CHAPTER 10

Implementing Information Security

Projects, Governance, Certifications & Careers

Principles of Information Security

Whitman & Mattord — 6th Edition

Topic	Edition	Chapter
Implementation	6th (2018)	10 of 12

LEARNING OBJECTIVES

- Understand the IS implementation process and the role of the CISO and security team
- Describe the information security project management process and SDLC integration
- Explain security governance structures: committees, roles, and reporting relationships
- Understand security policy implementation: development, dissemination, and compliance
- Describe security education, training, and awareness (SETA) program design
- Identify key information security professional certifications and their focus areas
- Understand the information security profession: roles, career paths, and ethics
- Apply security metrics and performance measurement to security programs

10.1 Introduction to Implementing Information Security

Translating plans into action

Planning for information security — developing policies, frameworks, and risk assessments — is only the beginning. Chapter 10 focuses on the challenging process of actually implementing an information security program: organizing the security function, managing security projects, building governance structures, and developing the people and culture that make security work in practice.

Information Security Implementation	The process of translating information security plans, policies, and frameworks into operational security controls, programs, and organizational structures that protect the organization's information assets.

KEY INSIGHT

The most common reason security programs fail is not technical — it is organizational. Poor governance, lack of executive support, inadequate funding, insufficient trained staff, and failure to integrate security into business processes are the primary causes of security program failure.

10.1.1 The Role of the CISO

Chief Information Security Officer (CISO)	The senior executive responsible for the organization's information security program. The CISO develops security strategy, manages the security team, reports security posture to the board and executives, and ensures security is integrated into all business processes.

CISO responsibilities include:

- **Strategic planning:** Develop and maintain the information security strategic plan aligned with organizational objectives
- **Policy development:** Oversee creation and maintenance of all information security policies
- **Risk management:** Lead the risk management program; report risk posture to executives and board
- **Compliance:** Ensure compliance with applicable laws, regulations, and standards (HIPAA, PCI DSS, SOX, GDPR)
- **Incident response:** Lead or oversee response to security incidents; coordinate with law enforcement when necessary
- **Security awareness:** Champion the SETA (Security Education, Training, and Awareness) program
- **Vendor management:** Oversee security requirements in vendor contracts and third-party risk management

10.1.2 Information Security Organizational Structures

Where the security function sits in the organizational hierarchy significantly impacts its effectiveness and independence:

Structure	CISO Reports To	Advantages	Disadvantages
Reports to CIO	Chief Information Officer	Close alignment with IT operations; efficient resource sharing	Potential conflict of interest: IT availability vs. security
Reports to CEO	Chief Executive Officer	High visibility; strong mandate; independence from IT	CISO must compete with other senior leaders for attention
Reports to CFO	Chief Financial Officer	Financial oversight integration; risk-cost focus	May prioritize financial over operational security concerns
Reports to Board	Board of Directors (or Audit Committee)	Maximum independence; strongest governance	Distance from operations; may lack technical context
Reports to CLO	Chief Legal Officer	Strong compliance and legal integration	May prioritize regulatory over operational security

BEST PRACTICE

The CISO should report to the CEO or directly to the Board (or Audit Committee) to ensure independence from IT operations and maximum authority. When the CISO reports to the CIO, there is an inherent conflict of interest: IT leadership prioritizes availability and functionality, while security must sometimes restrict both.

10.2 Security Project Management

Managing security as a project and program

Information security initiatives are best managed as formal projects using established project management methodologies. Security projects have unique characteristics: they often involve sensitive information, require specialized expertise, and may face significant organizational resistance.

10.2.1 Project Management Fundamentals

Project	A temporary endeavor undertaken to create a unique product, service, or result. Security projects are temporary (defined start and end) and unique (not routine operations). Examples: implementing a new SIEM, deploying encryption, conducting a risk assessment.
Program	A group of related projects managed in a coordinated way to obtain benefits not available from managing them individually. The information security program encompasses all security-related projects and ongoing operations.

Project management triple constraint (Iron Triangle):

- Scope: What the project will deliver
- Time: When the project will be completed
- Cost: How much the project will cost
- Quality (fourth constraint in modern PM): The standard to which deliverables must meet

TRIPLE CONSTRAINT

Changes to one constraint affect the others. Increasing scope typically increases time and cost. Compressing the timeline requires additional cost (resources) or reduced scope. Security projects often struggle with scope creep when security requirements are discovered after project initiation.

10.2.2 Security Project Management Process

Phase	Key Activities	Security-Specific Considerations
Initiating	Define project charter; identify stakeholders; gain executive sponsorship	Classify project sensitivity; identify security requirements; assess regulatory constraints
Planning	Develop project management plan; define scope, schedule, budget, and risks	Threat modeling; security architecture design; compliance mapping; resource security vetting
Executing	Implement planned activities; manage project team; procure resources	Secure development practices; security testing integration; vendor security compliance
Monitoring & Controlling	Track progress; manage changes; report status	Security metrics tracking; vulnerability scanning; compliance monitoring; risk reassessment
Closing	Finalize deliverables; obtain acceptance; document lessons learned	Security handoff procedures; documentation archival; post-implementation security review

10.2.3 Security and the SDLC

Systems Development Life Cycle (SDLC)	A structured process for planning, creating, testing, and deploying an information system. Security must be integrated into every phase of the SDLC rather than added at the end. "Security by design" (or "shift left") is significantly more cost-effective than retrofitting security.

SDLC Phase	Security Activities
Planning/Initiation	Define security requirements; preliminary risk assessment; regulatory compliance check
Analysis/Requirements	Identify security functional requirements; threat modeling; privacy impact assessment
Design	Security architecture design; authentication/authorization design; cryptography selection
Development/Acquisition	Secure coding practices; code review; third-party component vetting; SAST (static analysis)
Testing	Security testing: SAST, DAST, penetration testing; vulnerability assessment; compliance testing
Implementation	Secure configuration; hardening; change management; security acceptance testing
Operations/Maintenance	Continuous monitoring; patch management; incident response; periodic security reviews
Disposal	Secure data destruction; decommissioning procedures; license management

EXAM TIP

Integrating security into the SDLC early (during design) is MUCH LESS expensive than finding vulnerabilities in production. The "1-10-100 rule": fixing a defect costs 1x in design, 10x in development, and 100x after release. Security must be a design requirement, not an afterthought.

10.3 Information Security Governance

Structures, committees, and oversight

Information Security Governance	The system by which an organization directs and controls information security. It specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while resources are used responsibly. Governance answers: Who makes security decisions? How are they made? How is performance measured?

10.3.1 Governance Structures

Governance Body	Composition	Role
Board of Directors	Board members; typically audit committee oversight	Set risk appetite; approve security policy; provide executive accountability
Executive Security Committee	C-suite executives (CEO, CFO, CIO, CLO, CISO)	Strategic direction; resource allocation; major security decision authority
IS Steering Committee	Senior managers from key business units + CISO	Coordinate security across business units; prioritize security initiatives
Security Working Groups	Technical staff; subject matter experts	Develop standards; implement controls; address specific technical domains
CISO / Security Team	Security professionals reporting to CISO	Day-to-day security operations; policy development; monitoring; incident response

10.3.2 Security Roles and Responsibilities

Role	Primary Responsibilities
Chief Information Security Officer (CISO)	Leads security program; develops strategy; reports to executives; owns security policy
Security Manager	Day-to-day security operations management; team supervision; policy implementation
Security Analyst	Monitor systems for threats; investigate incidents; conduct vulnerability assessments
Security Architect	Design secure systems and infrastructure; develop security standards
Security Engineer	Implement and maintain technical security controls and tools
Penetration Tester (Red Team)	Conduct authorized ethical hacking to identify vulnerabilities before attackers
Incident Responder	Investigate and contain security incidents; conduct forensic analysis
Compliance Analyst	Monitor regulatory compliance; prepare audit evidence; manage compliance frameworks
Data Owner	Business executive responsible for data classification and protection decisions
Data Custodian	IT staff responsible for implementing data protection as directed by data owner
System/Application Owner	Responsible for specific systems; accepts residual risk; approves security controls
End User	Follows security policies; reports incidents; completes security awareness training

10.4 Security Policy Implementation

From policy to practice

Security policies are the cornerstone of the security program, but a policy that is not known, understood, and enforced provides no protection. Implementing security policy requires a structured approach to development, dissemination, training, and enforcement.

10.4.1 Policy Development Process

Step	Activity	Key Considerations
1. Identify Need	Identify the business requirement or risk driving the policy need	Regulatory requirements; incident lessons learned; risk assessment findings
2. Research	Research applicable laws, regulations, standards, and industry practices	Legal review; benchmark against similar organizations; review existing policies
3. Draft	Draft the policy document with clear, actionable language	Avoid technical jargon; ensure alignment with higher-level policies; define scope
4. Review	Circulate for review by legal, HR, IT, business units, and end users	Legal enforceability review; technical feasibility; operational impact assessment
5. Approve	Obtain formal approval from appropriate executive authority	Authority level must match policy scope; document approval date and approver

Step	Activity	Key Considerations
6. Dissemi nate	Distribute through appropriate channels; ensure access by all affected parties	Email; intranet; policy management system; new employee onboarding
7. Implem ent	Configure systems, train staff, update processes to comply with policy	Technical enforcement where possible; training for behavioral policies
8. Enforce	Consistently apply consequences for policy violations	Uniform enforcement is a legal enforceability requirement (see Ch. 4)
9. Review	Annually or after triggering events; update as needed	Regulatory changes; organizational changes; incident findings

10.4.2 Policy Compliance Monitoring

Policies without compliance monitoring are ineffective. Key compliance monitoring mechanisms:

- **Technical enforcement:** Configure systems to enforce policy automatically (e.g., minimum password length enforced by the system — most reliable)
- **Automated scanning:** Vulnerability scanners and configuration management tools that check for policy compliance
- **Security audits:** Periodic audits by internal audit or external auditors to verify policy compliance
- **Management reviews:** Regular security metrics reporting to management demonstrates compliance trends
- **Employee attestation:** Annual sign-off confirming employees have read and understood policies
- **Exception management:** Formal process for documenting and approving policy exceptions with compensating controls

10.5 Security Education, Training, and Awareness (SETA)

Building a security-aware workforce

SETA Program	A comprehensive program designed to improve organizational security through education, training, and awareness activities. The CISO owns the SETA program. Employee error and negligence are consistently ranked as the top sources of security incidents — SETA directly addresses this.

10.5.1 Three Components of SETA

Component	Purpose	Duration	Method	Assessment
Security Education	Develop deep understanding of security principles and their WHY. Produces security professionals and informed managers.	Long-term (months to years)	University degrees; professional certifications; seminars; reading	Essays; exams; certification s
Security Training	Develop specific job-relevant security SKILLS. Produces ability to perform specific security tasks.	Intermediate (days to weeks)	Hands-on labs; workshops; simulations; role-specific courses	Performanc e-based; practical exercises

Component	Purpose	Duration	Method	Assessment
Security Awareness	Create short-term exposure to security topics. Keeps security top-of-mind for all employees.	Short-term (ongoing)	Posters; newsletters; screensavers; phishing simulations; brief videos	Phishing test click rates; quiz scores

10.5.2 Designing an Effective Security Awareness Program

Key elements of an effective security awareness program:

- **Relevance:** Tailor content to the audience — different messages for executives, IT staff, and general users
- **Frequency:** Regular, brief touchpoints are more effective than annual all-day training sessions
- **Variety:** Mix media — videos, posters, newsletters, interactive quizzes, tabletop exercises
- **Phishing simulations:** Send simulated phishing emails; measure click rates; train those who fall for them
- **Management support:** Executive sponsorship and visible participation increases employee engagement
- **Measurement:** Track metrics: click rates, training completion rates, incident counts, quiz scores
- **Culture:** Aim to create a security culture where employees see themselves as the last line of defense

SETA EFFECTIVENESS

Phishing simulation programs that immediately train employees who click links are among the most cost-effective security controls available. Organizations that run regular phishing simulations see click rates drop from 30%+ to under 5% within 12 months of consistent training.

10.6 Information Security Professional Certifications

Industry credentials for security professionals

Professional certifications validate knowledge and skills in information security. They are important for career advancement, establishing credibility, and meeting regulatory requirements (some roles legally require certain certifications). Certifications are grouped by level (entry, intermediate, advanced) and domain focus.

10.6.1 Key Certifications Overview

Certification	Full Name	Issuer	Level	Focus Area
CISSP	Certified Information Systems Security Professional	(ISC)²	Advanced	Broad InfoSec management; 8 domains; 5 years experience required
CISM	Certified Information Security Manager	ISACA	Advanced	InfoSec management and governance; manager-level focus
CISA	Certified Information Systems Auditor	ISACA	Advanced	IS auditing, control, and assurance; audit focus
CRISC	Certified in Risk and Information Systems Control	ISACA	Advanced	IT risk management and controls
CGEIT	Certified in the Governance of Enterprise IT	ISACA	Advanced	IT governance; executive/board focus
CEH	Certified Ethical Hacker	EC-Council	Intermediate	Offensive security; ethical hacking methodology
OSCP	Offensive Security Certified Professional	Offensive Security	Advanced	Practical offensive security; hands-on penetration testing
Security+	CompTIA Security+	CompTIA	Entry/Mid	Broad security foundation; DoD 8570 baseline
Network+	CompTIA Network+	CompTIA	Entry	Network fundamentals; prerequisite for Security+
SSCP	Systems Security Certified Practitioner	(ISC)²	Entry/Mid	Technical security administration; 1 year experience
GSEC	GIAC Security Essentials	GIAC/SANS	Entry/Mid	Technical security fundamentals; hands-on focus
GPEN	GIAC Penetration Tester	GIAC/SANS	Intermediate	Penetration testing methodology
CAP	Certified Authorization Professional	(ISC)²	Mid	NIST RMF authorization process; government focus
FITSP	Federal IT Security Professional	FITSI	Mid	US federal government IT security

10.6.2 CISSP in Depth

The CISSP (Certified Information Systems Security Professional) is widely considered the gold-standard advanced InfoSec certification. The CISSP Common Body of Knowledge (CBK) is organized into 8 domains:

Domain	Topic Area
1. Security and Risk Management	Ethics; governance; compliance; risk management; BCP concepts
2. Asset Security	Asset classification; data lifecycle; data security controls; retention
3. Security Architecture and Engineering	Security models (Bell-LaPadula, Biba); cryptography; hardware security
4. Communication and Network Security	OSI/TCP-IP; network attacks; protocols; firewalls; VPNs
5. Identity and Access Management (IAM)	Authentication; access control models; federated identity; SSO
6. Security Assessment and Testing	Audit strategies; vulnerability assessment; penetration testing; log management
7. Security Operations	Incident management; forensics; BCP/DRP; physical security; monitoring
8. Software Development Security	SDLC security; secure coding; application security; DevSecOps

CISSP REQUIREMENTS

5 years of paid work experience in 2 or more CISSP domains (4 years with a relevant 4-year degree). Must pass the CAT (Computerized Adaptive Testing) exam — 100–150 questions, 3 hours. Must be endorsed by an (ISC)² member. Must agree to the (ISC)² Code of Ethics.

10.7 Ethics in Information Security

Professional responsibility and ethical frameworks

Ethics in information security encompasses the moral principles that guide the behavior of security professionals. Given the power and access that security professionals hold, ethical conduct is essential — both for protecting the organization and maintaining public trust.

10.7.1 The (ISC)² Code of Ethics

The (ISC)² Code of Ethics preamble commits members to safety of the commonwealth, duty to principals, and advancement of the profession. The four mandatory canons, in priority order:

Priority	Canon	Meaning
1st (Highest)	Protect society, the common good, necessary public trust and confidence, and the infrastructure	Security professionals' first duty is to society as a whole, not just to their employer
2nd	Act honorably, honestly, justly, responsibly, and legally	Maintain personal integrity in all professional activities
3rd	Provide diligent and competent service to principals	Serve clients and employers well; maintain expertise; disclose conflicts of interest
4th (Lowest)	Advance and protect the profession	Promote the security profession; mentor others; avoid discrediting the profession

CANON PRIORITY

The priority ordering is critical: society > personal integrity > client/employer > profession. If your employer asks you to do something that harms society (e.g., covering up a breach that harms customers), the code of ethics requires you to put society first — even if this conflicts with your employer's wishes.

10.7.2 Ethical Frameworks for Security Professionals

Framework	Description	Application to InfoSec
Ten Commandments of Computer Ethics	Published by the Computer Ethics Institute. Guidelines for ethical computer use.	Prohibits: unauthorized access, causing harm, snooping, creating malware, using computers to steal/lie
IAB Standards of Conduct	Internet Activities Board standards for acceptable Internet use.	Prohibits: unauthorized access; deliberate disruption; wasting resources; compromising privacy
ACM Code of Ethics	Association for Computing Machinery professional code.	Emphasizes: public interest; honesty; competence; privacy; intellectual property rights
RFC 1087	Ethics and the Internet — outlines unacceptable activities on the Internet.	Prohibits: unauthorized system access; disruption; theft of computing resources

10.8 Security Metrics and Performance Measurement

Demonstrating security program value and effectiveness

Security Metrics	Measurements that provide management with quantitative or qualitative data about the effectiveness of security controls and the state of the security program. The goal: make security visible and measurable to enable informed management decisions.

10.8.1 Types of Security Metrics

Metric Type	Examples	Audience
Operational Metrics	Number of unpatched critical vulnerabilities; mean time to patch; open firewall rule count	CISO; Security Manager; IT staff
Incident Metrics	Number of incidents per month; mean time to detect (MTTD); mean time to respond (MTTR); incidents by type	CISO; executives; board
Risk Metrics	Number of high-risk findings; risk score trends; CARs (Corrective Action Requests) open vs. closed	CISO; executives; risk committee
Compliance Metrics	Percentage of systems compliant with baseline; audit findings; open control deficiencies	Compliance; audit; legal; board
Awareness Metrics	SETA training completion rates; phishing simulation click rates; security quiz scores	CISO; HR; executives
Program Metrics	Security budget as % of IT budget; FTE per security function; certification levels of staff	CISO; CFO; executives

10.8.2 Key Performance Indicators (KPIs) vs. Key Risk Indicators (KRIs)

Key Performance Indicator (KPI)	A measurable value demonstrating how effectively the security program is achieving key objectives. KPIs look backward at what has been accomplished. Example: "90% of critical vulnerabilities patched within 30 days of disclosure."

Key Risk Indicator (KRI)	A metric providing early warning that a risk is increasing or that risk thresholds may be exceeded. KRIs look forward at increasing risk exposure. Example: "Number of unpatched critical vulnerabilities older than 30 days exceeds 10 — threshold breach."

METRICS

Security metrics must be: (1) Meaningful — tied to business objectives, (2) Measurable — objectively quantifiable, (3) Actionable — management can respond to them, (4) Consistent — measured the same way over time for trend analysis. Avoid "vanity metrics" that look impressive but don't enable better decisions.

BEST PRACTICE

10.9 Change Management and Configuration Management

Controlling changes to maintain security

Change Management	The formal process for controlling modifications to hardware, software, firmware, documentation, and processes to ensure security, availability, and compliance are not inadvertently compromised by unauthorized or poorly controlled changes.

10.9.1 Change Management Process

Step	Activity
1. Request	Formal change request submitted describing the proposed change, rationale, and affected systems
2. Review	Change Advisory Board (CAB) reviews the change for security, operational, and compliance impact
3. Approve/Reject	Authorized approver (or CAB) approves, rejects, or requests modification of the change
4. Schedule	Approved change scheduled for a maintenance window; stakeholders notified
5. Test	Change tested in a non-production environment before deployment to production
6. Implement	Change implemented in production; security controls verified post-implementation
7. Document	All changes documented: what changed, who approved, when implemented, result
8. Review	Post-implementation review to verify change achieved objectives without adverse effects

Configuration Management (CM)	The process of maintaining systems in a known, secure state by tracking and controlling changes to hardware, software, and configuration settings. A Configuration Management Database (CMDB) records the configuration of all managed assets.

Baseline Configuration	A documented set of specifications for an information system that has been formally reviewed and agreed upon and serves as a basis for future work. Security baselines define the minimum secure configuration for systems (e.g., CIS Benchmarks, DISA STIGs).

10.10 Chapter Summary & Exam Review

Key concepts, roles, and review questions

Key Terms Summary

CISO	Chief Information Security Officer: leads security program, strategy, and governance
IS Governance	System directing/controlling InfoSec: who decides, how, and how performance is measured
IS Steering Committee	Senior managers + CISO coordinating security across business units
Project	Temporary endeavor with defined start/end to create a unique deliverable
Program	Group of related projects managed together to achieve benefits impossible individually
SDLC Security	Integrate security into every SDLC phase; fixing security in design costs 1x vs. 100x in production
SETA	Security Education, Training, and Awareness: addresses the #1 threat — human error
Security Education	Long-term; develops WHY understanding; degrees, certifications
Security Training	Intermediate; develops specific SKILLS; labs, workshops, simulations
Security Awareness	Short-term; ongoing exposure; posters, phishing simulations, newsletters
CISSP	Advanced $(ISC)^2$ certification; 8 domains; 5 years experience; gold standard for senior practitioners
CISM	ISACA management certification; information security management and governance focus
CISA	ISACA audit certification; information systems auditing, control, and assurance
CEH	EC-Council offensive security certification; ethical hacking methodology

Security+	CompTIA entry/mid-level; broad foundation; DoD 8570 baseline requirement
(ISC)² Code of Ethics	4 canons in priority: Society > Integrity > Client/Employer > Profession
KPI	Key Performance Indicator: backward-looking measure of security program achievement
KRI	Key Risk Indicator: forward-looking early warning of increasing risk exposure
Change Management	Formal process controlling modifications to prevent inadvertent security degradation
Configuration Management	Maintaining systems in a known, secure state; CMDB tracks all asset configurations
Baseline Configuration	Minimum secure configuration specification (CIS Benchmarks, DISA STIGs)
Data Owner	Business executive responsible for data classification and protection decisions
Data Custodian	IT staff implementing data protection as directed by the data owner
Triple Constraint	Project management: Scope + Time + Cost are interdependent constraints

Review Questions

#	Question	Answer / Guidance
Q1	Who owns the SETA program and why?	The CISO owns the SETA program. Since human error is the leading cause of security incidents, improving employee security behavior is a core CISO responsibility.
Q2	What are the three components of SETA and how do they differ?	Education: long-term, develops WHY understanding (degrees, certs). Training: intermediate, develops specific SKILLS (labs, workshops). Awareness: short-term, ongoing exposure (posters, phishing simulations).
Q3	What is the correct priority order of the (ISC)² Code of Ethics canons?	1st: Protect society; 2nd: Act honorably; 3rd: Serve principals (clients/employers); 4th: Advance the profession. Society comes first, even before employer.
Q4	What is the difference between a KPI and a KRI?	KPI = backward-looking measure of program achievement. KRI = forward-looking early warning of increasing risk. Both are important for security program management.
Q5	Why should the CISO NOT report to the CIO?	Conflict of interest: IT leadership prioritizes availability and functionality, while security must sometimes restrict both. CISO should report to CEO, Board, or Audit Committee for independence.

#	Question	Answer / Guidance
Q6	What is the CISSP and what are its requirements?	CISSP: (ISC)² advanced certification covering 8 security domains. Requires 5 years paid experience in 2+ domains (4 years with degree), pass the CAT exam, be endorsed by an (ISC)² member, and agree to the Code of Ethics.
Q7	What is a baseline configuration and give two examples?	A formally approved minimum secure configuration for systems. Examples: CIS Benchmarks (Center for Internet Security) and DISA STIGs (Security Technical Implementation Guides for US government systems).
Q8	What is the cost implication of not integrating security into the SDLC?	Security flaws found in production cost ~100x more to fix than if found during design. This is the "1-10-100 rule." Security must be a design requirement, not an afterthought.

FINAL EXAM TIPS

CISO should report to CEO or Board — NOT CIO (conflict of interest: availability vs. security).
SETA: Education (WHY, long-term) → Training (SKILLS, intermediate) → Awareness (exposure, ongoing).
(ISC)² Code of Ethics canon priority: Society > Integrity > Client/Employer > Profession.
CISSP: 8 domains; 5 years experience; (ISC)²; gold standard senior security certification.
CISM: ISACA management focus. CISA: ISACA audit focus. CEH: EC-Council ethical hacking. Security+: CompTIA entry/mid.
KPI = backward-looking (achieved). KRI = forward-looking (risk increasing). Both needed for governance.
SDLC security: fixing flaws costs 1x (design) vs 10x (dev) vs 100x (production) — shift left.
Change management: Request → Review → Approve → Schedule → Test → Implement → Document → Review.
Data Owner = business executive (decides classification). Data Custodian = IT staff (implements controls).
Security metrics must be: Meaningful, Measurable, Actionable, and Consistent for trend analysis.