SECURITY OPERATIONS AND ADMINISTRATION

(ISC)²®

The Waterfall Model

- Requirement Gathering and Analysis
- System Design
- Implementation
- Integration and testing
- Deployment of system
- Maintenance

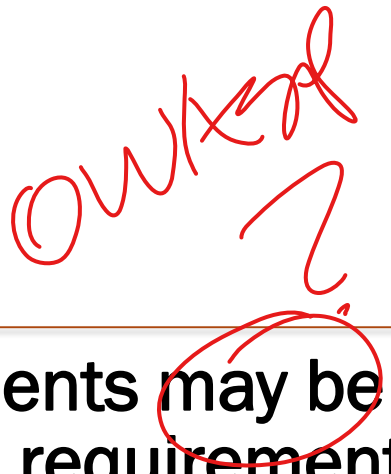
Benefits and Drawbacks

- **Benefits**
  - Ease of use and management
  - Broad scope
  - Detailed specificity of systems documentation

- **Drawback**
  - Assumes a static set of requirements captured before design and coding phases begin

Requirements Definition

Functional and nonfunctional requirements are documented



Security requirements may be incorporated within the nonfunctional requirements specification

System Design

Design may first be laid out in a general design document

Design walkthroughs are often held to review the design before construction

Implementation

Software programming is completed in this phase

Functional design specifications are translated into executable processes using one or more programming languages

Integration

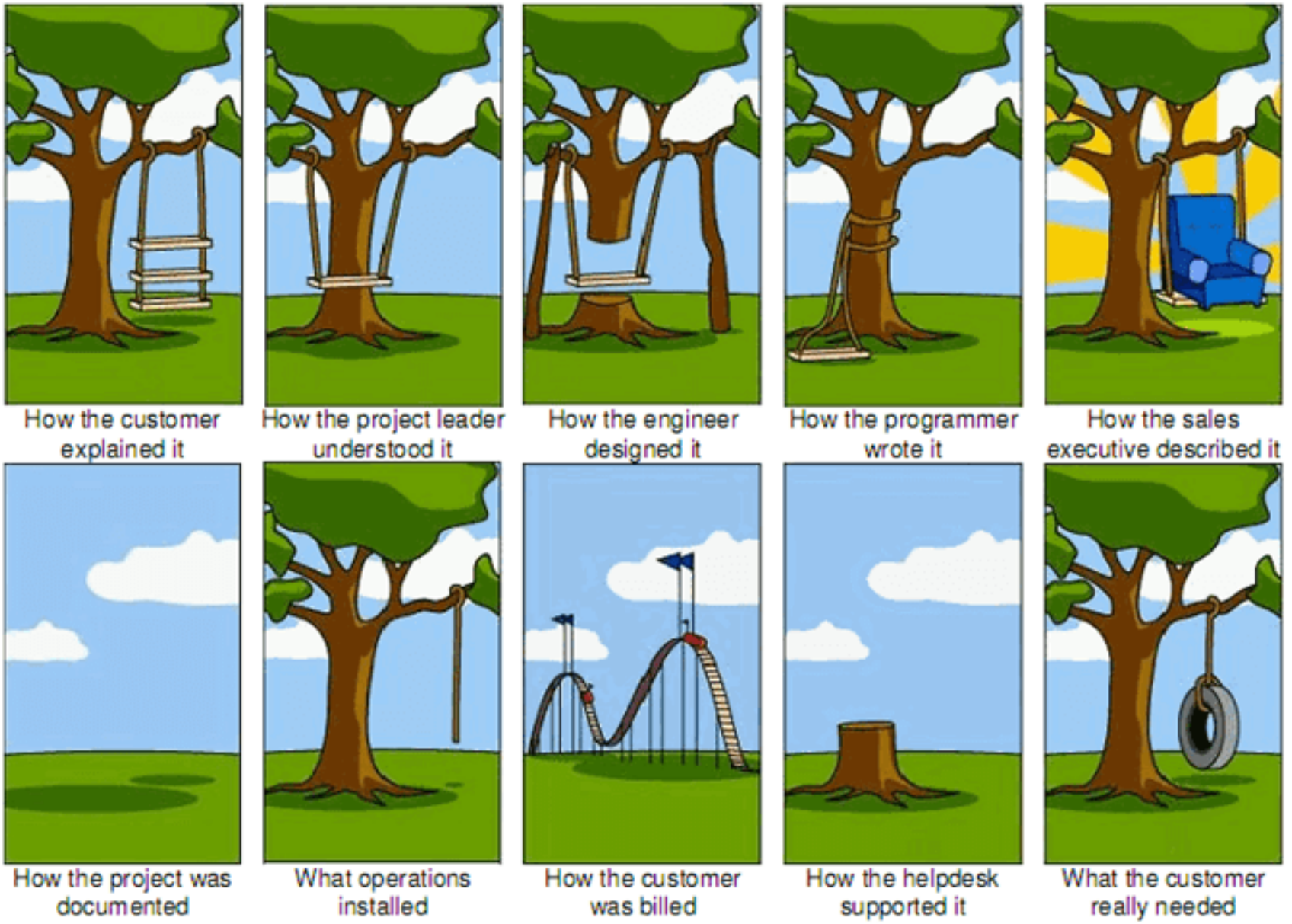
Integration occurs when multiple functional units of code or modules that form the application are compiled and run together

Testing

- Testing is not a separate phase of waterfall development projects
- Different types of testing and debugging occur from construction to installation and beyond
  - Unit testing
  - Integration testing
  - System testing

Deployment of System

- When the application has been system tested, it is installed into a controlled environment for quality assurance and user acceptance testing
- At this stage, the application is considered to be in its final form


How the customer explained it
How the project leader understood it
How the engineer designed it
How the programmer wrote it
How the sales executive described it
How the project was documented
What operations installed
How the customer was billed
How the helpdesk supported it
What the customer really needed

Maintenance

Changes in business needs and practices, newly discovered bugs and vulnerabilities, and changes in the technical environment all necessitate changes to production applications

Additional Application Development Methods

Spiral model

Extreme Programming and Rapid Application Development

Agile Development

Component Development and Reuse

Open Web Application Security Project (OWASP) Top Ten

The OWASP provides a freely available listing of the top vulnerabilities found in web applications

Guidelines for Developers

- Authentication
- Authorization
- Session management
- Encryption of sensitive data
- Input validation ← Fuzzing
- Disallow dynamic queries
- Out-of-band confirmation
- Avoid exposing system information
- Error handling

Device Management

Hardware Asset Management (HWAM)

Software Inventory Management (SWAM)

Configuration Setting Management (CSM)

Vulnerability (Patch) Management (VUL)

The SSCP's Challenge

Many companies consider Hardware Asset Management (HAM)/Software Asset Management (SAM) to be an unnecessary expense

SSCP®
Systems Security
Certified Practitioner

(ISC)²®

Secure Information Storage

- **File/folder encryption is simpler and faster to implement**
  - Presents exposures if the operating system or user of the machine writes data to an unencrypted location

- **Full disk encryption protects the entire contents of a laptop's hard drive**

Database Encryption

Database size

Performance

Application compatibility

Data Scrubbing

- Wholesale replication of data from production to test is a common practice
- Wholesale replication of security controls from production to test is not
- The goal of data sanitization is to obfuscate sensitive data

Data Deduplication

Deduplication is a process that scans the entire collection of information looking for similar chunks of data that can be consolidated

Managing Encryption Keys

- Key management refers to the set of systems and procedures used to securely generate, store, distribute, use, archive, revoke, and delete keys
- Key management policy identifies roles, responsibilities, and security requirements

Considerations

- Roles and responsibilities
- Key generation and storage
- Distribution
- Expiration
- Revocation and destruction
- Audit and tracking
- Emergency management

Information Rights Management (IRM)

IRM functions to assign specific properties to an object such as how long the object may exist, what users or systems may access it, and if any notifications need to occur when the file is opened, modified, or printed

Data Retention and Disposal

Record retention policy and schedule

Handling procedures

Shredders

Strip-cut shredders

Cross-cut shredders

Particle-cut shredders

Hammermills

Granulators

Destruction of Magnetic Media

Methods of destroying data contained on magnetic media include various techniques for clearing or sanitizing data

Cloud service providers should support eradication of data when deleted

Disclosure Controls: Data Leakage Prevention

- Data discovery
- Labeling
- Policy creation
- Content detection/monitoring
- Prevention or blocking
- Reporting

Technical Controls

- **Technical controls are security controls that the computer system executes**
- **The controls can:**
  - Provide automated protection from unauthorized access or misuse
  - Facilitate detection of security violations
  - Support security requirements for applications and data

Operational Controls

- Operational Control policies address process-based security controls implemented and executed by people
- Two types of operational security problems:
  - Accidental misconfigurations
  - Deliberate misconfigurations

Operational Solutions

- Operational security policy
- Change management process
- Access control
- Authorization
- Dual control
- Secure and verify
- Automation

" WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US. HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

Subject-Specific Security Policies

Subject-specific security policies typically address a limited area of risk related to a particular class of assets, type of technology, or business function

- E-Mail and Internet Usage Policies
- Antivirus Policy
- Remote Access Policy
- Information Classification Policy
- Encryption Policies
- Document Format Policy

Components of a Security Policy

State the objective

Draft the policy specifics

Identify methods for measurement and enforcement

Compliance with policy expectations

Communication

Periodic review

Standards and Guidelines

- **Standard**
  - A formal, documented requirement that sets uniform criteria for a specific technology, configuration, nomenclature, or method

- **Guidelines**
  - Recommended practices to be followed to achieve a desired result
  - Not mandatory

Procedures

Procedures are step-by-step instructions for performing a specific task or set of tasks

Ensure consistent and repeatable results

Provide instruction to those who are unfamiliar with how to perform a specific process

Provide assurance to management and auditors that policies are being enforced in practice


IT ALERTS US IF ANYONE ACCIDENTALLY TRIES TO SEND CONFIDENTIAL DATA TO A PRIVATE EMAIL ADDRESS.
SLANE CO. NZ
SLANE CARTOONS

Release Management Policy

The conditions that must be met for an application or component to be released to production

Roles and responsibilities for packaging, approving, moving, and testing code releases

Approval and documentation requirements

Release Management

- Controls the release of applications, updates, and patches to the production environment
- Goal:
  - To provide assurance that only tested and approved application code is promoted to production or distributed for use

Release Manager

Responsible for planning, coordination, implementation, and communication of all application releases

Assures that all documentation and communication regarding the release are prepared and distributed

Release Management Process

- The release management process actually begins with the QA testing environment
- Once user acceptance testing is complete, the application is packaged for deployment to the production or preproduction environment and the final package is verified

Release Management Tools

- Role-based access control
- Approval checking and rejection of unapproved packages
- Component verification tools
- Rollback and demotion facilities
- Auditing and reporting tools

Configuration Management (CM)

Manage configuration changes so that they are appropriately approved and documented, so that:

- The integrity of the security state is maintained
- Disruptions to performance and availability are minimized

CM System Goals

Baseline hardware, software, and firmware configurations

Design, installation, and operational documentation

Changes to the system since the last baseline

Software test plans and results

Automated Configuration Management Tools

Most development platforms include:

- Source code comparators
- Comment generators
- Version checkers
- Check in/check out functions

Hardware Inventory

Make	Model	MAC addresses	Serial number
Operating system or firmware version	Location	BIOS and other hardware-related passwords	Assigned IP address if applicable
	Organizational property management label	Owner	

Software Inventory

Software name

Software vendor

Keys or activation codes

Type of license and for what version

Number of licenses

Software Inventory

License expiration

License portability

Organizational software librarian or asset manager

Organizational contact for installed software

Upgrade, full or limited license

Configuration Lists

A configuration list for each device should be maintained

Devices such as firewalls, routers, and switches can have hundreds or thousands of configuration possibilities

Configuration Management for Operating Systems

- Operating systems and applications also require configuration management
- Organizations should have configuration guides and standards for each operating system and application implementation

Control

Control mechanisms govern:

- Change requests
- Approvals
- Change propagation
- Impact analysis
- Bug tracking
- Propagation of changes

Auditing

Auditing is a process of logging, reviewing, and validating the state of CIs in the CMDB, ensuring that:

- All changes are appropriately documented
- A clear history of changes is retained
- Compares CMDB with the actual system configuration


MikeKeefeINTOON.com 04-11-14
MY PATCHES NEED PATCHES!
RIP
RIP RIP
CYBER SECURITY BLANKET
HACKERS
TEAR

Security Impact Assessment

The analysis conducted by qualified staff within an organization to determine the extent to which changes to the information system affect the security posture of the system

System Architecture/ Interoperability of Systems

- **Interoperability:**
  - The extent to which systems and devices can exchange data and interpret that shared data

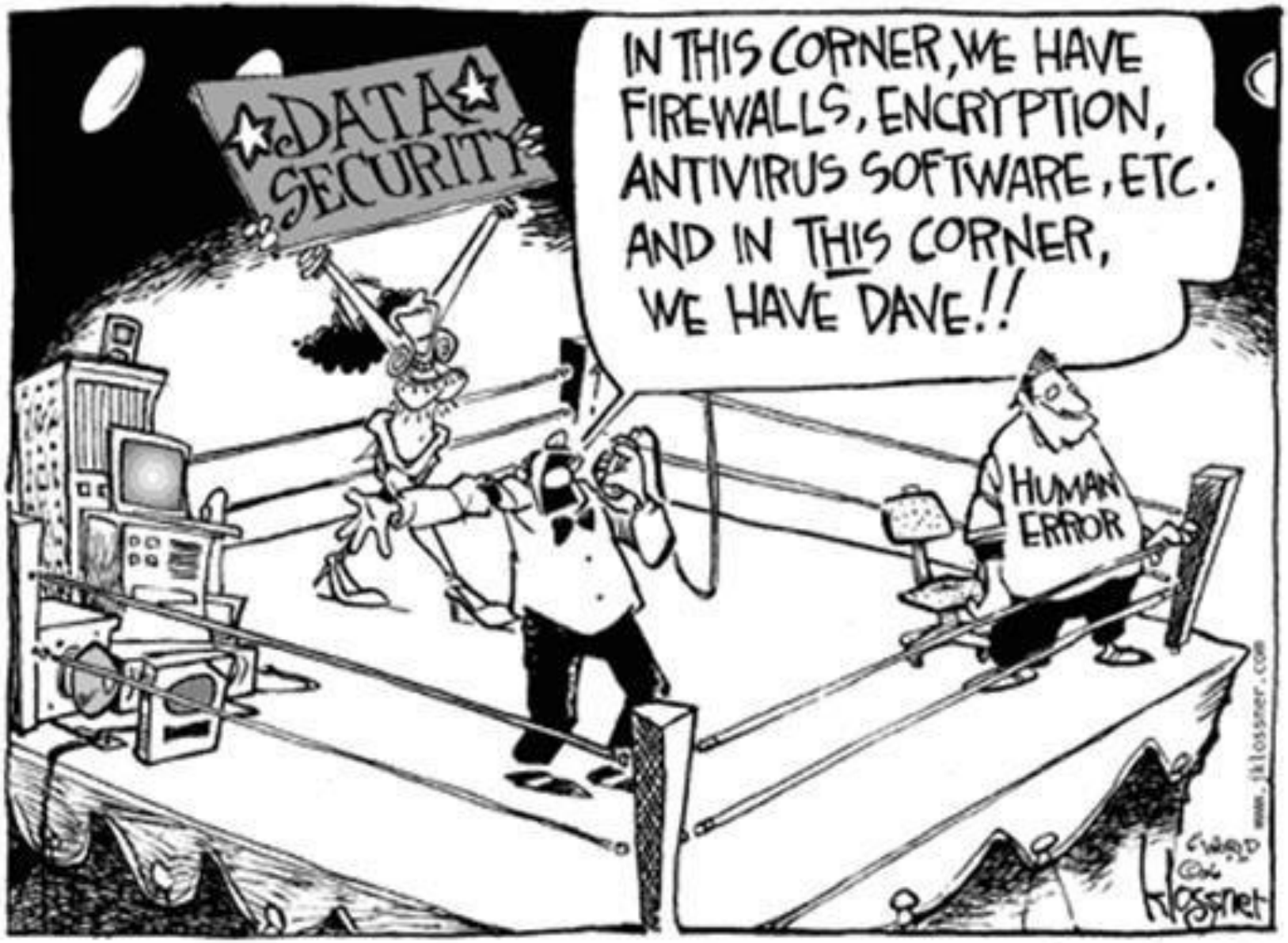
- **For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that a user can understand it**

Patch Management Process

- Acquisition
- Testing
- Approval
- Packaging
- Deployment
- Verification

Security Awareness Training

Security awareness seeks to reduce the risk related to human error


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Critical Success Factors

Senior management support

Cultural awareness

Set communication goals and build a strategy to meet these goals

Taking a change management approach

Measurement

Potential Training Topics

Labeling and handling of sensitive information

Appropriate use policies for e-mail, Internet, and other services

Customer privacy laws, policies, and procedures

Detecting and reporting security incidents

Protecting intellectual property and copyright