



# Security Principles

December 2018





# Security Architecture Principles

## Architecture Principles

Simplicity over Flexibility

Usability over Restriction

Defence in Depth

## Implementation Principles

Usability over Restriction

Context is Key

Secure Coding Practices

Protection against Insider and Outsider Attacks

## Operational Principles

Complete Mediation

Explicit Responsibility and Ownership

Least Privilege and Separation of Roles

Accountability



# Security Architecture Principles

## Architecture Principles:

- **Simplicity over Flexibility:** your security mechanisms should be pervasive, simple, scalable, and easy to manage - flexibility often leads to complexity.
- **Usability over Restriction:** focus on making the control usable, so your users are not inclined to find methods to work around them.
- **Defence in Depth:** do not rely on single controls which in the event of failure have no secondary compensating controls.

## Implementation Principles:

- **Open Design:** security by obscurity is ineffective.
- **Context is Key:** context should be explicit and not assumed.
- **Secure Coding Practices:** build the system securely, reduce costs and future security issues.
- **Protection against Insider and Outsider Attacks:** do not assume insiders are always benign.



# Security Architecture Principles

## Operational Principles

- **Complete Mediation:** every event must be checked for authority.
- **Explicit Responsibility and Ownership:** ensure your system and data owners are aware of their responsibilities. \*
- **Least Privilege and Separation of Roles:** only grant the access required for a specific role.
- **Accountability:** solutions must collect audit information on system operations.

\* It is implicit that data and systems have explicit owners



# Security Objectives

Meeting these objectives ensures your business's security:

- Focus on the business
- Deliver quality and value to the stakeholders
- Comply with relevant legal and regulatory requirements
- Provide timely and accurate information on security performance
- Evaluate current and future information threats
- Promote continuous improvement in information security
- Adopt a risk-based approach
- Protect classified information
- Concentrate on critical business applications
- Develop systems securely
- Foster a security-positive culture



# Rheinberry – an introduction...

- Rheinberry created in 2014
- Formed by experienced IT and business consultants
- Expertise across aviation, telecoms, utilities, retail, finance, pharmaceuticals and engineering
- Delivery focussed & flexible
- Provision of seasoned consultants providing programme & project management, business & technical analysis, architecture and strategy
- IBM Business Partner
- Siemens MindSphere Partner

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

[info@rheinberry.com](mailto:info@rheinberry.com)