KPMG

Secure Development Lifecycle

KPMG Cybersecurity

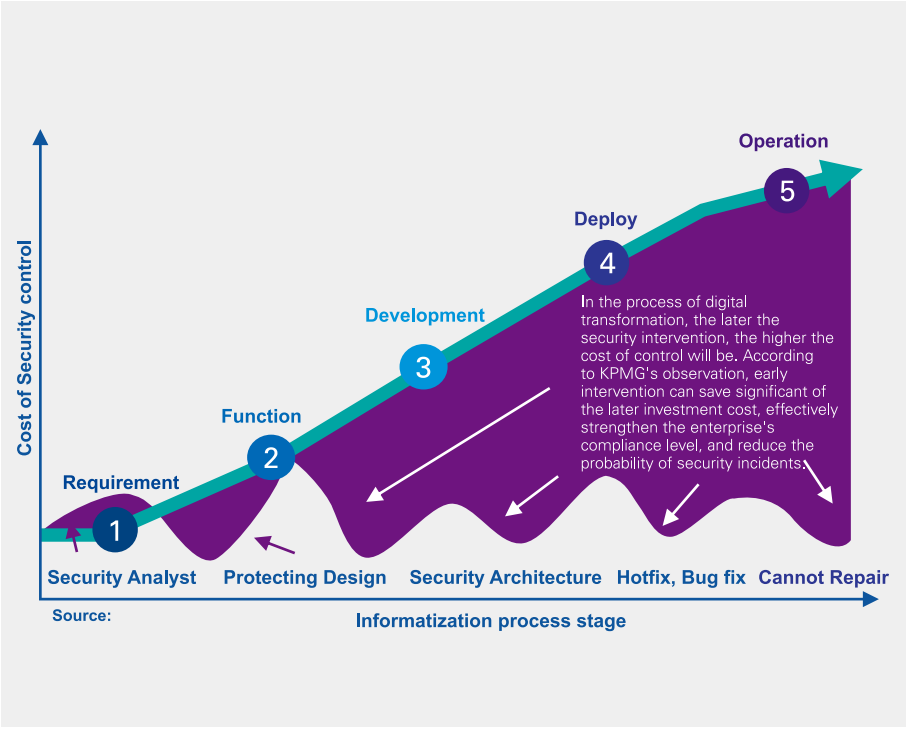
KPMG China

kpmg.com/cn

What is Secure Development Lifecycle ?

Secure Development Lifecycle(SDL) is a system development process that helps developers build more secure systems and solve security compliance requirements while reducing development costs. The core idea of SDL is to integrate security considerations into every stage of system development: requirements analysis, design, coding, testing and maintenance. The security activities executed in different stages are also different. Each activity can play a certain role in system security even if it is executed separately.

According to the report of NIST and other authorities, more than 90% of hacker security incidents happen in the application system itself, not in the network. However, most of the IT risk events that cause damage to the organization come from application logic defects rather than general component defects.The National Institute of standards and Technology (NIST) estimates that if a project executes a bug fix plan after it is released, the cost of the fix is equivalent to 30 times the cost of the fix at the design stage.



Secure Development Lifecycle is now a key compliance requirement

In recent years, cybersecurity has become a key area of supervision by national regulatory authorities. More and more regulators have realized that one of the key tasks of cybersecurity is to embed the security controls in the early stage of information system development, and relevant regulatory regulations of various industry sectors have been issued successively, for example:

- **China Cybersecurity Law - personal information security engineering**
- **European Union General Data Protection Regulation - privacy by design**
- **Guidelines for IT Risk Management of Commercial Banks**
- **Automatic Software Process Improvement and Capability Determination**
- **Trusted Information Security Assessment Exchange -**
- **……..**

KPMG Secure Software Development Service

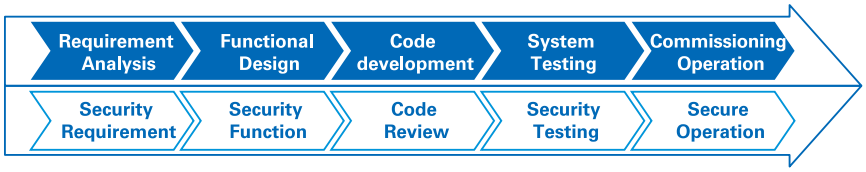
KPMG Secure Software Development Service combines compliance requirements with organizations' current situation, fully evaluates organizations' potential risks in the process of software development, and adopts different secure development methods in combination with different development modes to improve organizations' security capability and software efficiency.

Based on our industry experience, we provide different secure development methods according to different development models, including:

- **Secure development of traditional waterfall steady state method (SSD)**
- **Secure development of agile method with fast iteration(SAD)**
- **Secure development in DevOps method(DevSecOps)**

Secure development of traditional waterfall steady state method (SSD)

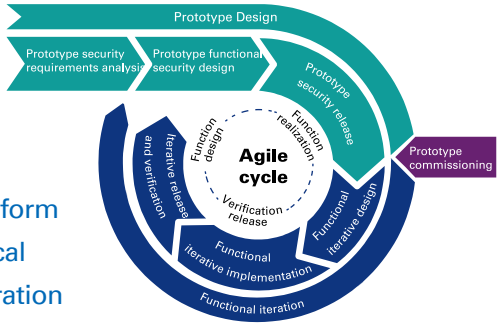
The waterfall steady-state development method pays more attention to the smoothness of work connection with project teams. The steady-state method is dominated by linear process and output check. The security team will participate in the development phase as the role of security and quality control supervision. The meaning of "left shift" refers to promoting the security to move left on the development cycle line.



Secure development of agile method with fast iteration(SAD)

In the prototype design stage, agile secure development pays more attention to the design and implementation of the underlying security architecture, the development of the program standard security SDK library, the collection of the standard function library and the formulation of the API service security standard, so as to lay a solid security foundation for the future rapid iteration

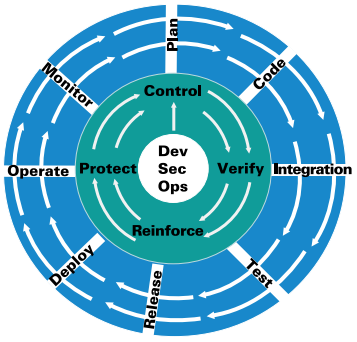
Key success factor
-Cultural uniform
-Goal Identical
-Team integration



Secure development in DevOps method(DevSecOps)

In the framework of DevOps cooperation, security protection is the common responsibility of the whole IT team, which needs to run through every link of the full life cycle. Effective DevOps security requires more than just tools. It needs the whole organization to realize DevOps cultural change, so as to integrate the work of security team as early as possible

Key success factor
-Empowerment
-Enablement
-Education



Benefits from Secure Software Development

According to organizations' different development models, establishing secure software development framework can help organizations improve the confidence of stakeholders on informatization and digital transformation, enhance public trust, reduce the probability of security incidents, and meet compliance requirements.

-Accidents
-Errors
-Attacks
-Security Breaches

-Trust
-Compliance
-Security Investment
-Quality

Contact us

Henry Shek
KPMG China
Cybersecurity
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang
KPMG China
Cybersecurity
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Quin Huang
KPMG China
Cybersecurity
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Danny Hao
KPMG China
Cybersecurity
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

Brian Cheung
KPMG China
Cybersecurity
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

Frank Wu
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

Jason Song
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

Jason Li
KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

John Chiu
KPMG China
Cybersecurity
Associate Director
Tel: +852 2847 5096
john.chiu@kpmg.com

Kevin Zhou
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

Kevin Fan
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 2200
kc.fan@kpmg.com

Olive Wang
KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8553 3630
oh.wang@kpmg.com

Andy Yuen
KPMG China
Cybersecurity
Associate Director
Tel: +852 3927 4697
andy.yuen@kpmg.com

William Xu
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 4633
william.q.xu@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg.com/cn/en/home/about/offices.html