Security Application Management Services

Creating value, managing risk
A continuous improvement approach to security management

Overview

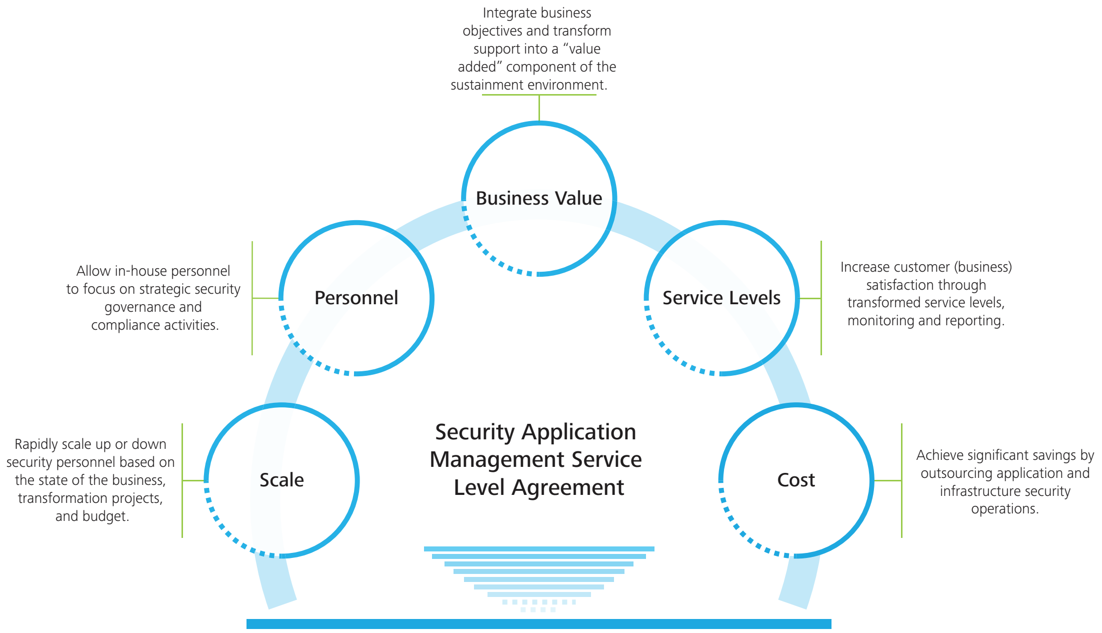
An expansive landscape demands secure management

For organizations struggling to keep up with an ever-evolving security landscape, finding the right balance between improving overall security effectiveness and controlling the growing cost of security operations can be a formidable task. Additional and equally important concerns, such as scarcity of skilled resources, lack of formal processes, and governance complexities, can also be daunting challenges. As a result, many organizations are looking to outsource some or all of their security management processes.

> As much as 60 percent to 70 percent of the energy that information technology (IT) security teams put into technology is focused on maintaining what has already been built. That's a considerable effort, considering how rapidly technology can become obsolete. And that effort is beginning to hinder some of our clients' ability to innovate. That's where Deloitte can help.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Top reasons why our clients outsource security management


Integrate business objectives and transform support into a "value added" component of the sustainment environment.
Business Value
Allow in-house personnel to focus on strategic security governance and compliance activities.
Personnel
Service Levels
Increase customer (business) satisfaction through transformed service levels, monitoring and reporting.
Rapidly scale up or down security personnel based on the state of the business, transformation projects, and budget.
Scale
Security Application Management Service Level Agreement
Cost
Achieve significant savings by outsourcing application and infrastructure security operations.

The problem

Managing security talent

Organizations are challenged to attract, retain, and afford the personnel required to provide high levels of security. But without proper analysis and strategic sourcing, talent management can become increasingly expensive and directly impact solution quality, agility, and return on investment (ROI). In addition, security staff workloads are not static. Ideally, the size and composition of the team should change with the peaks and valleys of demand. What's more, it can be difficult for security professionals to focus on proactive, higher value work when they are overwhelmed with day-to-day operational tasks.

Maintaining a high-performance, high-quality security environment

With rapid changes in user behavior and business models, many security teams are hard-pressed to respond. For example, cloud computing models and enterprise mobility represent a fundamental challenge to organizations' traditional security architecture, perimeters, and solutions. Add the growing burden from regulators and partners, and it's clear that a new approach to security is needed — one that benefits from world-class resources, strategies, standardized methodologies, and consistent processes to create a responsive and agile security program.

Preparing for the future

In the face of rapidly evolving threats, it may be difficult for organizations to effectively pre-design the way they protect today's critical data and Intellectual Property (IP) through tomorrow's technology. Effective security application management can handle the smarter, bolder, and more cunning cyber-attacks of the future, without adding to the management burden or slowing down business processes.

How can organizations get more for their investments in security? Deloitte can help.

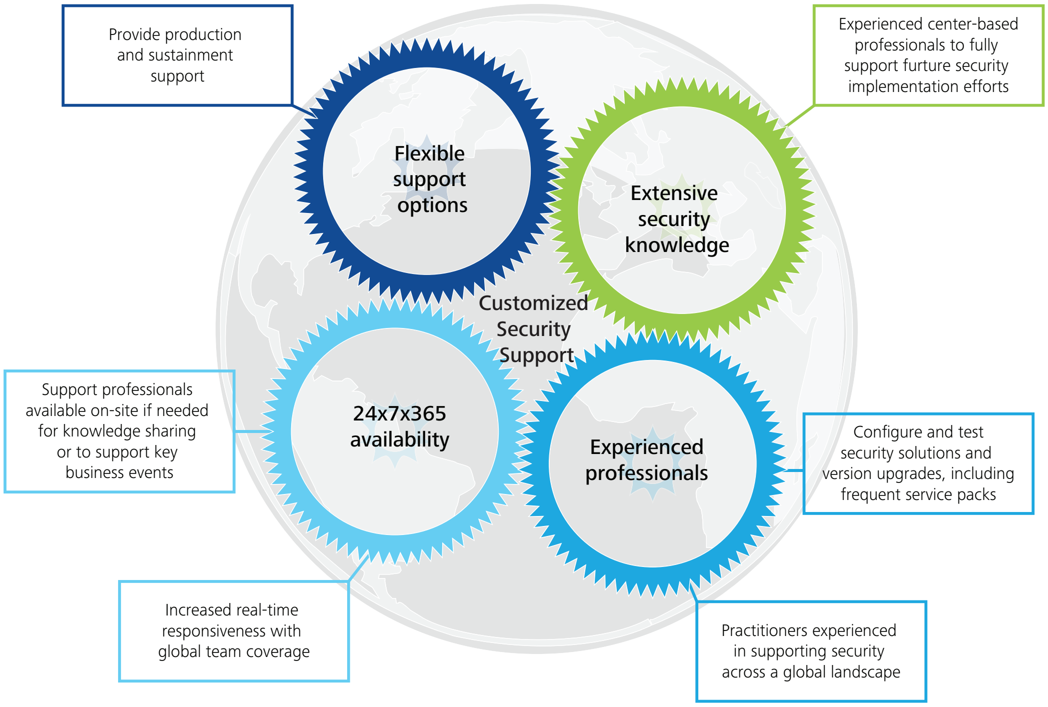
A fresh approach

Managed services global delivery

Traditionally, managed services have been defined as the set of disciplines encompassing services for managing, enhancing, and maintaining custom or packaged software. Deloitte's Security Application Management Services (AMS) go beyond the traditional, providing specific services and solutions to help clients manage the ongoing security of their platforms and infrastructures. Security AMS is also part of our broader Cyber Risk Services, which are designed to help companies reap the value of their strategic investments by becoming more secure, vigilant, and resilient.

Deloitte's security management methodology, demonstrated tools, and resources, as well as the capabilities and deep experience of our global team, are focused on delivering managed security that meets each client's specific business requirements. We offer a full suite of flexible, customized security operations and support services, including:

- **Infrastructure Security:** Operating system, network, and storage device hardening; firewall management; Network Intrusion Detection Systems and Intrusion Protection Systems (IDS/IPS) management; Security Operations Center (SOC); Public Key Infrastructure (PKI) management and administration
- **User Identity and Access:** Identity administration; identity lifecycle management; user access review/ certification; access management; privileged user management; cloud identity and access management
- **Application Security:** Enterprise resource planning (ERP) systems; user administration; application role management; governance, risk, and compliance (GRC) tools management (e.g., SAP, Approva, Oracle)
- **Security Operations Support:** Ongoing controls review and testing (e.g., periodic control rationalization and review; ongoing IT security controls benchmarking)
- **Cyber Operations:** Threat and vulnerability management; security information event management (SIEM); cyber threat monitoring; data loss prevention (DLP); operations management


Flexible support options
Extensive security knowledge
Customized Security Support
24x7x365 availability
Experienced professionals

Provide production and sustainment support

Experienced center-based professionals to fully support furture security implementation efforts

Support professionals available on-site if needed for knowledge sharing or to support key business events

Configure and test security solutions and version upgrades, including frequent service packs

Increased real-time responsiveness with global team coverage

Practitioners experienced in supporting security across a global landscape

A structured, seamless transition

Every organization has unique business requirements and security challenges. As a part of our methodology, we conduct a risk assessment to help examine the current environment and identify critical needs. This information is used to guide the transition plan and target areas of focus. For example, if institutional knowledge transfer is determined to be a risk, a plan can be developed to capture that information prior to the transition.

Through the risk assessment process, business and technology outcomes are clearly documented and a plan is created to achieve them. The ultimate objective is to forge a working relationship where services are delivered in an open and transparent manner.

To help deliver a smooth transition to full production support of a client's security environment, we follow a rigorous three-phase process that relates to clients' production support set-up, stabilization and steady state needs.

Plan and define activities

- Gain an understanding of the existing security operations environment
- Identify and document the client professionals or departments who are to be "Responsible, Accountable, Consulted, Informed" via a RACI chart
- Create security support run-books to capture activities that the team will own

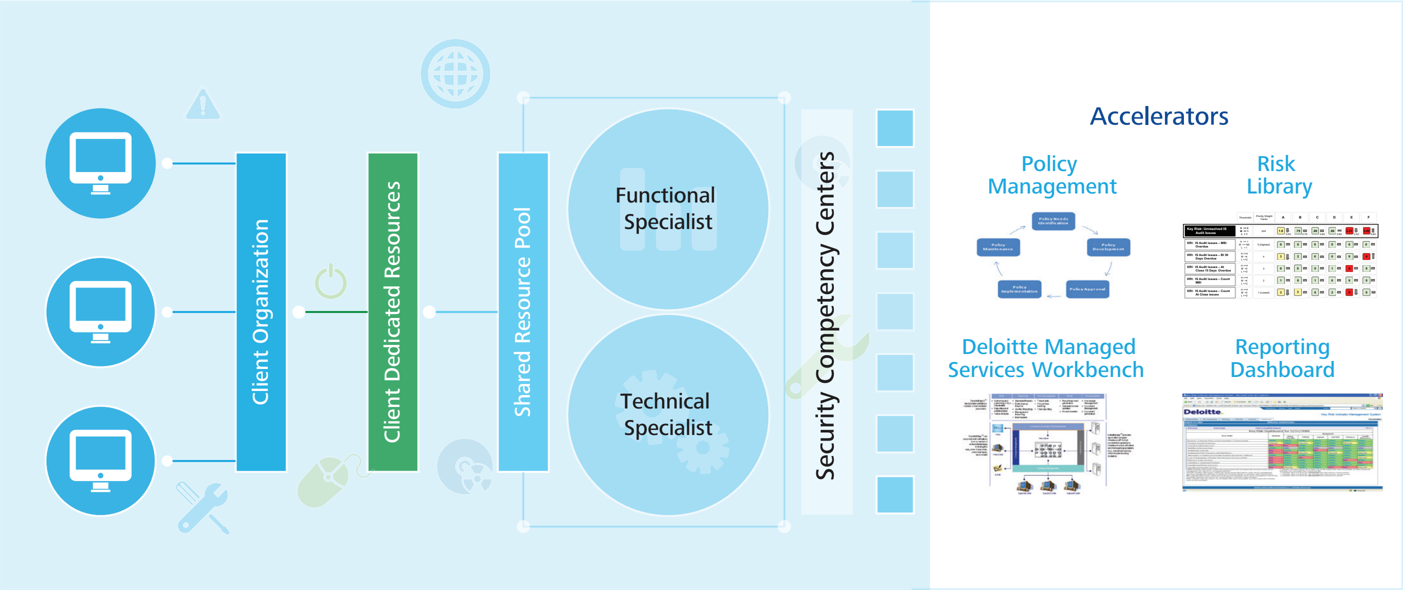
Stabilization activities

- Use a managed services support solution that utilizes a cost-competitive, flexible, and scalable staff augmentation model
- Develop a broad security support model (e.g., 24x7x365 or 18x5x365) with finely defined response times on security issues

Steady state

- Create an approach to help the clients' security team focus on allowing for more complex solving in-house
- Develop and enhance existing security policies and obtain recommendations for new security procedures
- Create a standardized security roles approach that considers risk for performing security activities

Our managed services transition methodology facilitates a seamless process from implementation to application operations and service delivery excellence — while minimizing disruption to business operations.



Ongoing security management

Once security management has fully transitioned to Deloitte, our operating model allows us to dynamically respond to client needs with the appropriate resources in an efficient manner. For example, capacity can quickly scale up or down as dictated by business events through the use of shared resource pools.

Quality and risk are closely managed via standardized processes, technologies, and trained professionals. Our integrated collaboration network puts the collective knowledge of the entire Deloitte community at the fingertips of security professionals — expediting the use of leading practices and innovative approaches to help address strategic opportunities.

In addition to managing day-to-day security operations, we look for opportunities to deliver additional value through proactive maintenance that promotes data quality, process improvement to identify and address recurring problems, special projects, and more. By engaging Deloitte's Security Application Management Services, clients gain access to top security professionals across the globe to assist in addressing a wide variety of business challenges, from implementation of new solutions to responding to the rise of new threats.

Innovative security tools and accelerators

Tools and accelerators — Deloitte managed services workbench

Our standard Deloitte workbench focuses on efficiently executing tasks and delivering managed services to our clients. Designed to meet global standards, this set of tools, methods, and processes allows us to respond dynamically to client needs.

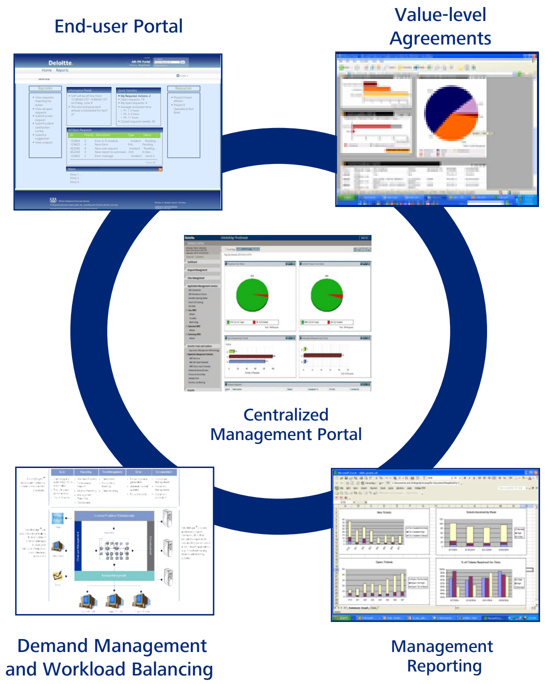
We have also developed a portfolio of proprietary accelerator tools to assist with the analysis of security-related information and the execution of Security AMS, which include:

Key IT Risks and Key Risk Indicators library: A library of measurable risks and KRIs for common business functions and processes to establish baselines for key security performance indicators, value, and the prioritization of improvement opportunities for our clients.

Reports and dashboards: A series of custom, IT security-focused analysis reports that proactively identify risk areas and address concerns related to risk.

RACI templates: An inventory of activities used to effectively design IT management security processes according to roles and responsibilities within an organization — streamlining clients' internal processes and identifying any gaps that may exist.

Deloitte application managed services workbench


End-user Portal
Value-level Agreements
Centralized Management Portal
Demand Management and Workload Balancing
Management Reporting

A dynamic portal to provide collegues a one-stop shop to access standard tools, templates, methods, and processes to more consistently and efficiently deliver managed services

Proof-of-concept environments: A separate area to develop and test integration plans and system functionality, provide ongoing benchmarking against industry-leading security practices, and assist with routine and proactive identification of potential security risks.

Risk catalog: An integrated risk and compliance solution used to identify the applicable laws, regulations, and industry standards and leverage the relevant requirement sections to generate the custom set of control requirements for policies and/or standards.

Business unit self-assessment methodology: An enterprise approach for evaluating and optimizing operational risk and compliance in a meaningful, efficient, and consistent approach across the enterprise.

Policy management lifecycle: A customizable set of processes and activities for establishing, developing, reviewing, approving, monitoring, and updating policies, standards, and procedures through their lifecycle as the business and regulatory environments evolve.

Problem management tools and knowledge database: Application- and process management-specific capabilities that streamline incident reporting, escalation, and response and support knowledge management; help sharing of problem resolutions for future reference across Deloitte.

A pre-configured platform to accelerate the scoping, configuration, and execution of managed services, providing:

- Management Methods Manager (M-MM): Modular playbook and templates for defining and delivering managed services
- Management Estimating Model (M-EM): Data-driven, quantitative model for estimating application management resource capacity
- Management Knowledge Manager (M-KM): Knowledge base with reusable deliverables, templates, and accelerators
- Management Client Manager (M-CM): Set of interactive applications and survey tools to measure satisfaction and improve client experience

The Deloitte difference

End-to-end security services from a single provider

With access to more than 40 Service Centers around the globe, Deloitte has the ability to leverage a large pool of security professionals located on-site, near-site, and offshore. Furthermore:

- Our broad portfolio of security capabilities is backed by personnel with very deep technical knowledge regarding threats and the processes and tools to protect against them
- Our methodologies and tools represent some of the most innovative thinking in the security industry
- Our specialists continually evaluate and integrate new capabilities as they become available
- Our skills and focus cover more than outsourced security management, allowing us to help organizations address nearly every security challenge or need

We offer multiple delivery models to suit the maturity and security needs of our clients, including:

- A reactive support augmentation model that supplements a client's current resources and practices
- Several joint management models, which allow Deloitte to share security responsibilities with a client's team
- A value-level management model that streamlines security to minimize risks, optimize resources, and achieve the maximum ROI

Our specialists, who come from regulatory and auditing backgrounds, have completed intensive immersion security training. They also have deep experience with cyber and application risks and compliance concerns, understand business processes, and focus on executing high-quality services at a competitive price.

Boosting results

Going beyond point solutions to provide full-cycle managed services, Deloitte helps organizations address today's security management challenges. Deloitte is well-positioned to:

- Deliver leading IT security services, processes, and functions by drawing on leading practices, accessing a global network of resources, and utilizing an ITIL-based integrated workbench
- Enable desired business outcomes and performance improvement by making practical decisions about application alignment, enhancements, and innovations
- Drive the development of better, smarter, and faster applications, operations, and frameworks by focusing on the business of IT security
- Continuously evolve and innovate the application security portfolio in line with evolving business objectives
- Provide actionable intelligence to help clients respond more quickly and effectively to cyber threats
- Help improve a company's security posture and protect its infrastructure by helping to define and move toward its end-state vision

Our Security Application Management Services assist with resource alignment, information protection, and risk management while utilizing leading practices, driving efficiencies, and helping our clients protect their organizations against even the most dangerous

> "The firm (Deloitte) continually develops, tests, and launches methodologies that reflect a deep understanding of clients' cyber security and help the firm stay ahead of the curve and set the bar in terms of addressing cyber security consulting needs."

— Kennedy Consulting Research & Advisory; Cyber Security Consulting; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC. Reproduced under license

Our credentials

Staff — Deloitte in the U.S., and globally through the Deloitte Touche Tohmatsu Limited network of member firms, has:

- 11,000 risk management and security professionals globally
- 8,000+ staff involved with ISACA globally; ~2,000 certified as CISA, CISM and CGEIT
- 7,100 security professional in the Americas
- Over 1,100 CISSPs — more than any other organization

Analyst accolades

- Ranked #1 in security consulting, globally and in North America, by Gartner[1]
- Listed as a global leader in cyber security consulting by Kennedy[2]
- Named a global leader in security consulting by Forrester[3]
- Ranked #1 in 2013 World's Best Outsourcing Advisors List by the International Association of Outsourcing Professionals®[4]

Industry and academic sponsorships

- Proprietary industry proficiency and certification program
- American Society for Industrial Security (ASIS)
- Cloud Security Alliance
- Information Systems Audit & Controls Association (ISACA)
- International Information Systems Security Certification Consortium (ISC)2
- International Associate of Privacy Professionals (IAPP)

Industry and academic sponsorships

- Executive Women's Forum
- ISC(2) Cybersecurity Children's Awareness Program

[1] Lawrence Pingree, "Market Share Analysis: Security Consulting, Worldwide, 2012," Gartner, Inc., 16 May 2013.

[2] Kennedy Consulting Research & Advisory; Cyber Security Consulting; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC

[3] Ed Ferrara and Andrew Rose, "Forrester Wave™: Information Security Consulting Services Q1 2013," Forrester Research, February 1, 2013.

[4] "The World's Best Outsourcing Advisors for 2013," International Association of Outsourcing Professionals® (IAOP®).

Contact us

To discuss your unique challenges and how Deloitte can help you, please contact any of the Deloitte professionals below or visit us online at **www.deloitte.com/us/cyberrisk.**

Ed Powers
National Managing Principal
Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

Tapan Shah
Director
Security Application Management
Services Lead
Cyber Risk Services
Deloitte & Touche LLP
+1 571 766 7469
tapanshah@deloitte.com

Manoj Bhale
Senior Manager
Deloitte & Touche
India Private Limited
+1 615 718 5756
mbhale@deloitte.com

Chirag Patel
Senior Manager
Deloitte & Touche LLP
+1 713 982 3172
chirpatel@deloitte.com

Stephen Sutherland
Specialist Leader
Deloitte & Touche LLP
+1 415 783 5846
stsutherland@deloitte.com

Industry leaders

Consumer Products
Beth Larson
Deloitte & Touche LLP
+1 612 397 4190
belarson@deloitte.com

Financial Services
Vik Bhat
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

State & Local Government
Srini Subramanian
Deloitte & Touche LLP
+1 717 651 6277
ssubramanian@deloitte.com

Energy & Resources
Adnan Amjad
Deloitte & Touche LLP
+1 713 982 4825
aamjad@deloitte.com

Health Care
Mark Ford
Deloitte & Touche LLP
+1 313 394 5313
mford@deloitte.com

Technology, Media & Telecom
Irfan Saif
Deloitte & Touche LLP
+1 408 704 4109
isaif@deloitte.com

Federal
Gordon Hannah
Deloitte & Touche LLP
+1 571 882 5930
ghannah@deloitte.com

Life Sciences
Bruce Murphy
Deloitte & Touche LLP
+1 973 602 6020
brmurphy@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, shall not be responsible for any loss sustained by any person who relies on this publication.