006

Test Manager and Group Manager / Microsoft Corporation

Led product development and software testing in various groups, including Microsoft India.

Awards, Certifications and Education

Awards

Microsoft Gold Star Bonus

- 2004: Excellence in leadership in problem solving and driving product release during the Placeware/LiveMeeting acquisition and transition.
- 2006: Excellence in leadership in hiring, training, and managing a 25-member software development team in Microsoft Hyderabad Indian Development Center.

Certifications Held

ISC2 Certified Information Systems Security Professional (CISSP) 390112 (2012)

SANS Institute/GIAC GWAPT (2012), GSLC (2012), GCIH (2013) GMOB (2018)

Certified HITRUST Practitioner (recertified 2020)

Education

Bachelor of Arts, International Relations / Brigham Young University

GPA: 3.88. Dual major with German Literature.