Module - 2
Outcomes:

- Cloud Computing: benefits and Issues related to information Security
- Standards available for InfoSec: Cobit, Cadbury, ISO 27001, OWASP, OSSTMM.
- An Overview, Certifiable Standards: How, What, When, Who.

Self-learning Topics: Cloud Threats, Impact of cloud computing on users, examples of cloud service providers: Amazon, Google, Microsoft, Salesforce etc.

Cloud Computing: Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote datacentre managed by a cloud services provider (or CSP). The CSP makes these resources available for a monthly subscription fee or bills them according to usage.

Types of cloud computing:

There are four main types of cloud computing: private clouds, public clouds, hybrid clouds, and multiclouds.

Benefits of cloud computing:

1) Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

2) Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3) Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

4) Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5) Mobility

Cloud computing allows us to easily access all cloud data via mobile.

6) IServices in the pay-per-use model

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

7) Unlimited storage capacity

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

8) Data security

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

Cloud security

- **Shared responsibility for security:** Generally, the cloud provider is responsible for securing cloud infrastructure and the customer is responsible for protecting its data within the cloud—but it's also important to clearly define data ownership between private and public third parties.

- **Data encryption:** Data should be encrypted while at rest, in transit, and in use. Customers need to maintain full control over security keys and hardware security module.

- **User identity and access management:** Customer and IT teams need full understanding of and visibility into network, device, application, and data access.

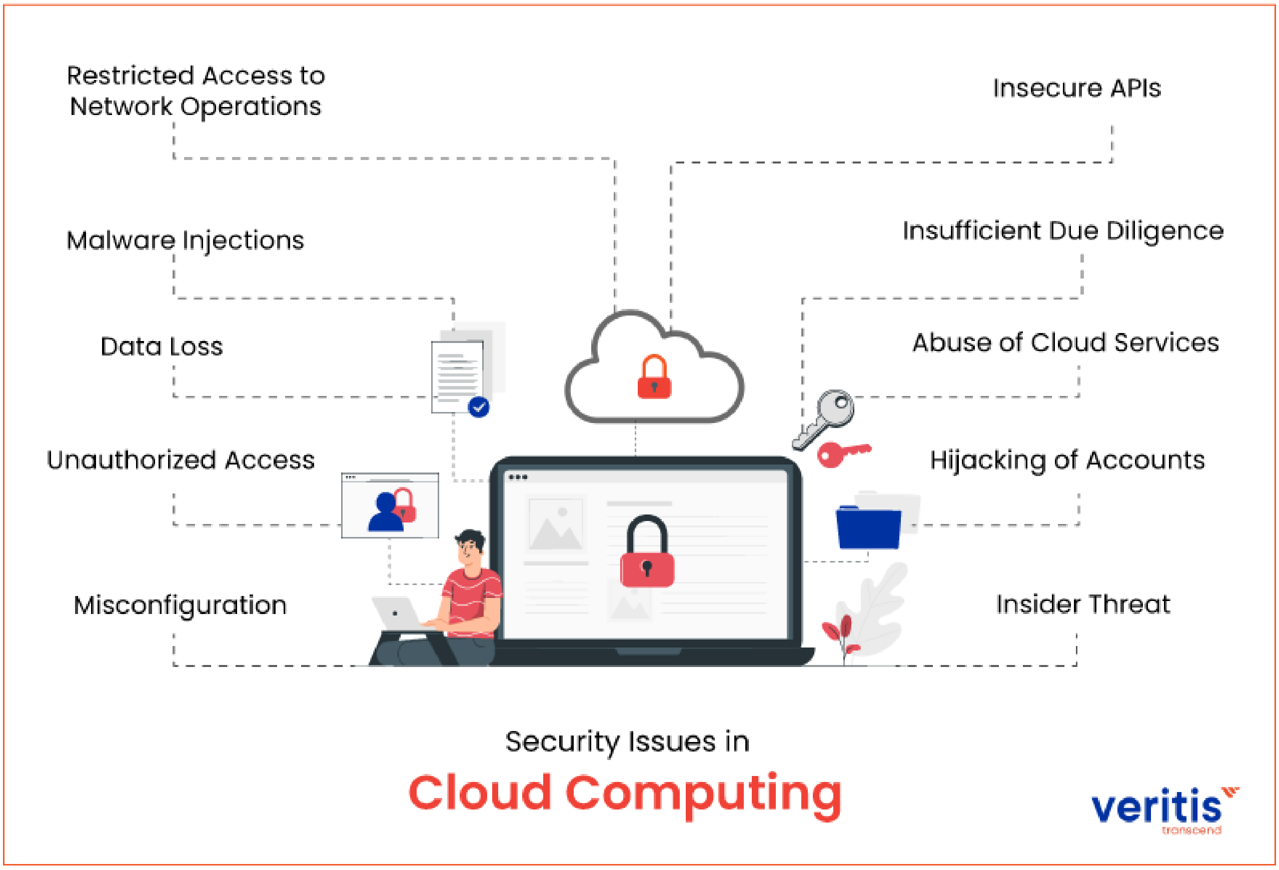
- **Collaborative management:** Proper communication and clear, understandable processes between IT, operations, and security teams will ensure seamless cloud integrations that are secure and sustainable.

- **Security and compliance monitoring:** This begins with understanding all regulatory compliance standards applicable to your industry and setting up active monitoring of all connected systems and cloud-based services to maintain visibility of all data exchanges between public, private, and hybrid cloud environments.

What are the benefits of cloud computing?

Cloud computing enables businesses to operate from virtually anywhere and with more efficiency. Some benefits of cloud computing include:

- **Cost savings:** One of the greatest benefits of cloud computing is reduced costs. Since businesses do not need to build their own IT infrastructure or purchase hardware or equipment, it helps companies reduce capital expenses significantly.
- **Flexibility/scalability:** Cloud computing offers greater flexibility to businesses of all sizes. Whether they require extra bandwidth, computing power or storage space, they can seamlessly scale up or down computing resources depending on their needs and budget.
- **Security:** Data security is a major concern for businesses today. Cloud vendors provide advanced security features like authentication, access management, data encryption, etc., to ensure sensitive data in the cloud is securely handled and stored.
- **Mobility:** Cloud computing allows users to access corporate data from any device, anywhere and at any time, using the internet. With information conveniently available, employees can remain productive even on the go.
- **Increased collaboration:** Cloud applications allow businesses to seamlessly communicate and securely access and share information, making collaboration simple and hassle-free. Cloud computing empowers multiple users to edit documents or work on files simultaneously and in a transparent manner.
- **Disaster recovery:** Data loss and downtime can cause irreparable damage to businesses of any size. Major cloud vendors are well-equipped to withstand unforeseen disruptive events, such as hardware/software failure, natural disasters and power outages, to ensure high application availability and business continuity.
- **Automatic updates:** Performing manual organization-wide software updates can take up a lot of valuable IT staff time. However, with cloud computing, service providers regularly refresh and update systems with the latest technology to provide businesses with up-to-date software versions, latest servers and upgraded processing power.



1. Misconfiguration

Incorrectly configured cloud security solutions settings frequently cause cloud data breaches.

2. Unauthorized Access

Cloud-based installations are outside the network perimeter and immediately reachable from the public Internet, in contrast to an organization’s on-premises infrastructure. However, this makes the infrastructure more accessible to users and customers. It also makes it simpler for attackers to access a company’s cloud-based services without authorization. An attacker may be able to get direct access without the organization’s knowledge if security is improperly configured or credentials are compromised.

3. Data Loss

In cloud computing, one of the problems is data loss. This is often referred to as a data leak. Insiders such as employees and business partners have access to sensitive data. Therefore, it’s feasible that hackers will gain access to our private information or sensitive data if the security of a cloud service is breached.

Enterprises using cloud computing security issues must cede part of their control to the CSP. Due to this, someone outside your IT department may oversee protecting some of the most critical data in your company. Your company will lose its data and intellectual property and be held liable for any ensuing damages if the cloud service provider is breached or attacked.

4. Malware Injections

Malware injections are scripts or pieces of code that are added to cloud services. And pose as "legitimate instances" while running as SaaS from cloud servers. This implies that malicious code can be introduced into cloud services and be perceived as a component of the program or service operating on the cloud servers themselves.

Attackers can eavesdrop, jeopardize the integrity of private data, and steal data once the malware injection has been completed. And the cloud has started working in conjunction with it. The East Carolina University Report on security threats on cloud computing vulnerabilities examines the risks of malware installations on cloud security breaches issue. And concludes that "malware injection assault has become a key security concern in cloud computing systems."

5. Restricted Access to Network Operations

Lack of visibility into network operations is a significant disadvantage of switching from an on-premises data storage architecture to a cloud based infrastructure. Businesses provide CSPs with varying degrees of control over their IT infrastructure in return for advantages like cost savings and easy scalability with on-demand storage provisioning. Another essential security concern associated with cloud computing security issues is the lack of visibility.

The kind of service model determines how much control CSPs have and what data security obligations enterprises have. However, the lack of insight into cloud environments poses an ongoing threat to the companies that depend on them for mission-critical data management, regardless of the shared responsibility model.

6. Insecure APIs

Application programming interfaces (API) allow customers to personalize their cloud experience.

However, the very nature of APIs may pose threaten cloud security issues. They authenticate, grant access, and implement encryption, enabling businesses to tailor the features of their cloud based infrastructure services to suit their business requirements.

Security threats increase when API infrastructure expands to offer better services. APIs give developers the tools to create their programs and integrate them with other mission-critical software. For example, developers can use YouTube as a well-known and straightforward example of an API to include YouTube in their websites or applications.

An API’s vulnerability is in the communication that occurs between apps. Even though this can benefit organizations and programmers, it leaves them vulnerable to security threats.

7. Insufficient Due Diligence

Most of the problems we’ve discussed thus far are technical. However, this particular security flaw arises when a company has a clear strategy for its objectives, resources, and cloud security solutions. It’s the people factor, to put it another way.

Additionally, rushing a multi cloud deployment migration without adequately planning for the possibility that the services will live up to consumer expectations might put a business at risk for security issues in cloud computing.

This is crucial for businesses that manage client financial data or whose data is subject to regulations like FERPA, PCI, PCI-DSS, and PII

8. Abuse of Cloud Services

Both small and enterprise-level firms may now readily hold enormous volumes of data thanks to the growth of cloud-based services. However, because of the cloud’s unheard-of storage capacity, malicious software, unauthorized software, and other digital goods. It can now be hosted and distributed by authorized users and hackers.

For instance, privileged users may violate the service provider’s terms by increasing security risks directly or indirectly.

9. Hijacking of Accounts

Account hijacking has become a whole new set of problems because of the expansion and adoption of the cloud in many enterprises.

Attackers can now remotely access sensitive data stored in the cloud using your (or your workers') login details. They can even change and falsify data using credentials that have been hijacked.

Other hijacking techniques allow attackers to quickly and frequently steal credentials without being noticed, such as scripting flaws and reused passwords. For instance, Amazon encountered a cross-site scripting flaw in April 2010 that targeted customer credentials. Threats from phishing, keylogging, and buffer overflow are all comparable. Tokens used by cloud services to validate individual devices without requiring logins with each update and sync are stolen in the most significant new threat, the Man in the Cloud Attack.

10. Insider Threat

Although an attack from within your company may seem implausible, the insider threat does occur. Employees with authorized access to a company's cloud-based services may misuse or gain access to sensitive data such as client accounts, financial forms, and other information.

What is COBIT?

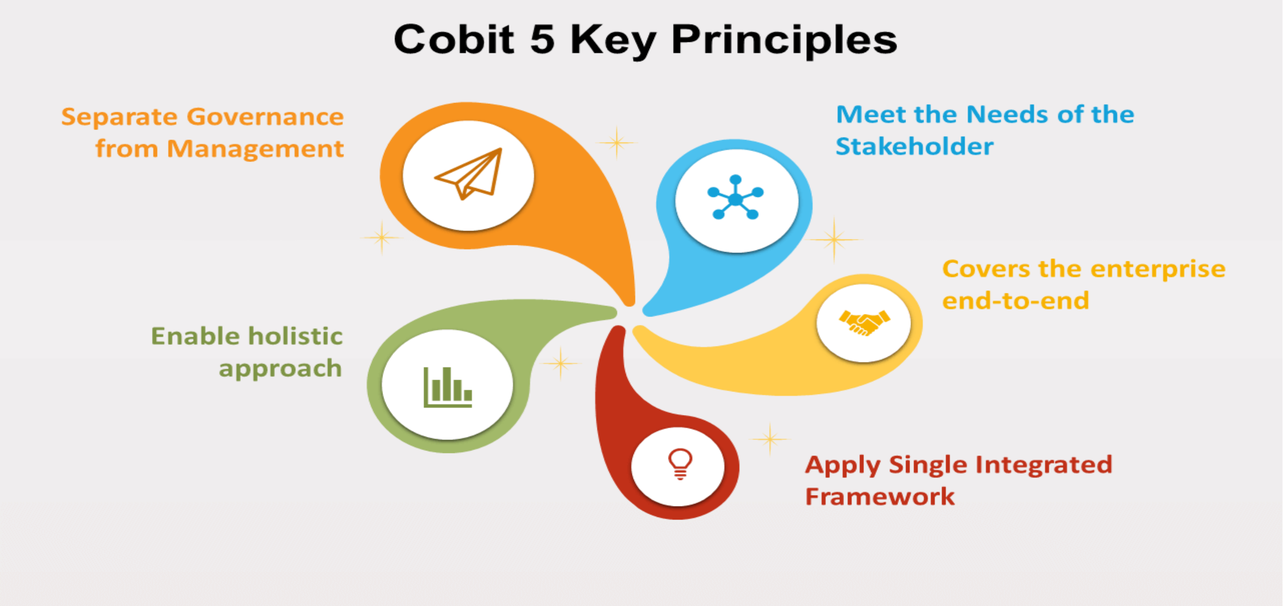
COBIT stands for Control Objectives for Information and Related Technology.

The COBIT business orientation includes linking business goals with its IT infrastructure by providing various maturity models and metrics that measure the achievement while identifying associated business responsibilities of IT processes.

- Planning & Organization
- Delivering and Support
- Acquiring & Implementation
- Monitoring & Evaluating

What is COBIT 5?

COBIT (Control Objectives for Information and Related Technology) helps organisations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organisational goals. COBIT 5, the latest iteration of the framework, was released in 2012.


Cobit 5 Key Principles
Separate Governance from Management
Meet the Needs of the Stakeholder
Covers the enterprise end-to-end
Enable holistic approach
Apply Single Integrated Framework

COBIT 5 principles

COBIT 5 is based on five principles that are essential for the effective management and governance of enterprise IT:

- Principle 1: Meeting stakeholder needs
- Principle 2: Covering the enterprise end to end
- Principle 3: Applying a single integrated framework
- Principle 4: Enabling a holistic approach
- Principle 5: Separating governance from management

These five principles enable an organisation to build a holistic framework for the governance and management of IT that is built on seven ‘enablers’:

1. People, policies and frameworks
2. Processes
3. Organisational structures
4. Culture, ethics and behaviour
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies

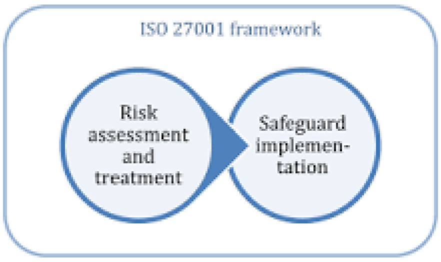
Benefits of COBIT

The COBIT 5 framework can help organisations of all sizes:

- Improve and maintain high-quality information to support business decisions.
- Use IT effectively to achieve business goals.
- Use technology to promote operational excellence.
- Ensure IT risk is managed effectively.
- Ensure organisations realise the value of their investments in IT; and
- Achieve compliance with laws, regulations and contractual agreements.

ISO 27001

What is the full form of ISO 27001 standard?



ISO 27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series. Its full name is “ISO/IEC 27001 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements.”

What is the ISO 27001 standards?

ISO/IEC 27001 is the international standard for information security. It sets out the specification for an effective ISMS (information security management system). ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes and technology.

What are the three principles of information security in ISO/IEC 27001, also known as the CIA triad?

1. **Confidentiality**
   → Meaning: Only the right people can access the information held by the organization.
   ⚠ Risk example: Criminals get hold of your clients’ login details and sell them on the Darknet.
2. **Information integrity**
   → Meaning: Data that the organization uses to pursue its business or keeps safe for others is reliably stored and not erased or damaged.
   ⚠ Risk example: A staff member accidentally deletes a row in a file during processing.
3. **Availability of data:**
   → Meaning: The organization and its clients can access the information whenever it is

necessary so that business purposes and customer expectations are satisfied.
⚠ Risk example: Your enterprise database goes offline because of server problems and insufficient backup.

An information security management system that meets the requirements of ISO/IEC 27001 preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

Why Should a Company Adopt ISO 27001? Is ISO 27001 Certification Worth It?

ISO 27001 is the only global standard that helps organizations to understand the various requirements of an information security management system (ISMS). The system is a combination of multiple policies, procedures, processes, and systems within an organization that works to manage information security risks.

ISO/IEC 27001 certification demonstrates that the organization followed the ISO 27001 guidelines and implemented the best-practice information security processes. Not all organizations decide to attain ISO 27001 certification, yet most use it as a framework to keep their information security management system secure from rising cyberattacks.

What Are the Domains of ISO 27001?

The current ISO 27001 standard has 14 domains

01 – Company security policy

02 – Asset management

03 – Physical and environmental security

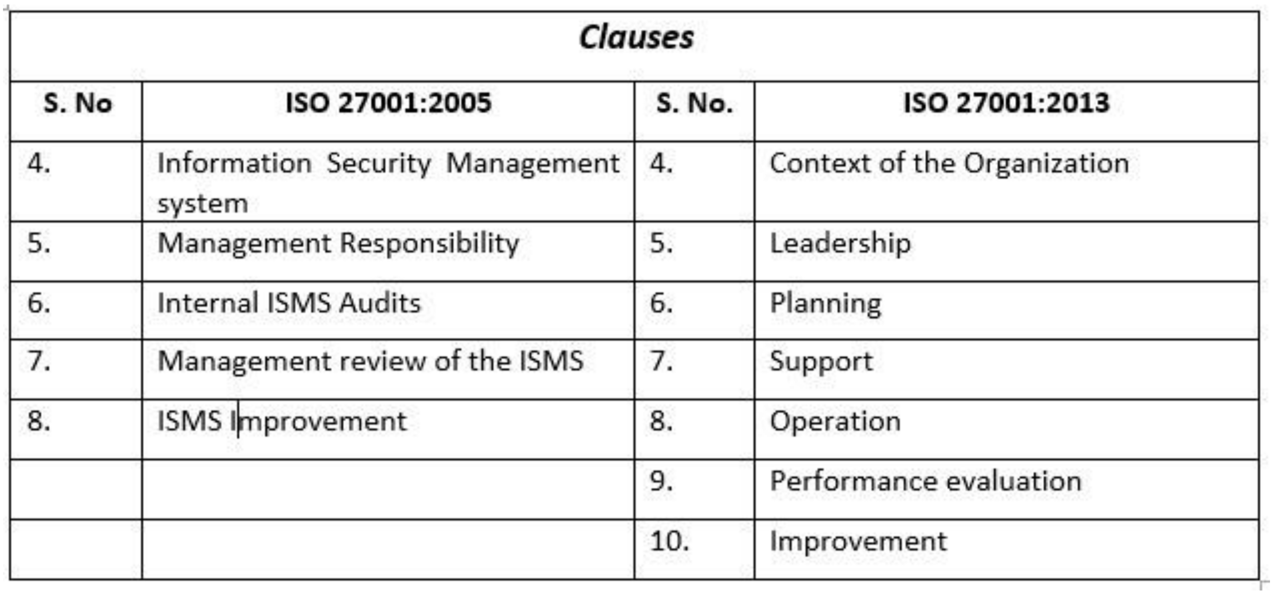
04 – Access control

05 – Incident management

06 – Regulatory compliance

The 14 domains of ISO 27001 are –

Information security policies	Organisation of information security
Human resource security	Asset management
Access control	Cryptography
Physical and environmental security	Operations security
Operations security	System acquisition, development and maintenance
Supplier relationships	Information security incident management
Information security aspects of business continuity management	Compliance



Clauses			
S. No	**ISO 27001:2005**	**S. No.**	**ISO 27001:2013**
4.	Information Security Management system	4.	Context of the Organization
5.	Management Responsibility	5.	Leadership
6.	Internal ISMS Audits	6.	Planning
7.	Management review of the ISMS	7.	Support
8.	ISMS Improvement	8.	Operation
		9.	Performance evaluation
		10.	Improvement

ISO 27001 benefits

- **Protect your data, wherever it is**

Protect all forms of information, whether digital, hard copy or in the Cloud.

- **Increase your attack resilience**

Increase your organisation’s resilience to cyber attacks

- **Reduce information security costs**

Implement only the security controls you need, helping you get the most out of your budget.

- **Respond to evolving security threats**

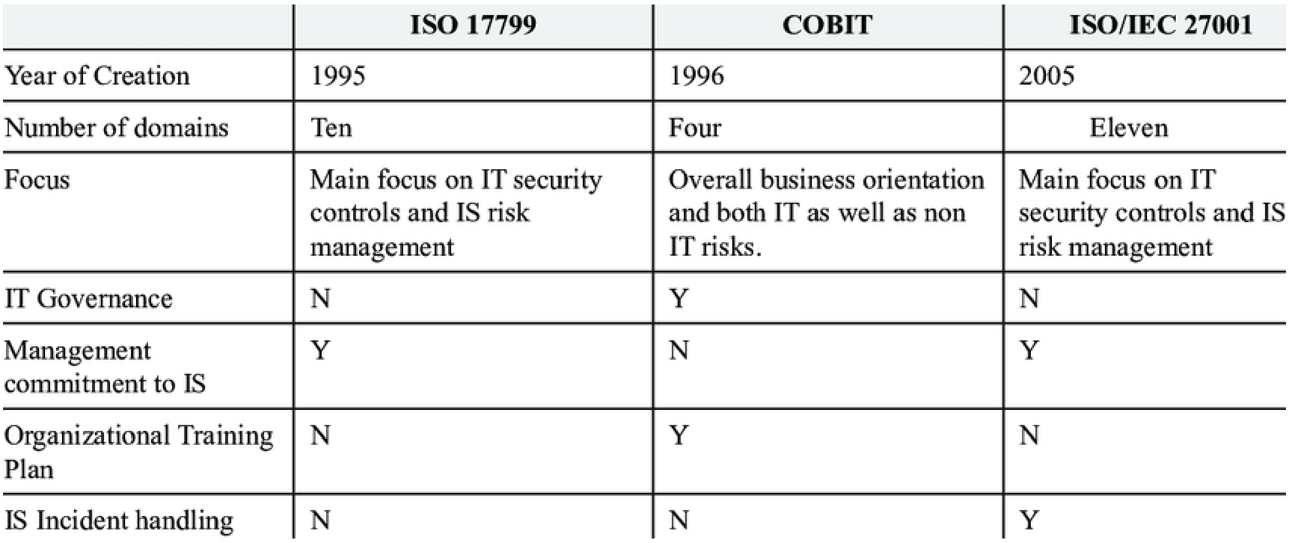
Constantly adapt to changes both in the environment and inside the organisation

- **Improve company culture**

An ISMS encompasses people, processes and technology, ensuring staff understand risks and embrace security as part of their everyday working practices.

- **Meet contractual obligations**

Certification demonstrates your organisation's commitment to data security and provides a valuable credential when tendering for new business.



	ISO 17799	COBIT	ISO/IEC 27001
Year of Creation	1995	1996	2005
Number of domains	Ten	Four	Eleven
Focus	Main focus on IT security controls and IS risk management	Overall business orientation and both IT as well as non IT risks.	Main focus on IT security controls and IS risk management
IT Governance	N	Y	N
Management commitment to IS	Y	N	Y
Organizational Training Plan	N	Y	N
IS Incident handling	N	N	Y

How to achieve ISO 27001 compliance

Implementing an ISMS involves:

- Scoping the project.
- Securing management commitment and adequate resources;
- Identifying interested parties and applicable legal and contractual requirements;
- Conducting a risk assessment;
- Selecting and implementing the required controls;
- Developing internal competence to manage the project;

- Developing the appropriate documentation;
- Conducting staff awareness training;
- Continually measuring, monitoring, reviewing and auditing the ISMS; and
- Implementing the necessary corrective and preventive actions.

OWASP

- **Definition.** The Open Web Application Security Project (OWASP) is a nonprofit foundation dedicated to improving software security.
- The primary purpose or core is to be the thriving global community that drives visibility and evolution in the safety and security of the world's software.

What are the OWASP Security Design Principles?

- Asset clarification
- Understanding attackers
- Core pillars of information security
- Security architecture

Security principles

1. Minimise attack surface area

2. Establish secure defaults

3. The principle of Least privilege

4. The principle of Defence in depth

5. Fail securely

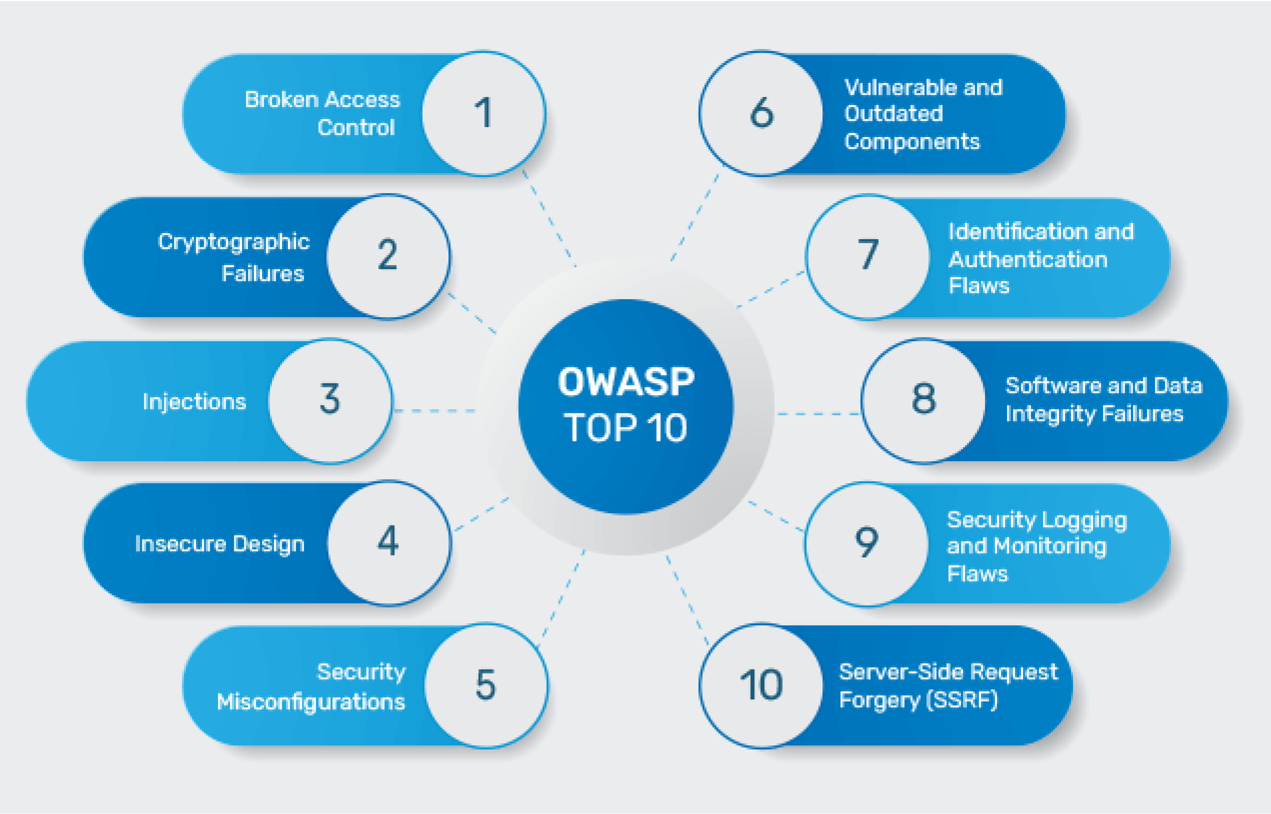
6. Don’t trust services

7. Separation of duties

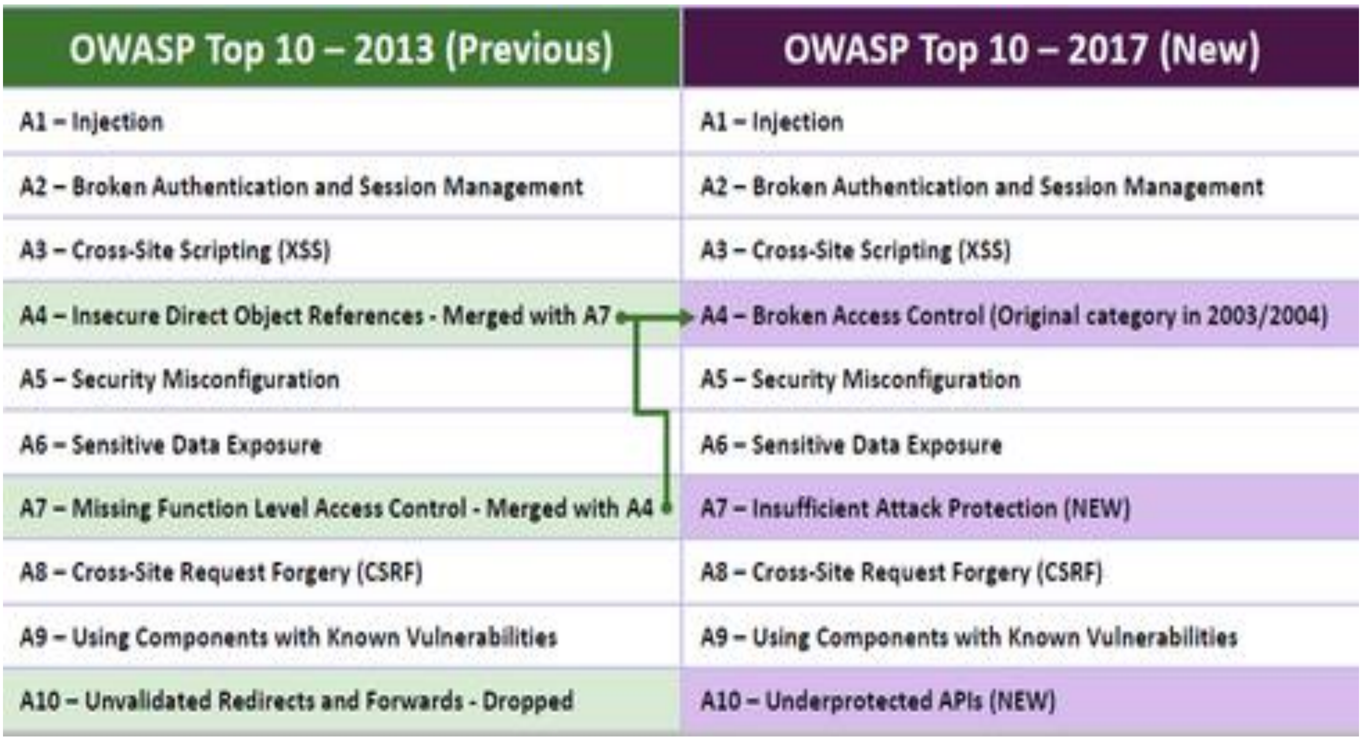
8. Avoid security by obscurity

9. Keep security simple

10. Fix security issues correctly


OWASP
TOP 10
1 Broken Access Control
2 Cryptographic Failures
3 Injections
4 Insecure Design
5 Security Misconfigurations
6 Vulnerable and Outdated Components
7 Identification and Authentication Flaws
8 Software and Data Integrity Failures
9 Security Logging and Monitoring Flaws
10 Server-Side Request Forgery (SSRF)

OWASP TOP 10



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

OSSTMM

The Open Source Security Testing Methodology Manual (OSSTMM) is peer-reviewed and maintained by the Institute for Security and Open Methodologies (ISECOM).

Who uses OSSTMM?

The OSSTMM is a great resource for any information security or IT team, as well as security professionals focused on penetration testing and red team engagements

The Open Source Security Testing Methodology Manual, or OSSTMM, is a peer-reviewed methodology for security testing, maintained by the Institute for Security and Open Methodologies (ISECOM).

The manual is updated every six months or so, to remain relevant to the current state of security testing. ISECOM says its main objective with the OSSTMM is to provide a scientific process for the accurate characterization of operation security that can be used for penetration testing, ethical hacking, and other security testing. ISECOM focuses on verified facts to make sure that organizations using the OSSTMM for their own penetration testing methodologies can know they are making fact-based decisions.

The OSSTMM is used by KirkpatrickPrice to develop our advanced penetration testing services. Our penetration tests are reliable, effective, and thorough because they are ever influenced by the best sources in the industry.

OSSTMM includes the following key sections:

- Operational Security Metrics.
- Trust Analysis.
- Work Flow.
- Human Security Testing.
- Physical Security Testing.
- Wireless Security Testing.
- Telecommunications Security Testing.
- Data Networks Security Testing.

1. **Human Security**: The security of human interaction and communication is evaluated operationally as a means of testing

2. **Physical Security**: The OSSTMM tests physical security defined as any tangible element of security that takes physical effort to operate
3. **Wireless Communications**: Electronic communications, signals, and emanations are all considered wireless communications that are part of the operational security testing
4. **Telecommunications:** Whether the telecommunication network is digital or analog, any communication conducted over telephone or network lines are tested in the OSSTMM
5. **Data Networks**: The security testing of data networks includes electronic systems and data networks that are used for communication or interaction via cable and wired network lines