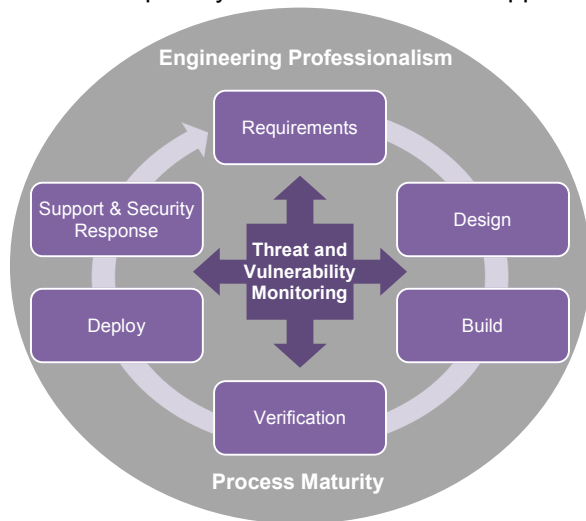


# Nexor Service Description: CyberShield Secure™ Development Service

In today's connected world, more and more organisations are moving information across cyberspace, whether to improve decision making, increase productivity or to reduce IT spend by adopting lower cost models such as the Cloud. When it comes to moving sensitive information, there needs to be confidence that the underlying software systems will provide adequate protection. Whilst many IT systems come ready-made off-the-shelf, there is often a need for a specific solution or integration work to achieve the required level of security and Information Assurance. Creating secure systems is a specialised job that requires processes and methods designed to build in security from the very first stages in the lifecycle. Nexor has over 20 years' experience of developing secure solutions for defence and government agencies, so has the capability and infrastructure to support these activities.



Nexor's CyberShield Secure™ Development facility provides a UK sovereign capability to produce high assurance software. Nexor offers a full outsourcing service to build, enhance, integrate, port or productise secure solutions for customers. The CyberShield Secure™ Lifecycle can be applied in both Agile and Waterfall projects. In either case, Nexor ensures that security objectives are established and developed throughout the lifecycle.

## Security

Threats and security requirements are analysed alongside the functional requirements; both are captured in Unified Modelling

### Requirements

- Threat types
- Intrusion attempt types
- Attack methods
- Resilience, availability and redundancy
- Information sensitivity levels
- Implications of encryption and decryption
- Accessibility constraints

Language (UML), a standardised methodology for modelling the structure, behaviour and interactions of system elements. Security objectives and requirements are identified from both physical, platform and software perspectives.

### Design

- Threat elimination, protection and mitigation
- Threat modelling
- Surface attack modelling
- Third party component review
- Traceability of design against requirements

In developing high and low level design documents, the security requirements are translated into the design using proven

best practices, patterns and principles, paying particular attention to any approaches that are prone to the introduction of security error. A comprehensive Threat Model is also built, which facilitates accreditation activity.

During the Build phase, several approaches are employed to embed security into the systems. Nexor uses a configuration management system to securely manage and store the source code.

### Build

- Rigorous coding standards
- Elimination of banned functions
- Static analysis
- Peer review
- Common libraries
- Trusted suppliers

## Benefits:

### Reduced Risk:

- Expert skills from domain specialists
- Professional engineering teams:
  - Certified Secure Software Lifecycle Professionals (CSSLP)
  - Certified Information Systems Security Professionals (CISSP)
  - Members of the Institute of Information Security Professionals
- Established methodologies
- Constant threat and vulnerability monitoring
- Robust and integral methods and techniques based on industry best practice: CMMi, TickITplus; ISO9001/TickIT, ISO/IEC27001:2005 and Lean

### Reduced Cost:

- Right first time
- On or below budget
- Superior quality
- Open standards
- Standardised output
- Agile approach for faster project completion

connect transform protect

**NEXOR**®  
www.nexor.com

# Security Through the CyberShield Secure™ Lifecycle cont'd

Completed code passes through the CyberShield Secure™ verification suite where it is thoroughly tested by ISEB qualified testers. During this phase, accreditation document sets are written ready for delivery with the final

## Verification

- Bound checking
- Fuzz testing
- Resilience tools
- Verify threat model
- Negative testing
- Traceability of requirements against tests

Nexor's service includes

a step to ensure that the customer has processes in place to manage threats and attacks. A Support and Security Response service is available to maintain the currency of the system via patches. Nexor's patch management system ensures patches are prepared and fully tested for each identified code vulnerability. Patches are digitally signed before publication to guarantee integrity and authenticity.

## Deploy

- Incident response plan
- Release review

## Support & Security Response

- Security patch management
- Execute incident response plan

## About Nexor

We connect, transform and protect sensitive information in cyberspace

## Threat and Vulnerability Monitoring



To ensure state-of-the-art threat and vulnerability monitoring, Nexor uses a range of reference databases including:

- The Common Weakness Enumeration (CWE) database, which contains Software Weakness Types including the "SANS TOP 25 most dangerous software errors".
- The Open Web Application Security Project (OWASP), which contains lists and details of the Top Web application security risks.

## Engineering Professionalism

Nexor keeps a constant eye on new industry trends and best practice. CESG\* guidance, specifically that found in its assurance guidance model, is a primary influence.

Other inputs to best practice and procedure include CERT (from the US Software Engineering Institute), "Build Security In" initiatives and Microsoft's Secure Development Lifecycle. Feedback loops are built in throughout the CyberShield Secure™ Lifecycle to ensure early capture and rectification of

### Intrinsic:

- Provenance
- Build quality
- Methodology
- Process

### Extrinsic:

- Proof of security
- Test techniques applied

CESG Assurance Guidance

### Operational:

- Continuous operation
- On-going currency
- On-going security

### Implementation:

- Real world projection
- Test lab authenticity

## Process Maturity

Nexor has been committed to implementing industry standards and processes since the 1990s and was also the first UK company to achieve TickITplus certification. The CyberShield Secure™ Lifecycle has been developed over several years in accordance with Capability Maturity Model integration (CMMi) using Lean techniques. This work represents a major investment and a significant UK sovereign capability.

## Contact Us

For further information on CyberShield Secure™ Development, please contact [info@nexor.com](mailto:info@nexor.com)

[www.nexor.com](http://www.nexor.com)

Information in this document is provided "as is" without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement.

\* CESG is the UK National Technical Authority for Information Assurance