An
ISACA
White Paper
October 2011

ISACA®
Trust in, and value from, information systems

Web Application Security: Business and Risk Considerations

Abstract
The use of web applications in the enterprise has grown exponentially in the last decade. While businesses are benefiting in many ways from the new capabilities of these applications, the prevalence of inherent security vulnerabilities in web applications is creating significant exposure for many enterprises. This paper explores the root causes of these vulnerabilities, examines the associated risk and impacts, and provides guidance as to how enterprises can alter their practices to mitigate this risk.

While this document focuses specifically on web application security, the guidance presented applies to all types of software development activities.

ISACA®

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed and created *Web Application Security: Business and Risk Considerations* (the "Work") primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Web Application Security: Business and Risk Considerations

Acknowledgments

ISACA wishes to recognize:

Project Development Team
Salomon Rico, CISA, CISM, CGEIT, Deloitte Mexico, Mexico, Chair
Sarbjit Sembhi, CISSP-ISSAP, GAWN, GCIH, Incoming Thought, UK
Rob Singh-Latulipe, CISA, CISM, CGEIT, CISSP, USA

Expert Reviewers
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCAD, MCSD, IR, New Zealand
Munyaradzi D. Mufambisi, CISA, CISM, CISSP, ISSMP, Ernst & Young—Advanced Security Centre, Australia
Anthony Noble, CISA, Viacom Inc., USA
Jonathan D. Sternberg, CISA, CISM, CRISC, CISSP, FFSI, FLMI, Northwestern Mutual, USA
Mario Urena, CISA, CISM, CGEIT, CISSP, Secure Information Technologies, Mexico
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium
Carlos Villamizar R., CISA, CISM, CGEIT, CRISC, COBIT Foundation Certificate, ISO 27001 LA, ISACA Bogota Chapter, Colombia
Miguel (Mike) O. Villegas, CEH, CISA, CISSP, GSEC, Newegg Inc., USA
Peter Wood, CISSP, CITP, FBCS, MIEEE M.Inst.ISP, First Base Technologies LLP, UK
Vladimir Yastreboff, Westpac, Australia

ISACA Board of Directors
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA, CISSP, J.P. Morgan Chase, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Nestle USA, USA
John Ho Chi, CISA, CISM, CRISC, CFE, CBCP, Ernst & Young LLP, Singapore
Phil Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

Acknowledgments *(cont.)*

Guidance and Practices Committee
Phil Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Spain
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Yongdeok Kim, CISA, IBM Korea Inc., Korea
Perry Menezes, CISM, CRISC, Deutsche Bank, USA
Mario Micallef, CGEIT, CPAA, FIA, Advisory in GRC, Malta
Salomon Rico, CISA, CISM, CGEIT, Deloitte Mexico, Mexico
Nikolaos Zacharopoulos, Geniki Bank, Greece

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA chapters
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
ASI System Integration
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

The Impact of Web Applications

Web applications have become indispensable to the enterprise. Once used primarily as online brochures or rudimentary online storefronts, today the integration of web applications into key business processes has reached an unprecedented level. Whether providing new and innovative ways for a global customer base to interact with customer service, or serving as the interface for an enterprise resource planning (ERP) system, web applications have become a key strategic component in customer acquisition and service, as well as a viable replacement for many traditional client-server applications across the enterprise.

This growth is fueled in great part by the introduction of Web 2.0 technologies such as Asynchronous JavaScript Technology and XML (AJAX), Flash™ and HTML 5. These technologies have eliminated many of the limitations that once existed in the web-user interface, bringing them on par with traditional client-installed applications. This has opened up the possibility to web-enable many internal applications, eliminating the need for "thick" client-side applications and the management and maintenance overhead that went along with them.

Another key aspect of this evolution of web capabilities is the rich array of social media sites that have taken Internet usage to unprecedented heights. Corporations are being caught up in the wake of this phenomenon and are seeking every opportunity to leverage it to their benefit. A recent report from McKinsey[1] that studied the impact of Web 2.0 on more than 3,000 corporations provides this perspective:

> *A new class of company is emerging—one that uses collaborative Web 2.0 technologies intensively to connect the internal efforts of employees and to extend the organization's reach to customers, partners, and suppliers. We call this new kind of company the networked enterprise. Results from our analysis of proprietary survey data show that the Web 2.0 use of these companies is significantly improving their reported performance. In fact, our data show that fully networked enterprises are not only more likely to be market leaders or to be gaining market share but also use management practices that lead to margins higher than those of companies using the Web in more limited ways.*

What is so special about web applications?

Web applications differ from their predecessors in several important ways. Unlike traditional client-installed applications, web applications:

- **Are client-server applications that leverage a browser such as Microsoft® Internet Explorer, Google Chrome, Apple® Safari or the open source Firefox on the client side of the application**
- **Are generally platform-independent. They will run on Windows, LINUX, Mac OS and even on mobile devices platforms such as iOS and Android™.**
- **Generally require less computational power than their client-based predecessors**
- **Can be seamlessly integrated with a nearly limitless array of online resources and services**

Business Benefits of Web Applications

The drive for companies to keep up with their competition and stay relevant in the global marketplace compels enterprises to stay on the cutting edge of web innovation. Particularly with the advent of Web 2.0, the capabilities and associated benefits that enterprises can derive from leveraging web technology are too compelling to ignore. In a recent study conducted by McKinsey,[2] more than 3,000 executives were surveyed across a broad range of regions, industries and functions regarding their use of Web 2.0 technologies. A majority of the respondents reported that the use of Web 2.0

[1] Bughin, Jacques; Michael Chui; "The Rise of the Networked Enterprise: Web 2.0 Finds its Payday," *McKinsey Quarterly*, December 2010
[2] *Ibid*.

technologies was producing measurable business benefits internally, with customers, and with business partners and other external resources. Some of the benefits cited included:
- Increased marketing effectiveness
- Reduced time to market for products and services
- Increased satisfaction of suppliers, partners and external experts
- Reduced supply chain costs
- Increased customer satisfaction
- Increased employee satisfaction
- Reduced [internal] communication costs
- Increased revenue

While not called out specifically by McKinsey, it is important to note another important facet of the business benefits of these key web applications. Enterprises that successfully deploy and leverage these new technologies typically increase their stature in the eyes of their investors and business partners. To the extent that these applications perform as expected—in a secure and reliable manner—the perceived value and reputation of the overall enterprise increases. This additional value and confidence in turn increases support from internal stakeholders, encourages greater external investment and facilitates opportunities for new business expansion and partnerships.

There are also more traditional benefits. By replacing dated client or client-server applications with web-based applications, enterprises can reduce the number of end-user applications that require frequent patches and other updates, simplify license management, avoid operating system compatibility issues, and increase flexibility for hardware requirements. Additionally, web-based applications are often more readily used over virtual private network (VPN) and other types of remote connections—an important consideration, given the increasing prevalence of mobile and remote workers.

Given the current business climate, it is easy to understand why enterprises are looking at every opportunity to rapidly increase both the scope and the functionality of their web footprint. However, all of the aforementioned benefits can be quickly undermined by haste and inattention to the importance of ensuring security and reliability of these applications. As web developers around the globe strain to keep up with business demands for web sites with greater functionality and more "click appeal," this rapid expansion in web application development is also introducing new risk that, if realized, carries potentially significant financial impact that erodes many of the realized benefits.

This risk is related primarily to two specific factors:
- The significant number of code-based vulnerabilities that enterprises are allowing to exist in their web applications
- Many, if not most, web applications are accessible from the Internet.

The March 2011 report from Ponemon Institute places the average cost of a single data breach at US $7.2 million.

These two factors, combined with an ever-increasing number of threat agents, have resulted in countless cases of personal information breaches, disruption of service and theft of intellectual property. These unfortunate events are costing corporations millions of dollars in fines, lost sales, customer attrition, and other associated costs such as customer notification and credit monitoring, not to mention loss of confidence from investors and potential business partners. In fact, the March 2011 report from Ponemon Institute places the average cost of a single data breach at US $7.2 million.[3]

[3] Ponemon, Larry; "Cost of Data Breach Climbs Higher," Ponemon Institute, USA, 8 March 2011, *www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher*

It is obvious that enterprises cannot continue ignoring this risk, particularly with the level of reliance that they place today on web technology. The remainder of this publication discusses the specific risk that enterprises create by deploying flawed web applications in this production-line fashion, and will then outline the appropriate steps to effectively mitigate or eliminate the vast majority of this risk.

Risk and Security Concerns With Web Applications

As enterprises rush to deploy the latest innovations in web technology, many are doing so without sufficient focus on risk. Most frequently, security shortcomings within the overall web application development life cycle, formally known as the system (or software) development life cycle (SDLC), can result in applications being deployed with significant security vulnerabilities.

How severe is this issue? In 2010 the Ponemon Institute published the results of a broad survey of experienced security practitioners from multinational companies across the United States.[4] The questions in the survey centered on security professionals' perceptions of their enterprises' commitment to a secure SDLC process. Their responses provide a sobering account of the state of web application security in many, if not most, global enterprises:

- 70 percent of respondents do not believe their enterprises allocate sufficient resources to secure and protect critical web applications.
- 34 percent of urgent vulnerabilities are not fixed.
- 38 percent believe it would take more than 20 hours of developer time to fix one vulnerability.
- 55 percent of respondents believe developers are too busy to respond to security issues.

Given these responses and the trend that they suggest, it is not difficult to understand the current state of web application security. Virtually all studies over the past decade that have looked at web application security suggest that the consequences of ignoring or downplaying security requirements in the SDLC are quite real and have a significant impact on many enterprises—and the problem is only getting worse.

The consequences of ignoring or downplaying security requirements in the SDLC are quite real and have a significant impact on many enterprises—and the problem is only getting worse.

A recently released report from HP DVLabs made the following somber observation:

> *Web applications have continued to dominate the threat landscape in 2010, sustaining a steadily increasing trend over the last few years.... The staggering number of Web application vulnerabilities combined with more effective exploitation methods... demonstrates why attackers continue to target these systems… Web application vulnerabilities comprise nearly half of all [known] vulnerabilities*.[5]

This characterization is supported by the Verizon "2010 Data Breach Investigations Report," which observed:

> *After being edged out in 2008 as the most-used path of intrusion, web applications now reign supreme in both the number of breaches and the amount of data compromised through this vector.*[6]

[4] Ponemon Institute, "State of Web Application Security," Ponemon Institute Research Report, USA, 26 April 2010
[5] DVLabs, "2010 Full Year Top Cyber Security Risks Report: In-depth Analysis and Attack Data From HP DVLabs," DVLabs Tipping Point, USA, March 2011, *http://dvlabs.tippingpoint.com/img/FullYear2010%20Risk%20Report.pdf*
[6] Verizon, "2010 Data Breach Investigations Report," Verizon Business Resource Center, USA, 2010, *www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf*

It should be noted that in its just-released "2011 Data Breach Investigations Report," Verizon acknowledges that web applications are no longer leading the attack vector ranking; however, they are quick to add:

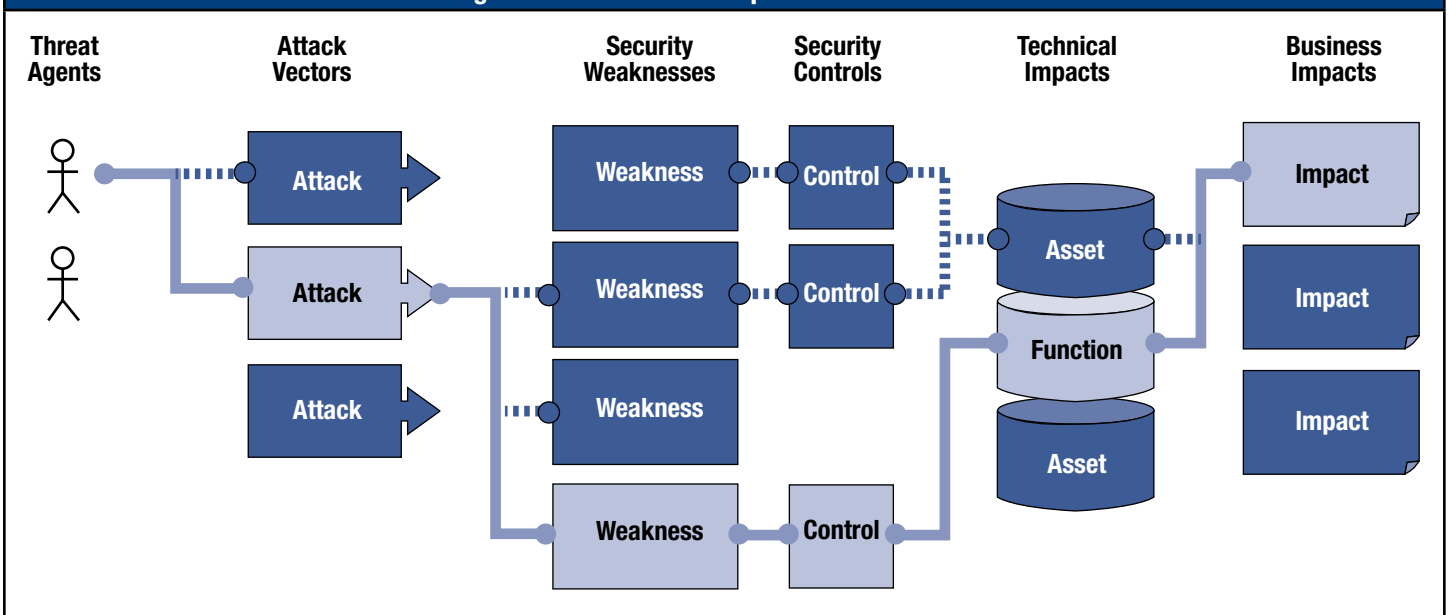
> *Just because web applications dropped as an overall percentage of attacks, don't believe for an instant that they are any less critical a vector than they were a year ago. If you remove hospitality and retail victims from this dataset, web applications are right back on top and are more numerous than ever.*[7]

There are certainly many other studies with similar findings that could be cited, but it takes no more than a quick glance at newspaper headlines to see the trend confirmed. In just the first months of 2011, there have been a number of high-profile cases of web-based attacks that have cost companies millions in revenue and have negatively impacted their public image. The Web Hacking Incident Database,[8] a project managed since 1999 by the Web Application Security Consortium (WASC), has logged 90 incidents for the first quarter of 2011 alone, and this includes only those attacks that meet very stringent criteria. Since many attacks go unreported and many more likely go undetected, it is clear that these vulnerabilities continue to be pervasive, despite the industry's full knowledge of their existence and, in many cases, how to correct them.

What are these vulnerabilities, how are they exploited and what impact can they have on an enterprise? Web application vulnerabilities come in many forms, and while it is not the intent of this paper to delve into the technical details, some discussion of how they function will help demonstrate the severity of the issue.

As a first step, **figure 1** will help to foster a high-level understanding of how an attack can ultimately impact a business.

Figure 1—An Attack's Impact on the Business



[7] Verizon, "2011 Data Breach Investigations Report," Verizon Business Resource Center, USA, 2011, *www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*
[8] See Web Hacking Incident Database, Web Application Security Consortium, *http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database*

As depicted in **figure 1**, there are typically a number of potential pathways into an enterprise's computing environment (represented by the security weaknesses). In many cases these pathways are not viable to the attacker for any number of reasons. It may be that behind a particular vulnerability (weakness) there is a dead end, with nothing to exploit. It also may be that there are sufficient compensating controls in place to mitigate any risk caused by the vulnerability, or at least sufficient controls to deter attackers and compel them to look elsewhere. However, in many cases, the vulnerability is an open door leading to sensitive corporate information—just waiting for someone to find and exploit it.

To better understand the correlation between vulnerabilities and their potential impact, **figure 2** lists several of the of the most common web application vulnerabilities along with their associated risk and potential impacts.

Figure 2—Common Web Application Vulnerabilities

Vulnerability Type	Risk	Impact
SQL injection	Back-end databases are compromised by threat agents sending malicious commands via web application to the command interpreter.	The entire database can usually be read or modified. It may also allow full database schema, account or even OS-level access, resulting in information being stolen or destroyed, or other systems being compromised. This vulnerability has been responsible for some of the most high-profile and expensive breaches ever reported, with costs topping US $170 million in one instance.
Cross-site scripting	Attackers take advantage of poor input validation in web forms to return malicious code to the client web browser.	This vulnerability, frequently used in conjunction with phishing attacks, can send users to authentic-looking malicious web sites that are designed to steal user log-in credentials and other sensitive information. These data, once collected, can be used to compromise users' accounts. The impact can vary widely depending on the nature and number of accounts compromised.
Insecure direct object reference	Attackers log in as an authorized system user, then change a parameter value that refers to another account, which can provide access to other accounts that they are not authorized to view.	Account or other sensitive data can be stolen or altered. Impact can vary widely depending on the nature of the accounts compromised, but a recent breach of this type led to the compromise of personal account data of more than 100,000 customers of one Fortune 100 company.
Information leakage	An application vulnerability in which an application exposes sensitive data, such as technical application information, information about the surrounding network environment or user-specific data.	The impact can vary widely, depending on the nature of the information leaked. However, recent incidents in the social media space have drawn attention to this vulnerability.
Insufficient anti-automation	This is an application vulnerability that allows an attacker to automate a process that is intended for manual execution by a single user, allowing the attacker to overwhelm system resources, frequently resulting in what is commonly known as a denial of service (DoS) attack.	The impact can vary widely and is dependent on the type of web site and the organization. Corporations can lose sales, suffer reputational damage, or have key business processes interrupted. In the increasingly interdependent world of Web 2.0 services, an attack on one site can impact not only the host company, but also thousands of affiliated sites around the world.

The common vulnerabilities and the high-profile breaches cited in **figure 2** are just the tip of the iceberg. The truly concerning fact is that despite the number and magnitude of the web-based breaches that have been reported, there is a significantly greater number that go unreported or are not detected when they occur.[9]

[9] While this publication deals with external attacks, it cannot be forgotten that threats exist within the enterprise network as well and must be mitigated via a systematic risk management program.

Despite the impact that can result from not addressing web application vulnerabilities, it seems that many, if not most enterprises, are not taking significant steps to address the issue. The Ponemon Institute study previously cited stated that 70 percent of the respondents did not believe that their enterprises allocate sufficient resources to protect web applications.[10] This is despite the constant parade in the headlines of high-profile attacks that cost enterprises millions of dollars each year. It is also despite the fact that many of the most common vulnerabilities, including those cited in **figure 2**, have existed for a number of years, as has the knowledge of how to address them. Independent, nonprofit organizations such as the Open Web Application Security Project (OWASP) and WASC provide an abundance of freely available information regarding web application vulnerabilities and how to avoid or mitigate them. Vendors such as Microsoft®, Adobe®, Hewlett-Packard Company and IBM® provide guidance for secure development practices using their respective products. Despite all of the available knowledge and resources, all indicators point to the problem continuing to worsen.

There are also regulatory drivers that should compel enterprises to address their unsecure web applications. Payment Card Industry Data Security Standards (PCI DSS) Version 2.0 contains specific requirements regarding securing the application development process and specifically calls out a number of vulnerabilities that consistently make top 10 lists of organizations such as the SANS Institute and OWASP. Certainly, the introduction of these requirements in PCI DSS have compelled enterprises to make headway in this area, but studies still indicate that a significant percentage of organizations that are required to be PCI DSS compliant are missing the mark when it comes to web application security.

Strategies for Addressing Web Application Risk

Applications, once deployed, must be continuously monitored for newly discovered vulnerabilities, and decisive action taken to address any vulnerabilities found.

The central factor to consider when addressing web application risk is, of course, the SDLC process. To get ahead of the problem of vulnerable web applications, security measures must be included as early as possible and must be nonnegotiable components of the process. This means that programmers must be trained appropriately in secure coding techniques and empowered to leverage that training. It requires a robust and effective quality assurance process to enforce continuous and controlled quality testing of not just the functional, but also the security aspects of the application. It also means that applications, once deployed, must be continuously monitored for newly discovered vulnerabilities, and decisive action taken to address any vulnerabilities found. From initial design to final disposition, applications must have security integrated at every step.

If the answer to web application security was simply to make sure that programmers know how to write secure code and then get out of the way, the problem would be fairly simple to address. However, web applications, like any other IT resource, are part of a large, complex system and they are impacted by numerous factors, some of which have little to do with technology. It follows, then, that any solution to this problem must utilize a systems-based approach to address it fully and effectively.

A Systems-based Approach to Secure Web Applications

A systems-based approach to complex problems is not a new concept, but frequently it is overlooked when addressing issues that appear to be purely technical in nature. A systems approach, as described in the ISACA Business Model for Information Security[11] (BMIS), promotes taking into account the broader context of an issue and approaching it from

[10] Ponemon Institute, "State of Web Application Security," Ponemon Institute Research Report, USA, 26 April 2010
[11] See ISACA, The Business Model for Information Security, USA, 2010, *www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx*

multiple perspectives. This considered, it follows that to establish an effective program that drives security throughout the SDLC (ultimately producing more secure web applications), all of the areas that support and impact the SDLC process must also be addressed.

Figure 3 contains a list of areas that impact web application development and outlines how each must be included to create an effective, holistic action plan.

Figure 3—Web Application Security Areas of Focus

Area	Recommended Action
Business/ executive support	Support from senior management is essential for any security initiative, and secure development practices are no exception. To garner support for the secure SDLC initiative, risk must be expressed in business terms and it must be demonstrated how adding security measures to the SDLC supports business objectives through the reduction of risk. Prior to approaching the business, a full risk assessment should be conducted for the current SDLC process. Additionally, business impact assessments (BIAs) should be conducted for several key applications. The results of these assessments should be summarized and included with any presentation to the business regarding funding SDLC security initiatives. Demonstrating the cost difference between finding and correcting code issues in development versus correcting them once in production can help establish the basis for the additional efforts required for secure development life cycle practices. Manage business expectations by clearly explaining the risk of circumventing secure practices in favor of accelerated development cycles (which typically lowers project delivery costs). Project teams should recognize the applicable enterprise risk and indicate the specifications for managing the risk. Enterprises face numerous objectives in securing their information infrastructure. Concepts of good governance dictate taking a risk-based approach to the prioritization of these objectives. Effective communication of the risk and potential impacts of exploitation of the vulnerabilities inherent to web applications is critical to ensuring that a program to introduce security measures into the SDLC receives sufficient resources to address the problem. Compliance can be a strong motivator for executive support. The requirements in area 6.6 of PCI DSS Version 2.0 clearly mandate securing the application development process and even suggest using guidance from organizations such as OWASP. Enterprises impacted by PCI DSS already have a strong case for senior management to endorse the initiative to secure the SDLC process.
Training	Formalized training of developers on secure coding practices, augmented by periodic updates on new techniques and vulnerabilities, is an essential step in securing the overall SDLC process. Numerous resources exist to assist with this process. Training in secure coding practices should be accompanied by periodic skills assessments to ensure that training has been effective. Additionally, successful acquisition and application of secure coding skills should be part of developer performance evaluations.
Supply chain	Secure the supply chain. Web applications are rarely developed completely in-house. Standards and effective code-review processes must be applied, not only to code developed in-house but also to code components such as plug-ins that are procured to augment internally developed code.
Policies and standards	Any program to address web application vulnerabilities must be appropriately framed by a complete set of security policies and supporting standards and procedures. Developing and effectively communicating these security standards will drive consistency across the enterprise's efforts to employ effective security in the application development process. Developers need a structured, documented approach that dictates what must happen at what time in terms of security, and that documents how much effort is sufficient at any given point in the development process. Additionally, the program should be periodically audited to ensure its continuing compliance with these policies and standards.
Technical controls	It is important to consider technical controls for the web application environment, particularly when there are web applications with legacy code that has not undergone security testing or has known vulnerabilities that have yet to be addressed. Web servers that serve Internet clients are typically on a protected or screened subnet, known as a demilitarized zone (DMZ), and this is a start, but to truly protect against application misconfigurations and other application layer vulnerabilities, a web application firewall is a better choice. However, a web application firewall is no replacement for secure code and should be considered only as a second layer of defense or, in some cases, a temporary measure until code can be modified to address vulnerabilities.

Figure 3—Web Application Security Areas of Focus *(cont.)*	
Area	**Recommended Action**
Ongoing program of scanning/code review	As part of the quality assurance process, audits of the software code using both automated tools and quality assurance reviewers will establish a level of rigor that, being absent in past SDLC processes, has also contributed to the problem of vulnerable software in web applications. The process of testing source code against secure coding standards should be deployed at defined points of the system's build process to ensure that vulnerabilities are caught early and do not combine to create a vulnerability greater than the sum of their parts. Using sound methods of quality assurance review for security specifications will provide the assurances required by audit to ensure that due diligence is being applied to the software design, build and test program.
Legacy code	Ensuring that new code is developed in a secure fashion is only part of the equation. There must also be processes and procedures to use systems to test and review existing production web environments for vulnerabilities on a regular basis. These systems can be updated on a regular basis to ensure that newly detected vulnerabilities do not exist in legacy environments. This is frequently viewed as an insurmountable "Pandora's box" as resource-strapped enterprises struggle to secure newly written code, let alone worry about what is already deployed. However, it is just as important to seek out and eradicate vulnerabilities in web applications that are already in use as it is to ensure that no new vulnerabilities are added. Secondary compensating controls can frequently be used to mitigate known risk until such time that it can be addressed.
Project management/ project management officer (PMO)	Ensure that project managers are aware of all required steps in the SDLC process and the time needed to complete them. They must understand that when time is needed to compensate for a project setback, the development cycle is not the place to make up that time. Support from senior management and clear, documented standards and procedures are critical to this area.
Effective incident response capabilities	Despite taking all of the previous steps, there is still a chance that a system will be compromised. Having a tested and well-defined incident response process is an additional compensating control that can significantly reduce the impact of a breach if it occurs.

While the previous steps can help address ensuring the security of web applications, there will be hurdles and challenges along the way. Each of the following points should be anticipated as potential challenges to be addressed during this process:

- The time and cost of training developers in secure coding techniques can create concerns/pushback.
- Introducing secure code can add to application response time, creating latency that may need to be compensated for in other ways.
- Vulnerability scanning can impact network traffic and application performance. Information security teams must work with the business and operations to determine optimal time frames and methods for scanning.
- All organizations at one time or another must make emergency code updates. Follow-up code review, vulnerability testing and additional control layers must be built into the emergency change process to ensure that emergency code changes are reviewed for vulnerabilities as quickly as feasible.
- Source code must be stored securely and monitored for movement and change as is done for any other critical intellectual property.

Governance and Change Issues

The role of governance is to ensure that a given activity is managed in a way that results in a consistent, effective, risk-based approach that is aligned with and actively supports the goals and objectives of the enterprise. Governance of the SDLC process, as with any other IT function, is best facilitated by the use of a framework such as ISACA's COBIT® 4.1.[12] COBIT is a framework and supporting tool set that allows managers to bridge the gap with respect to control requirements, technical issues and business risk, and communicates that level of control to stakeholders. COBIT also enables the development of clear policies and good practice for IT control throughout enterprises.

[12] See ISACA, COBIT 4.1, USA, 2007, *www.isaca.org/cobit*

The benefits of implementing COBIT as a governance framework include:
- Better alignment, based on a business focus
- A view (understandable to management) of what IT does
- Clear ownership and responsibilities, based on process orientation
- General acceptability with third parties and regulators
- Shared understanding among all stakeholders, based on a common language
- Fulfillment of the COSO requirements for the IT control environment, which addresses software development as a key component of its broader program of governance that addresses all IT processes

Figure 4 contains the COBIT domains, processes and corresponding control objectives that are directly related to the ***security*** of the SDLC process:

Figure 4—COBIT Control Objectives Directly Related to SDLC Security

COBIT Domains, Processes and Control Objectives	Relation to SDLC Process Security
Plan and Organise	
PO8 Manage quality. 8.1 Quality management system 8.2 IT standards and quality practices 8.3 Development and acquisition standards 8.5 Continuous improvement 8.6 Quality measurement, monitoring and review	Quality management requirements should have security considerations integrated throughout to ensure that software security flaws are detected, documented and corrected in a timely manner, and that the detection of code vulnerabilities helps drive process improvement for the SDLC.
Acquire and Implement	
AI1 Identify automated solutions. 1.1 Definition and maintenance of business functional and technical requirements 1.2 Risk analysis report 1.3 Feasibility study and formulation of alternative courses of action 1.4 Requirements and feasibility decision approval	The SDLC process should include the definition of the appropriate security requirements for each development project that has been derived from a risk assessment. The feasibility of the project will in part be determined by the impact of security requirements to the cost and/or functionality of the application.
AI2 Acquire and maintain application software. 2.1 High-level design 2.2 Detailed design 2.3 Application control and auditability 2.4 Application security and availability 2.5 Configuration and implementation of acquired application software 2.6 Major upgrades to existing systems 2.7 Development of application software 2.8 Software quality assurance 2.9 Applications requirements management 2.10 Application software maintenance	The control objectives in this category map specifically to the SDLC and are already addressed at length in other areas of this document. This set of control objectives provides the core set of control objectives for the SDLC process, and can be used as a guideline to ensure that appropriate controls are established at each step of the SDLC, regardless of whether the application is developed in-house or externally procured.
AI3 Acquire and maintain technology infrastructure. 3.1 Technological infrastructure acquisition plan 3.2 Infrastructure resource protection and availability 3.3 Infrastructure maintenance 3.4 Feasibility test environment	Just as it is important to ensure that code is developed as securely as possible, the infrastructure that contains and supports applications must also be implemented securely. Ensuring that appropriate security controls exist on web application servers and supporting network infrastructure is paramount to the overall security of web applications.

Figure 4—COBIT Control Objectives Directly Related to SDLC Security *(cont.)*	
COBIT Domains, Processes and Control Objectives	**Relation to SDLC Process Security**
Acquire and Implement *(cont.)*	
AI5 Procure IT resources. 5.1 Procurement control 5.2 Supplier contract management 5.3 Supplier selection 5.4 IT resources acquisition	Many organizations are leveraging externally procured code to augment their internal development programs. Appropriate requirements and standards should be in place to ensure that external code suppliers are selected and monitored based on appropriate security standards, that proper contract language is included to augment and support the security standards, and that the code procured from these suppliers undergoes the same level (or greater) of scrutiny as code developed in house. Additionally, appropriate policies and standards should be in place to appropriately control/restrict the use of open source code.
AI6 Manage changes. 6.1 Change standards and procedures 6.2 Impact assessment, prioritisation and authorisation 6.3 Emergency changes 6.4 Change status tracking and reporting 6.5 Change closure and documentation	It is critical to ensure that all changes to web applications are formally reviewed and approved by the appropriate stakeholders to ensure that code security is not compromised by unauthorized or *ad hoc* changes.
AI7 Install and accredit solutions and changes. 7.1 Training 7.2 Test plan 7.3 Implementation plan 7.4 Test environment 7.6 Testing of changes 7.7 Final acceptance test 7.8 Promotion to production 7.9 Post-implementation review	New systems need to be made operational once development is complete. Assurance that an application has been developed and configured securely must be an integral part of the preimplementation testing and accreditation process. This requires proper testing in a dedicated environment, definition of rollout and migration instructions, release planning and actual promotion to production, and a postimplementation review to ensure that all tests were conducted successfully.
Deliver and Support	
DS2 Manage third-party services. 2.1 Identification of all supplier relationships 2.2 Supplier relationship management 2.3 Supplier risk management 2.4 Supplier performance monitoring	Frequently organizations will have third parties providing web development services. These third-party organizations must be properly vetted and managed to the same secure coding standards and practices as would be applicable in-house.
DS5 Ensure system security. 5.1 Management of IT security 5.2 IT security plan 5.5 Security testing surveillance and monitoring 5.6 Security incident definition 5.7 Protection of security technology 5.9 Malicious software prevention, detection and correction 5.10 Network security 5.11 Exchange of sensitive data	The enterprise's IT security plan must include goals and objectives for both the secure development life cycle and for the security of the production environment that contains and supports the applications once deployed. All of the control objectives in this category either directly or indirectly support the security of web applications. Most of these controls have been discussed in other sections of this document.
DS7 Educate and train users. 7.1 Identification of education and training needs 7.2 Delivery of training and education 7.3 Evaluation of training received	Education for developers and, in some cases, end users of web applications supports the secure development process by ensuring that developers possess the appropriate skills and also helps ensure that users can recognize and report anomalies in web applications that could indicate a security flaw or compromise.

Figure 4—COBIT Control Objectives Directly Related to SDLC Security *(cont.)*	
COBIT Domains, Processes and Control Objectives	**Relation to SDLC Process Security**
Monitor and Evaluate	
ME3 Ensure compliance with external requirements. 3.1 Identification of external legal, regulatory and contractual compliance requirements 3.2 Optimization of response to external requirements 3.3 Evaluation of compliance with external requirements 3.4 Positive assurance of compliance 3.5 Integrated reporting	Frequently organizations will be required to comply with regulations such as PCI DSS or other local or global regulations that have requirements related to application security. These standards can be a helpful guide in directing and prioritizing steps to secure web applications, and can also be utilized as leverage to obtain senior management buy-in and support.

Change Considerations

There are several key change considerations associated with securing the development process. The obvious first consideration is the actual changes in the SDLC process itself that will introduce greater security rigor. These changes will likely entail new training for developers, which may result in their needing to alter perhaps long-ingrained practices. Additionally, there may be processes added to quality assurance, as well as ongoing vulnerably testing processes, that will be new and may at times conflict with other IT objectives and priorities. These changes in process must be managed carefully and should be presented to all stakeholders (well in advance) to be implemented effectively.

Another significant change may be in the time line required for development, given the additional overhead of secure processes. The expectations of the business will have to be managed (well in advance) to ensure an understanding and acceptance of the longer time frame needed to complete the development process. This is a critical consideration; if it is not addressed effectively, the development team is being set up to fail.

Finally, it is important to recognize that significant changes to SDLC processes or long-standing procedures can have broad cultural impacts to the enterprise. Despite best efforts to communicate and educate prior to instituting the required changes, some individuals may not understand or accept the new approaches and may seek ways to circumvent the new controls, introducing additional risk to the enterprise. Understanding the systemic nature of information security management, such as that described in ISACA's publication *The Business Model for Information Security*,[13] can assist in the development of strategies to address this risk.

Assurance Considerations

It is the role of the IT assurance professional to provide senior leadership with assurance that the SDLC is being managed effectively with all appropriate security considerations. It is the auditor's role to understand fully the risk that is inherent to the enterprise's SDLC and ensure that controls that have been implemented to mitigate that risk are effective and well managed, and that the security program is being run as required by organizational standards of governance and risk management. The four primary areas where assurance professionals should focus their ongoing monitoring of the SDLC process are as follows:

- **Strategy, governance and compliance**—Review the overall strategy for integrating security into the SDLC, along with any supporting policies and standards, and determine that they are (and remain) in line with overall business objectives. Verify that an effective governance framework is in place to ensure continued alignment of people, processes and technology. Ensure that applicable regulations, such as PCI, have been taken into consideration and are being adequately addressed.

[13] ISACA, The Business Model for Information Security, USA, 2010, *www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx*

- **People**—Establish that the appropriate stakeholders are engaged with the SDLC process. Review roles and responsibilities throughout the process to ensure that appropriate personnel with the correct skill sets are involved with each aspect of the SDLC process. Ensure that developers have adequate training in secure development procedures and a full understanding of how security is an integral part of the SDLC process. Check for plans for continuing development.
- **Process**—Review process documentation for SDLC and ensure that appropriate security measures are included at each step of the process. Ensure that there is a process of ongoing security testing for applications already in production and that legacy code is also reviewed for vulnerabilities. Verify that all software that is procured externally is tested and meets security standards set by the enterprise. Also ensure that there are standards and associated processes to ensure that web applications provided and/or managed by third parties are subject to the same security controls throughout their life cycle.
- **Technology**—Check for the presence and effective management of technical controls that specifically protect the enterprise's Internet-facing applications. Particularly for environments that have a great deal of legacy code still in production, ensure that technical controls such as application firewalls are in place to mitigate the risk of code that has yet to be reviewed.

The ISACA *Systems Development and Project Management Audit/Assurance Program*,[14] which was developed in alignment with the ISACA COBIT 4.1 framework,[15] is an effective tool that can be used to help plan and guide an audit of the SDLC.

Conclusion

Ensure that organizational leadership understands the issue and the potential impact of web application vulnerabilities.

It is possible for enterprises to enjoy the numerous benefits of web applications without incurring significant additional risk. However, a structured, systemic approach to securing the development life cycle and all of its ancillary processes is critical to ensure that web applications do not become a liability to the enterprise. There is a significant amount of information and support available, much of it free, that can provide assistance in this endeavor, but the most important first steps are to ensure that organizational leadership understands the issue and the potential impact of web application vulnerabilities and, based on that understanding, commit their support and the resources required to accomplish the task.

Additional Resources and Feedback
Visit *www.isaca.org/web-application-security* for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.

[14] See ISACA, *Systems Development and Project Management Audit/Assurance Program*, USA, 2009 *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/Audit-Programs/Documents/SysDevandProjMgmt_Prog_20Jan09_Research.doc*
[15] See ISACA, COBIT 4.1, USA, 2007, *www.isaca.org/cobit*