

How to Use ISO27002:2013

- What is ISO27002:2013 ?
 - Information technology -- Security techniques -- Code of practice for information security controls
 - Renamed from ISO 17799

How to Use ISO27002:2013

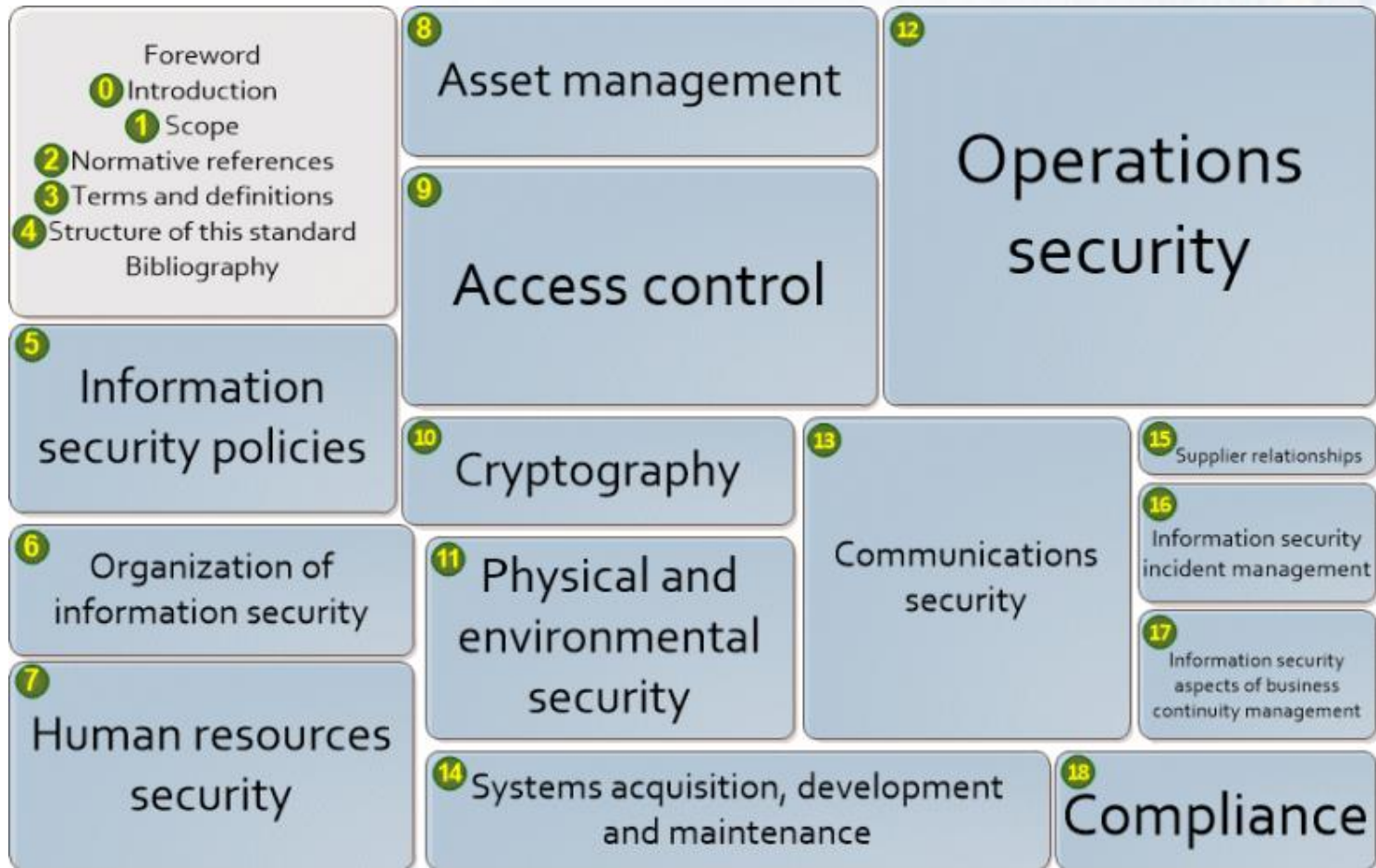
- 0.1 Background & Context
 - This Int'l Standard is designed for orgs to use as a **reference** for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001;

How to Use ISO27002:2013

- 0.1 Background & Context
 - or as a **guidance document** for organizations implementing commonly accepted information security controls.

How to Use ISO27002:2013

STRUCTURE OF ISO27002:2013



<http://www.iso27001security.com/html/27002.html>

How to Use ISO27002:2013

- Lets have a look at control A.5.1.2 (**Review Of The Policies Of Information Security**)

How to Use ISO27002:2013

ISO27001:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	<i>Control:</i> The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
---------	---	--

How to Use ISO27002:2013

ISO27002:2013

TITLE

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

CONTROL

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

27002 IMPLEMENTATION GUIDANCE

How to Use ISO27002:2013

ISO27002:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFOSEC	<i>27002: Implementation Guidance:</i> Each policy should have an owner who has approved mngmt responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the org's policies and approach to managing Infosec in response to changes to the org environment, business circumstances, legal conditions or tech environment.
---------	--	---

How to Use ISO27002:2013

- Practically:
 - ISO27001:2013 controls are brief and generic
 - 27002 clarifies further what is being referred to, gives further context & very useful implementation guidance

END

NIST FRAMEWORK

- The Computer Security Resource Center (CSRC) website guides users to NIST resources on **computer, cyber, and information security and privacy.**

NIST FRAMEWORK

- Its content includes **publications, projects, research, news and events** from the NIST Information Technology Laboratory's (ITL) two security divisions

NIST FRAMEWORK

[CONTACT](#) [SITE MAP](#)

Computer Security Division

Computer Security Resource Center

[CSRC Home](#) [About](#) [Projects / Research](#) [Publications](#) [News & Events](#)

Search

Fulltext search of NIST's computer security publications:

 [Advanced Search](#)

Browse Publications

NEW PUBLICATIONS

- SP 800-67 Rev. 2 (Draft)
- SP 800-190 (2nd Draft)
- NISTIR 8179 (Draft)
- SP 800-192
- SP 800-12 Rev. 1

CSRC HOME > PUBLICATIONS > NIST SPECIAL PUBLICATIONS

NIST SPECIAL PUBLICATIONS (SP)

NIST uses three NIST Special Publication subseries to publish computer/cyber/information security and guidelines, recommendations and reference materials:

- ***SP 800, Computer Security*** (December 1990-present):
NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the [NIST Library Catalog](#));
- ***SP 1800, NIST Cybersecurity Practice Guides*** (2015-present):
A new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; ***practical, user-friendly guides*** to facilitate adoption of standards-based approaches to cybersecurity;

NIST FRAMEWORK

- **SP 800, Computer Security** (December 1990-present):
NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the **NIST Library Catalog**);

NIST FRAMEWORK

PUBLICATIONS BY TOPIC/PROJECT

Browse FIPS, Special Publications, NISTIRs and ITL Bulletins *by topic or project*:

Security Concepts

- [General IT Security](#)
- [Audit & Accountability](#)
- [Authentication](#)
- [Awareness & Training](#)
- [Certification & Accreditation](#)
- [Contingency Planning](#)
- [Cryptography](#)
- [Digital Signatures](#)
- [Incident Response](#)
- [Maintenance](#)
- [Personal Identity Verification \(PIV\)](#)
- [Planning](#)
- [Privacy](#)
- [Public Key Infrastructure \(PKI\)](#)
- [Research](#)
- [Risk Assessment](#)
- [Security Automation](#)
- [Services & Acquisition](#)
- [Threats & Vulnerability Management](#)
- [Usability](#)

Technologies

- [Biometrics](#)
- [Cloud Computing & Virtualization](#)
- [Communications & Wireless](#)
- [Mobile](#)
- [Smart Cards](#)

Applications

- [Cyber-Physical Systems / Smart Grid](#)
- [Forensics](#)
- [Healthcare](#)
- [Internet of Things \(IoT\)](#)
- [Public Safety](#)
- [Supply Chain](#)
- [Voting](#)

Activities

- [Annual Reports](#)
- [Conferences & Workshops](#)

NIST FRAMEWORK

SP 800s - Computer Security

Number	Date	Title
SP 800-193 (Draft)	May 2017	DRAFT Platform Firmware Resiliency Guidelines ➤ Announcement and Draft Publication
SP 800-192	June 2017	Verification and Test Methods for Access Control Policies/Models 📄 SP 800-192 FAQ doi:10.6028/NIST.SP.800-192 [Direct Link]
SP 800-190 (Draft)	July 2017	DRAFT Application Container Security Guide (2nd Draft) ➤ Announcement and Draft Publication
SP 800-188 (Draft)	December 2016	DRAFT De-Identifying Government Datasets (2nd Draft) ➤ Announcement and Draft Publication
SP 800-187 (Draft)	November 2016	DRAFT Guide to LTE Security ➤ Announcement and Draft Publication
SP 800-185	December 2016	SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash 📄 SP 800-185 FAQ doi:10.6028/NIST.SP.800-185 [Direct Link] 📄 Comments Received on Draft SP 800-185
SP 800-184	December	Guide for Cybersecurity Event Recovery

NIST FRAMEWORK

This publication is available free of charge from <http://dx.doi.org/10.6028/NIST.SP.800-147B>

NIST Special Publication 800-147B

BIOS Protection Guidelines for Servers

Andrew Regenscheid

AUGUST 2014
32 PAGES DOC

<http://dx.doi.org/10.6028/NIST.SP.800-147B>

NIST FRAMEWORK

- NIST has a tremendous library of free documentation on a diverse range of topics
- **Relevance is often average, however, depth and detail of material is extraordinary**

END

PCI DSS V3

- PCI Data Security Standard (DSS): 
 - Designed to ensure that ALL companies that accept, process, store or transmit credit card info maintain a secure environment
 - Managed by Security Standards Council

<https://www.pcicomplianceguide.org/pci-faqs-2/>

PCI DSS V3

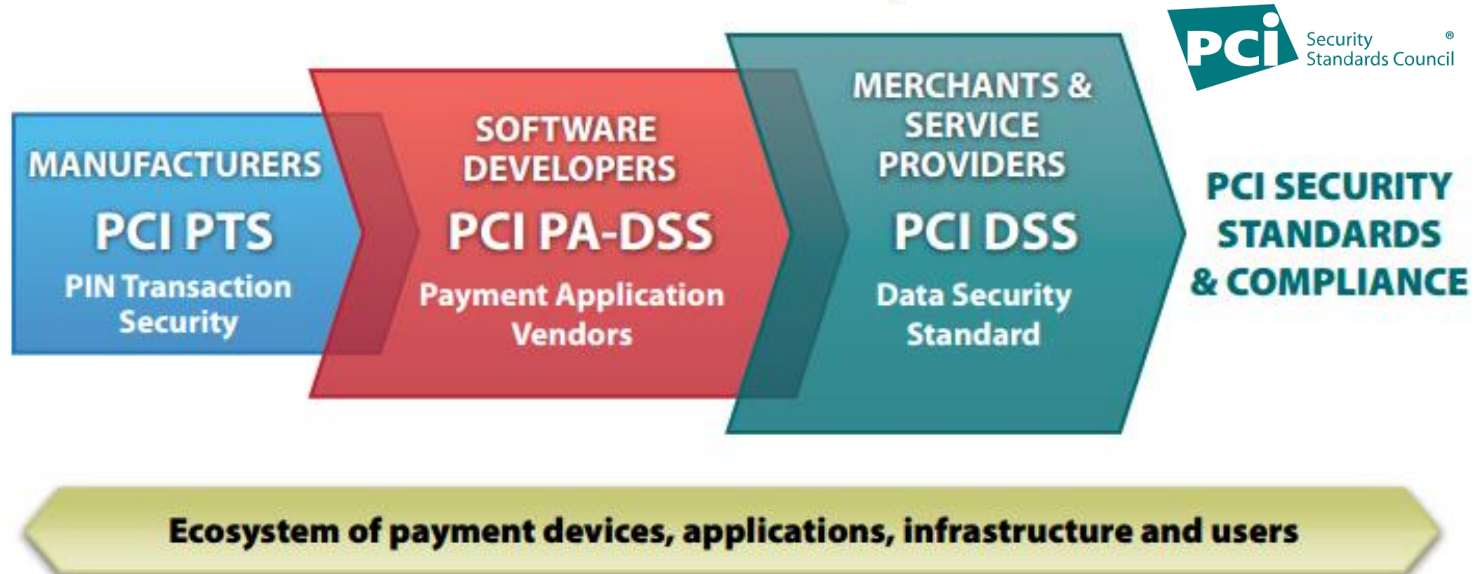
- PCI DSS: 
 - SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB)
 - 6 Broad goals and 12 requirements

REF: PCI Best Practices For Implementing Security Awareness;
<https://www.pcisecuritystandards.org/documents/>

PCI DSS V3

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

PCI DSS V3

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel



<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

REQUIREMENT

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	 Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

TESTING PROCEDURES

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

GUIDANCE

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
7.1.4 Require documented approval by authorized parties specifying required privileges.	7.1.4 Select a sample of user IDs & compare with documented approvals to verify that: -Documented approval exists for the assigned privileges -The approval was by authorized parties -That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
8.1.4 Remove/disable inactive user accounts within 90 days.	8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.

PCI DSS V3

- PCI is specific to the card environment to protect cardholder data
- PCI controls are very specific and in-depth compared to generic and high-level controls of ISO27001

END

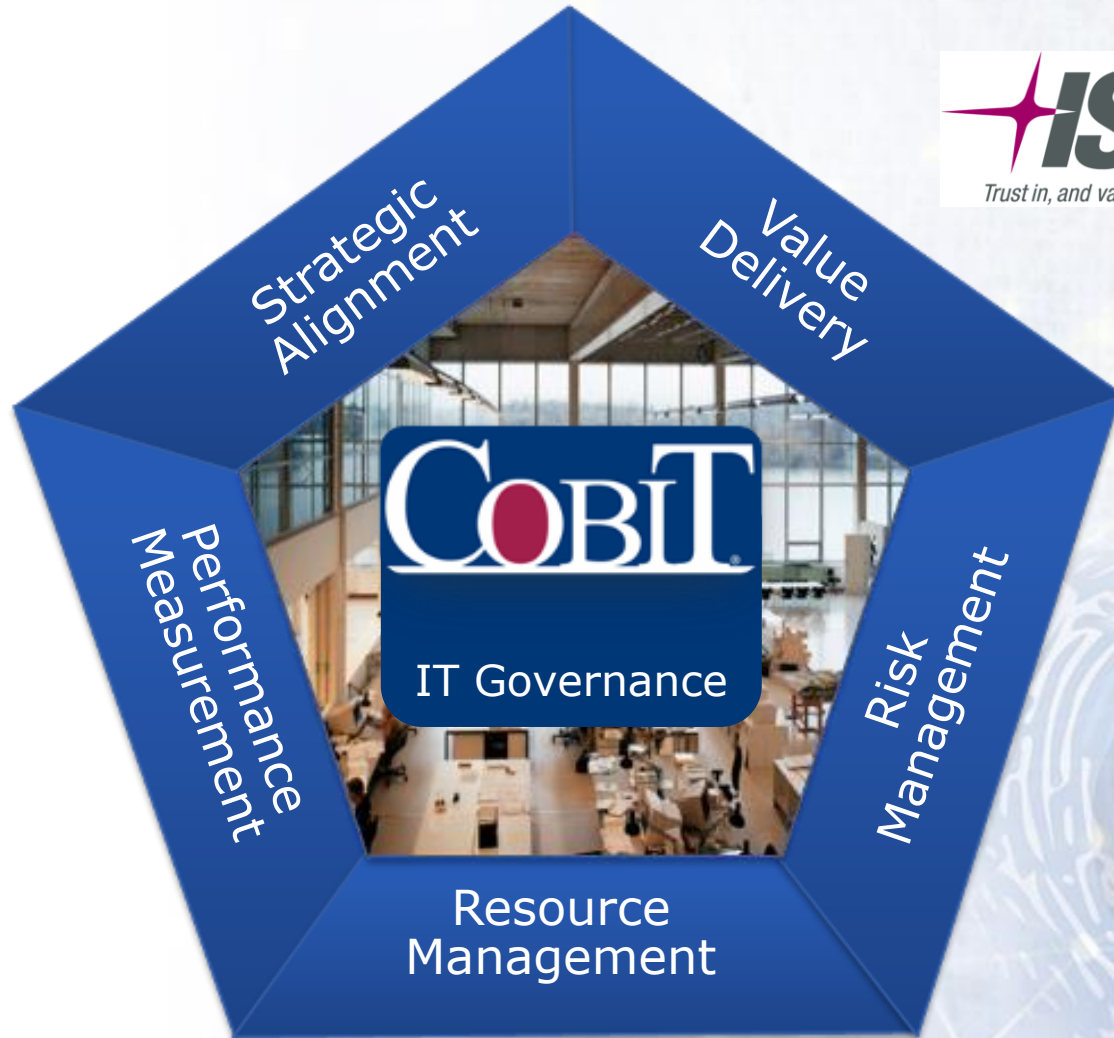
COBIT

- COBIT:



- ISACA framework for IT Governance
- COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)

COBIT

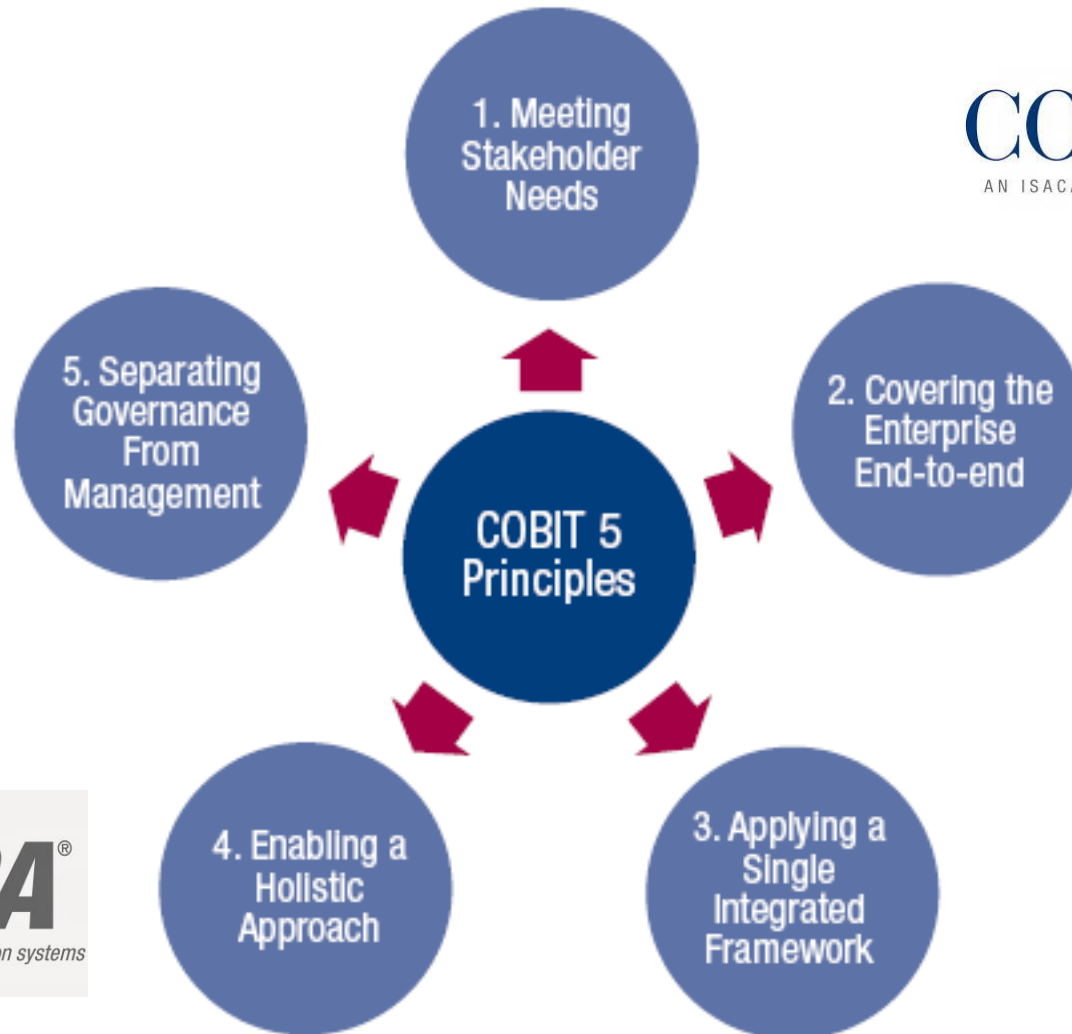


COBIT

- COBIT 5 brings together **five principles** that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of **seven enablers** that optimises IT investment and use for the benefit of stakeholders (ISACA)

COBIT

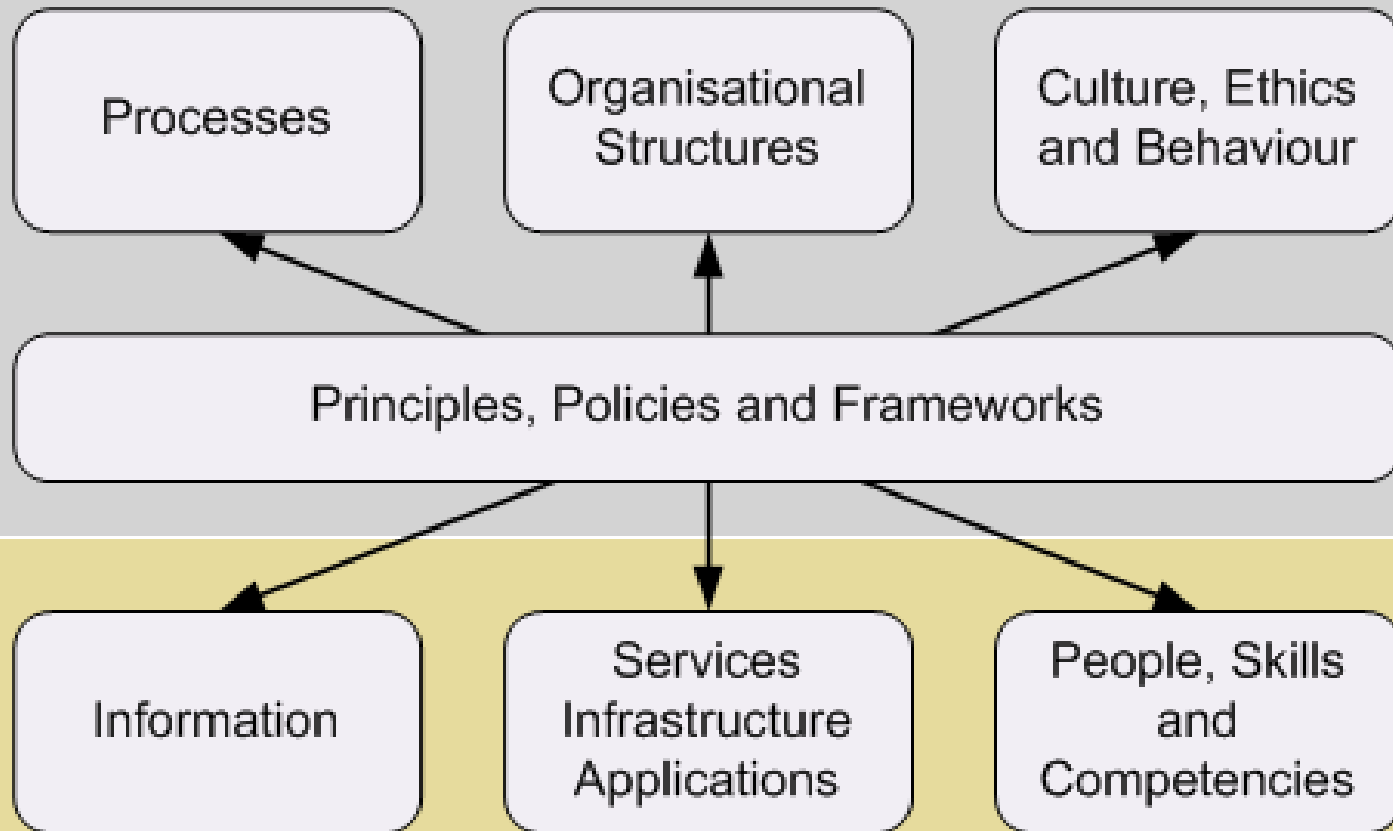
COBIT®
AN ISACA® FRAMEWORK



COBIT



COBIT 5 ENTERPRISE ENABLERS



COBIT

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions & options; setting **direction** through prioritisation & decision making;

COBIT

- ... & **monitoring** performance, compliance and progress against agreed direction and objectives (**EDM**)



COBIT

- **Management plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**)



COBIT



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Changes Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

COBIT

- COBIT 5 is a detailed framework for IT governance developed by ISACA which has principles, enablers, and processes
- These tools assist implementers and customer organizations to successfully deploy the framework
- Certifiable framework

END

MALWARE

MALICIOUS SOFTWARE

Malware

- Malicious software
- Rogue software
- Rogue
 - Large, destructive, anomalous or unpredictable
 - Operating outside normal or desirable controls

Malware

- Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.
- Researchers tend to classify malware into one or more sub-types (i.e. computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and keyloggers).
- Malware poses serious problems to individuals and businesses on the Internet.
- According to Symantec's 2018 Internet Security Threat Report (ISTR), malware variants number has increased to 669,947,865 in 2017, which is twice as many malware variants as in 2016.
- Cybercrime, which includes malware attacks as well as other crimes committed by computer, was predicted to cost the world economy \$6 trillion USD in 2021, and is increasing at a rate of 15% per year.
- Since 2021, malware has been designed to target computer systems that run **critical infrastructure** such as the electricity distribution network.
- The defense strategies against malware differ according to the type of malware but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems.
- Malware is now being designed to evade antivirus software detection algorithms.

Malware Types

- Virus
- Worm
- Trojan
- Logic bomb
- Time bomb
- Drive-by download
- Backdoor
- PUPs(Potentially Unwanted Program)
- Spyware
- Adware
- Scareware
- Ransomware
- FakeAV / Rogue security software
- Malvertising
- APT
- Fileless malware

Software versus Malware

- Writing a typical software
 - Software application (word processor, spreadsheet, graphics)
 - Higher-level programming language
 - Usually independent of OS
- Writing a virus
 - Detailed knowledge of OS

Computer Virus

- Biological virus
 - Latin → Poison
 - Shell filled with genetic material that it injects into a living cell, thereby infecting it
 - The cell then starts manufacturing copies of virus
- Computer virus behaves similarly
 - Injects its contents, a short computer program / instructions, into a host computer and infecting it
 - When the computer executes the virus code, it replicates the code, performs some task(s), usually of a malicious nature

- 
- A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs.
 - Computer viruses generally require a host program.
 - The virus writes its own code into the host program.
 - When the program runs, the written virus program is executed first, causing infection and damage.

- 
- By contrast, a computer worm does not need a host program, as it is an independent program or code chunk.
 - Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.

- 
- Any virus will by definition make unauthorised changes to a computer, which is undesirable even if no damage is done or intended.
 - The first page of Dr Solomon's Virus Encyclopaedia explains the undesirability of viruses, even those that do nothing but reproduce.

- The first academic work on the theory of self-replicating computer programs was done in 1949 by John von Neumann who gave lectures at the University of Illinois about the "Theory and Organization of Complicated Automata".
- The work of von Neumann was later published as the "Theory of self-reproducing automata".
- In his essay von Neumann described how a computer program could be designed to reproduce itself.
- Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical "father" of computer virology.

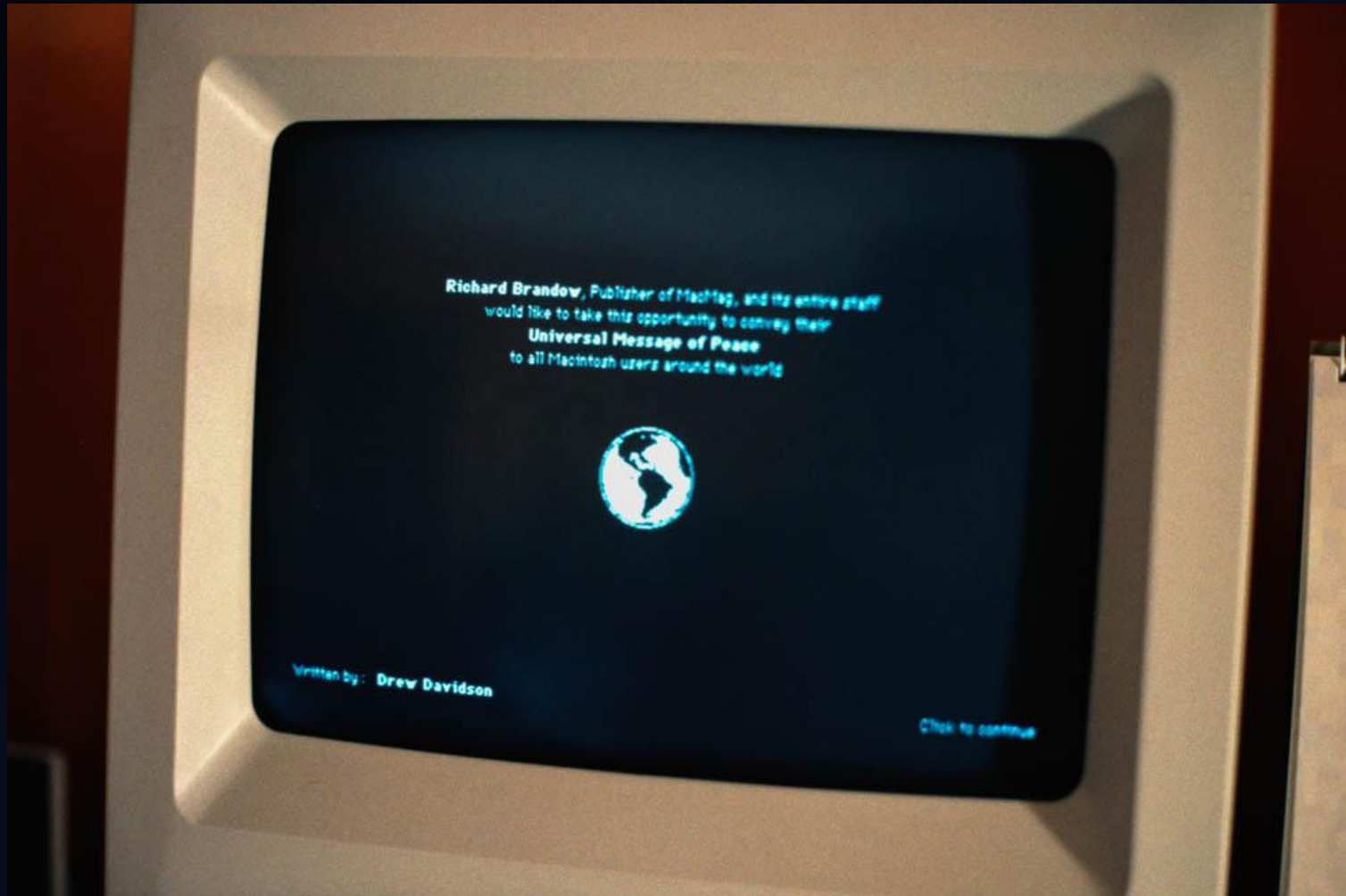
- In 1972, Veith Risak directly building on von Neumann's work on self-replication, published his article "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Self-reproducing automata with minimal information exchange).
- The article describes a fully functional virus written in assembler programming language for a SIEMENS 4004/35 computer system.
- In 1980 Jürgen Kraus wrote his diplom thesis "Selbstreproduktion bei Programmen" (Self-reproduction of programs) at the University of Dortmund.
- In his work Kraus postulated that computer programs can behave in a way similar to biological viruses.

Creeper / Reaper

- The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s.
- Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971.
- Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system.
- Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'M THE CREEPER. CATCH ME IF YOU CAN!" was displayed.
- The Reaper program was created to delete Creeper.

- 
- In 1984 Fred Cohen from the University of Southern California wrote his paper "Computer Viruses – Theory and Experiments".
 - It was the first paper to explicitly call a self-reproducing program a "virus", a term introduced by Cohen's mentor Leonard Adleman.

This is the MacMag virus 'Universal Peace' message,
as displayed on my Mac in March of 1988.



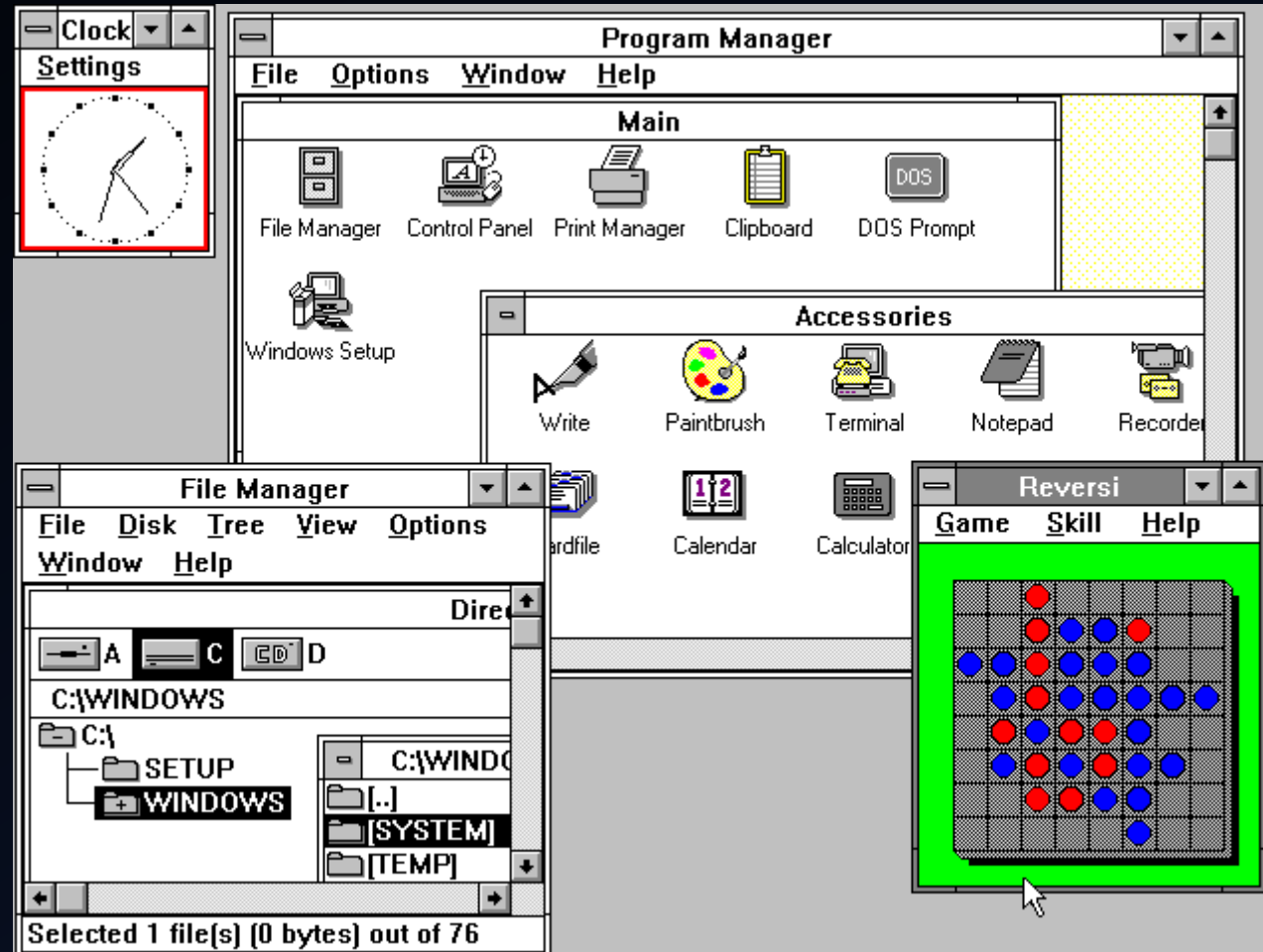
Brain virus

- 26 September 1988: front cover of Time magazine
- Title: “Invasion of the data snatchers”
- The first IBM PC compatible virus in the "wild" was a boot sector virus dubbed (c)Brain, created in 1986 and was released in 1987 by Amjad Farooq Alvi and Basit Farooq Alvi in Lahore, Pakistan, reportedly to deter unauthorized copying of the software they had written.

Hex dump of the Brain virus, generally regarded as the first computer virus for the IBM Personal Computer (IBM PC) and compatibles

Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20	-0J04↑●Π0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20	(c) 1986 Basit
0096(0060)	26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74	& Amjad (put) Lt
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	d.
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	BRAIN COMPUTER
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	SERVICES.. 730 NI
0160(00A8)	5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	ZAM BLOCK ALLAMA
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	.IQBAL TOWN
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	LAHDR
0208(00D0)	45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E	E-PAKISTAN..PHJN
0224(00E0)	45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B	E :430791,443248
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	,280530.

The first virus to specifically target Microsoft Windows, WinVir was discovered in April 1992, two years after the release of Windows 3.0.



Parts of a Virus

- A computer virus generally contains three parts:
 - the infection mechanism, which finds and infects new files
 - the payload, which is the malicious code to execute
 - the trigger, which determines when to activate the payload

Computer worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security failures on the target computer to access it.
- It will use this machine as a host to scan and infect other computers.
- When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.

Computer worm

- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on exploiting the advantages of exponential growth, thus controlling and infecting more and more computers in a short time.
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- Many worms are designed only to spread, and do not attempt to change the systems they pass through.
- However, as the **Morris worm** and **Mydoom** showed, even these "payload-free" worms can cause major disruption by increasing network traffic and other unintended effects.

Hex dump of the Blaster worm, showing a message left for Microsoft CEO Bill Gates by the worm's creator

```
0 00 00-6D 73 62 6C      msbl
0 6A 75-73 74 20 77      ast.exe I just w
9 20 4C-4F 56 45 20      ant to say LOVE
0 62 69-6C 6C 79 20      YOU SAN!! billy
0 64 6F-20 79 6F 75      gates why do you
3 20 70-6F 73 73 69      make this possi
0 20 6D-61 6B 69 6E      ble ? Stop makin
E 64 20-66 69 78 20      g money and fix
7 61 72-65 21 21 00      your software!!
0 00 00-7F 00 00 00      ♠♠♥♥      H      △
0 00 00-01 00 01 00      ð_ð_      ☺      ☺ ☺
0 00 00-00 00 00 46      á☺      L      F
C C9 11-9F E8 08 00      ♦lêèù~⌋⌋fþ☐
0 00 03-10 00 00 00      +▶H`☺      ♠♥▶
3 00 00-01 00 04 00      þ♥ ã      ð♥ ☺ ♦
```

Ransomware

- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.
- While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.
- It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Payment for private key



Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address

[REDACTED] and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

<< Back

Next >>



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Trojan horse

- In computing, a Trojan horse is any malware that misleads users of its true intent by disguising itself as a standard program.
- The term is derived from the ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

- 
- Once installed, Trojans may perform a range of malicious actions.
 - Many tend to contact one or more Command and Control (C2) servers across the Internet and await instruction.
 - Since individual Trojans typically use a specific set of ports for this communication, it can be relatively simple to detect them.



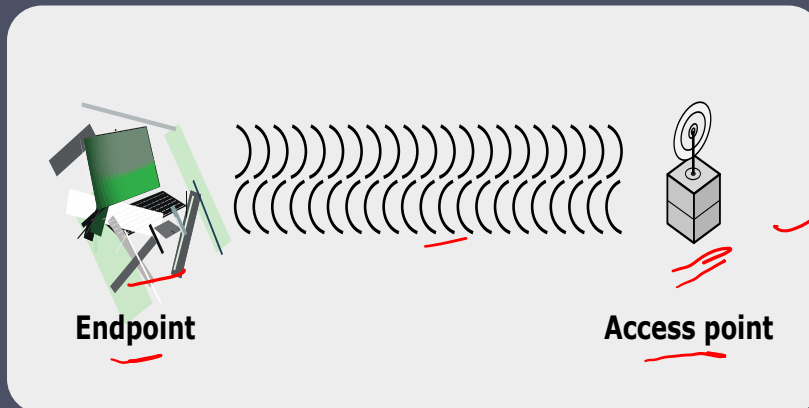
Wireless Network Security

Wireless Networking Components



Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
- **Channel**
 - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
 - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols
- **Mobility**
 - Wireless devices are far more portable and mobile, thus resulting in a number of risks
- **Limited Resources**
 - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware
- **Accessibility**
 - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks



IEEE 802.11 Standard

Wired and Wireless LANs

- LANs are designed for use in a **small area** (offices, campuses)
- IEEE has defined the specifications for a
 - wired LAN, called IEEE 802.3
 - wireless LAN, called IEEE 802.11,
- These specifications are concerning the physical and data link layers.

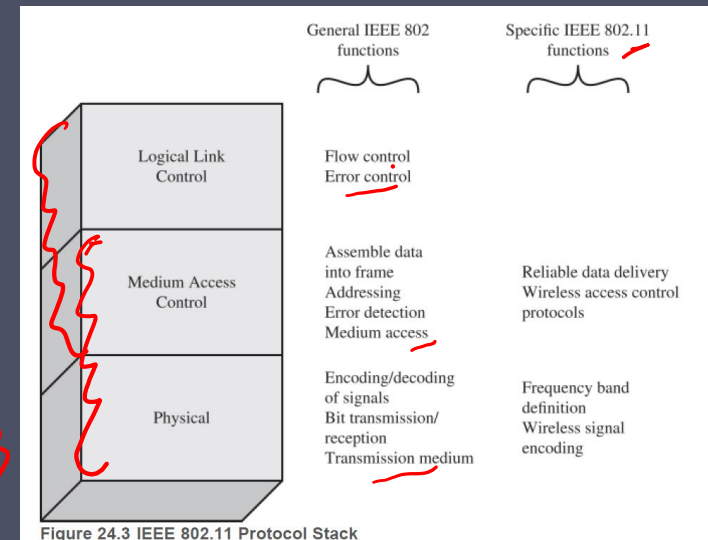
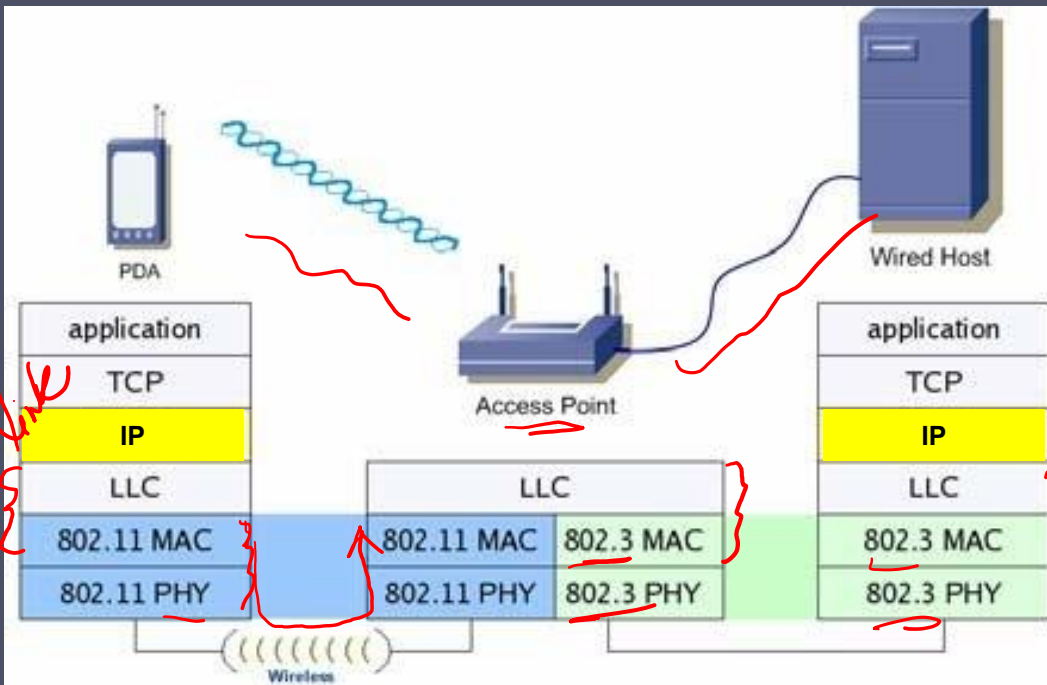


Figure 24.3 IEEE 802.11 Protocol Stack

Brief History of IEEE 802

- Since there are various types of computer system manufacturers, the IEEE's computer society started a project in 1985 called **Project 802** to enable standard communication between various devices.

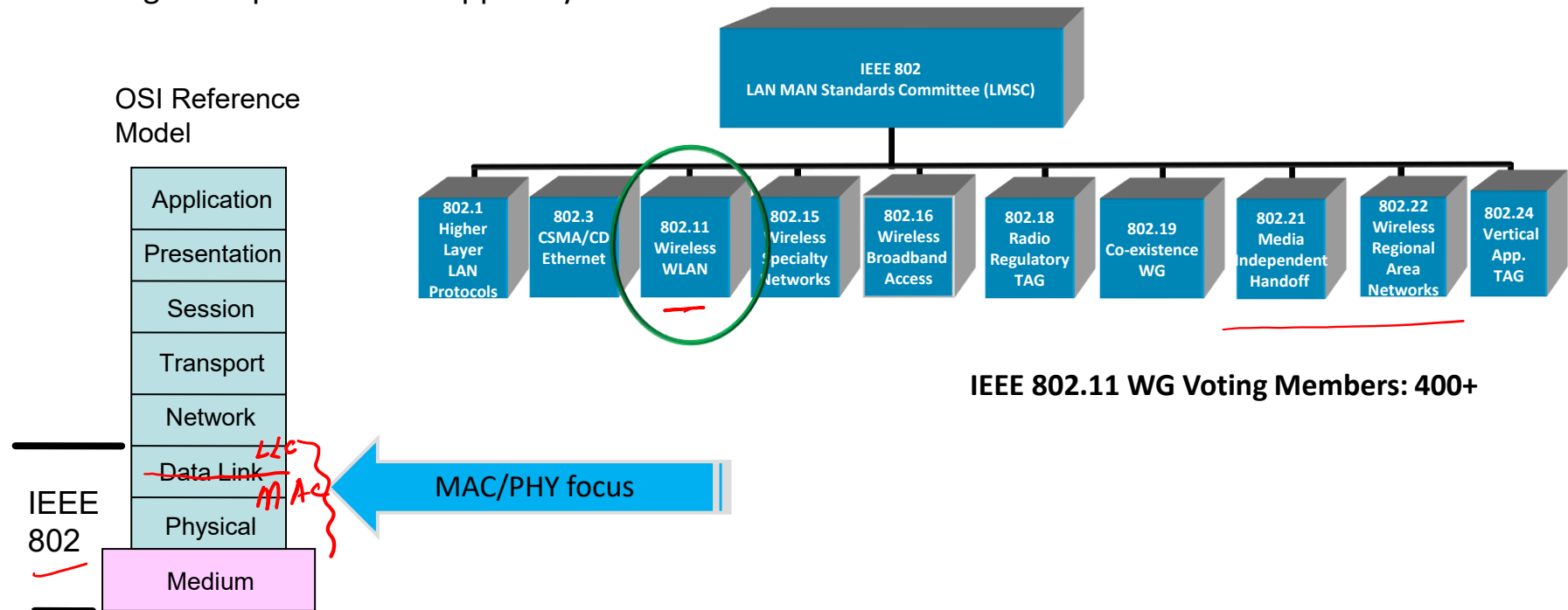


- The **IEEE 802 LAN/MAN Standards Committee (LMSC)** develops and maintains networking standards and recommended practices for **local, metropolitan, and other area networks**, using an open and accredited process, and advocates them on a global basis.

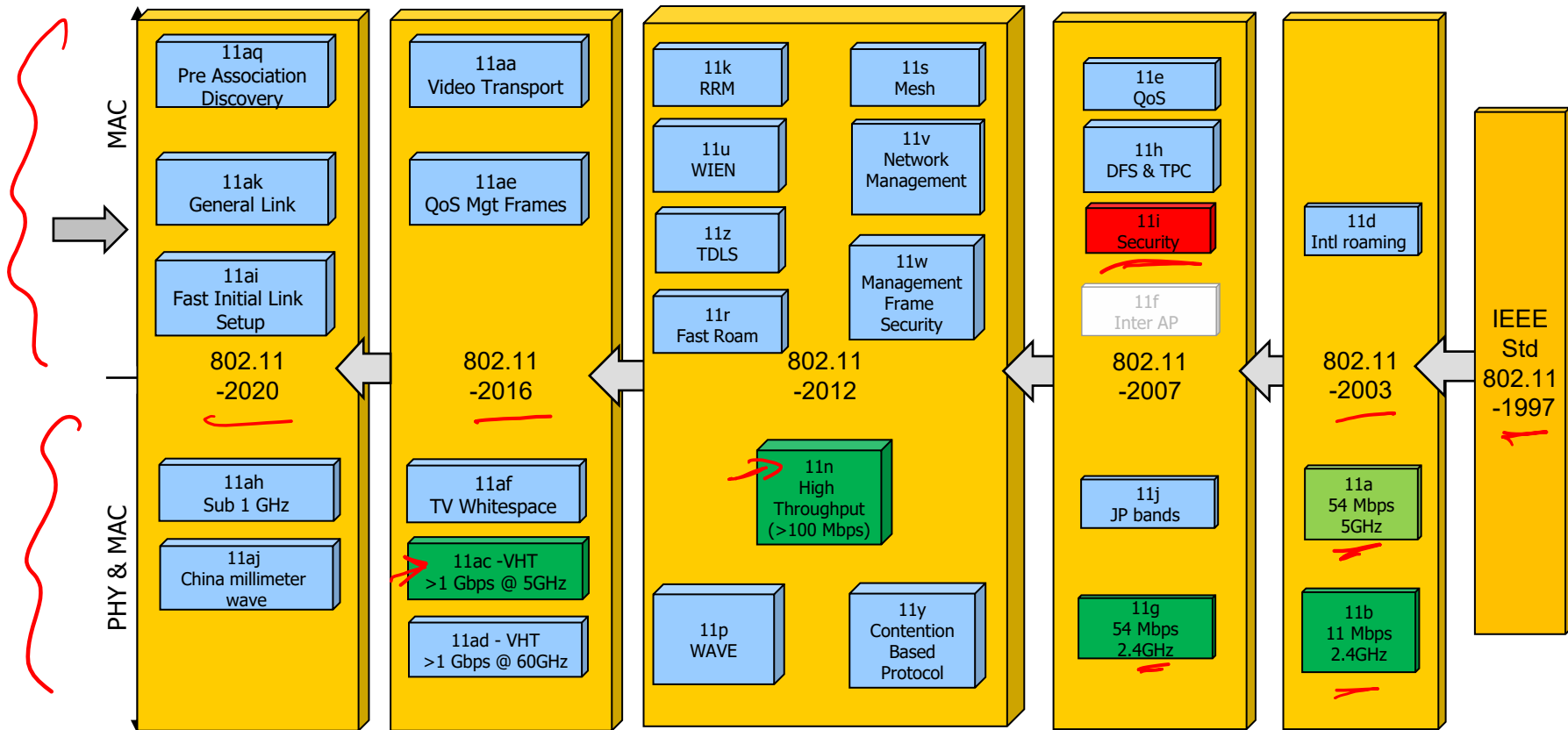
<https://www.ieee802.org/>

The IEEE 802.11 Working Group is one of the most active WGs in 802

- The 802.11 Working Group was established in 1990.
- Focus on **link and physical layers** of the network stack
- Leverage IETF protocols for upper layers



Development of the IEEE 802.11 Standard is ongoing since 1997



IEEE802.11 Wi-Fi standard evolution: 802.11be is under development

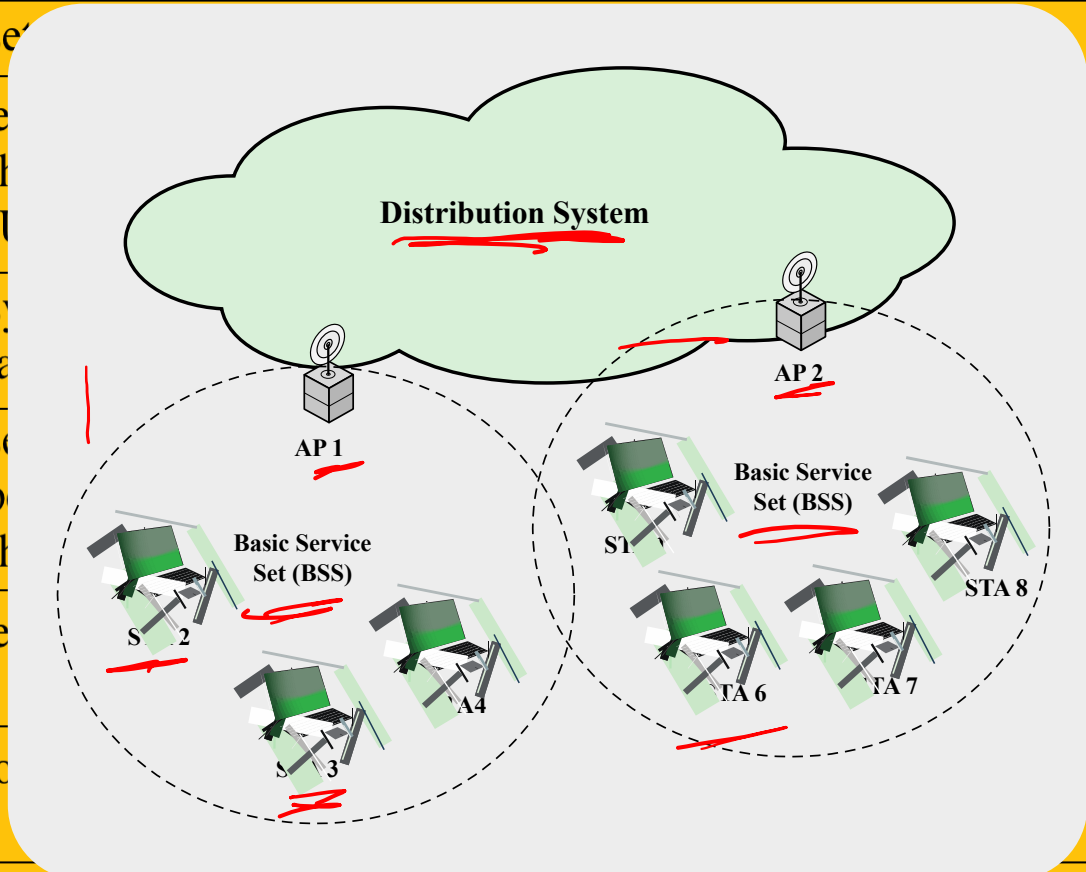
802.11n (2009) <u>Wi-Fi 4</u>	802.11ac (2013) <u>Wi-Fi 5</u>	802.11ax (2021) <u>Wi-Fi 6 6E</u>	802.11be (est. 2024) <u>Wi-Fi 7</u>
2.4GHz and 5GHz supported - Wider channels (40MHz) - Better modulation (64-QAM) - Additional streams (Up to 4) - Backward compatibility with 11a/b/g - Standard supports up to 600Mbps	5GHz only - Wider channels (80, 160MHz) - Better modulation (256-QAM) - Additional streams (Up to 8, implemented up to 4) - Backward compatibility with 11a/b/g/n - Standard supports up to 7Gbps	2.4GHz, 5GHz and 6GHz supported - Wider channels (80, 160MHz) - Better modulation (1024-QAM) - Additional streams (Up to 8, implemented) - Backward compatibility with 11a/b/g/n/ac - Standard supports up to 9.6Gbps	2.4GHz, 5GHz and 6GHz supported - Wider channels (40, 80, 160, 240, 320MHz) - Better modulation (4096-QAM) - Backward compatibility with 11a/b/g/n/ac/ax - Throughput minimum of 30Gbps, expect 40Gbps+ - Low latency features - Draft 2.0 now in Working Group Ballot

(Ratification date) Products available in the market typically ~2 years prior

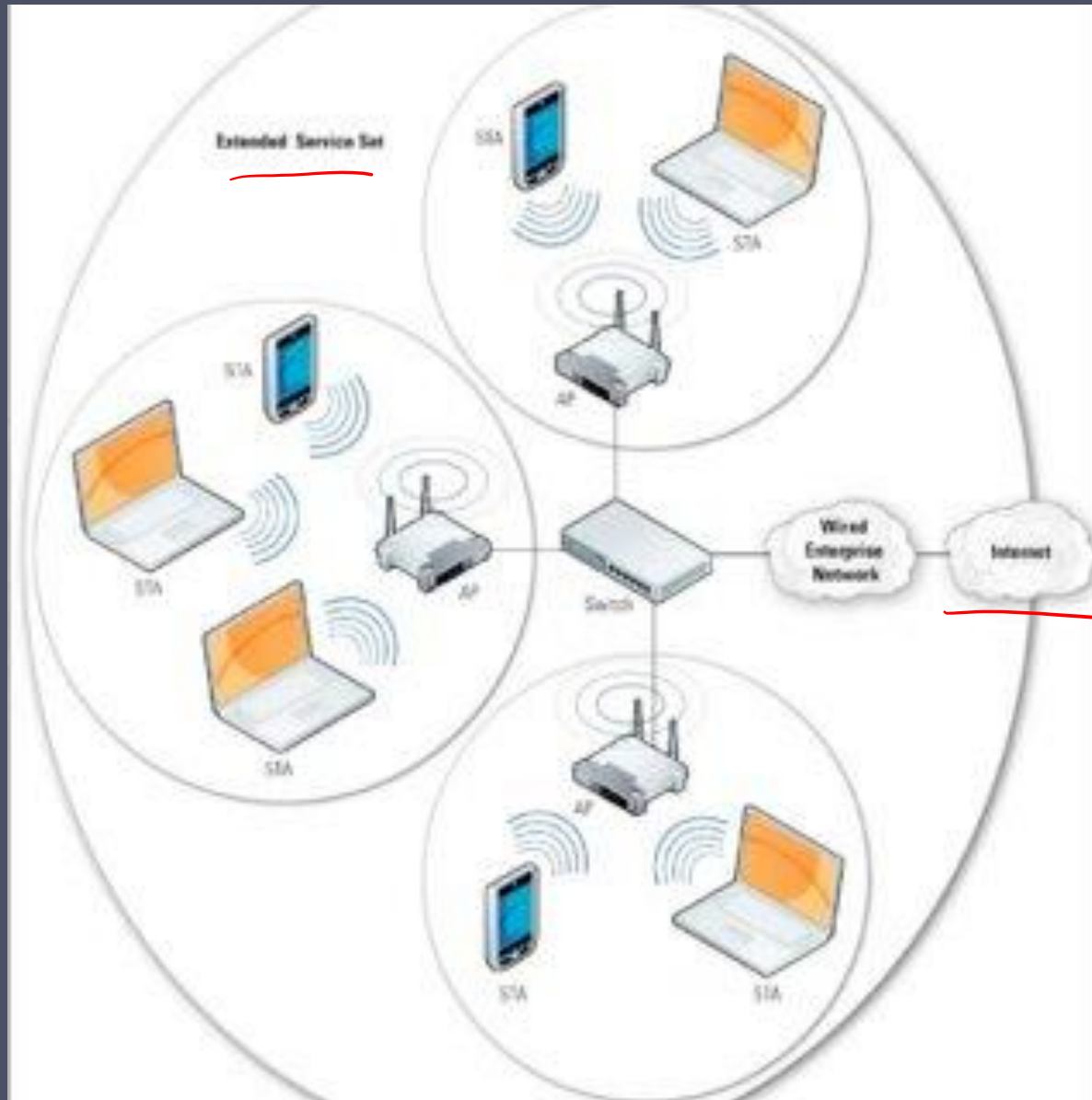
IEEE 802.11 Terminology

IEEE 802.11 Terminology

<u>Access point (AP)</u>	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
<u>Basic service set (BSS)</u>	A set of stations that share the same BSS color.
<u>Coordination function</u>	The function that coordinates the medium access between stations in a BSS.
<u>Distribution system (DS)</u>	A system that interconnects one or more BSSs and provides a means for stations in different BSSs to communicate.
<u>Extended service set (ESS)</u>	A set of one or more BSSs that share a common system architecture and a common set of management parameters.
<u>MAC protocol data unit (MPDU)</u>	The unit of data that is transferred between stations in a BSS.
<u>MAC service data unit (MSDU)</u>	The unit of data that is transferred between stations in a BSS.
<u>Station</u>	Any device that contains an IEEE 802.11 conformant MAC and physical layer.



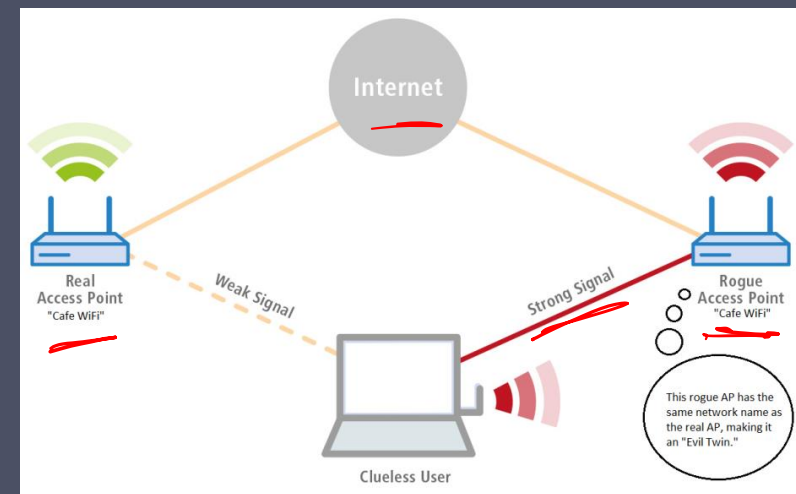
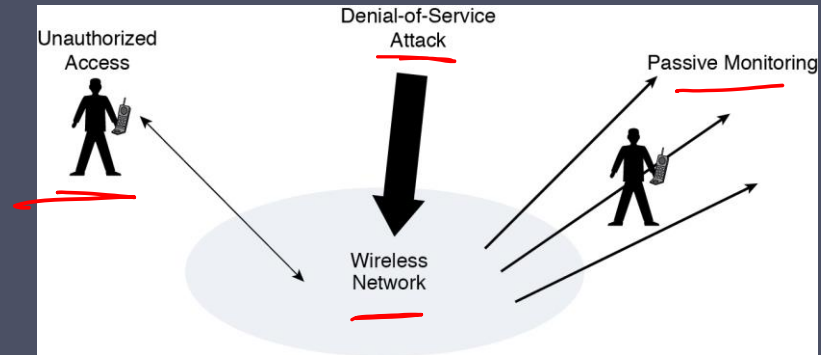
IEEE 802.11 Extended Service Set Example



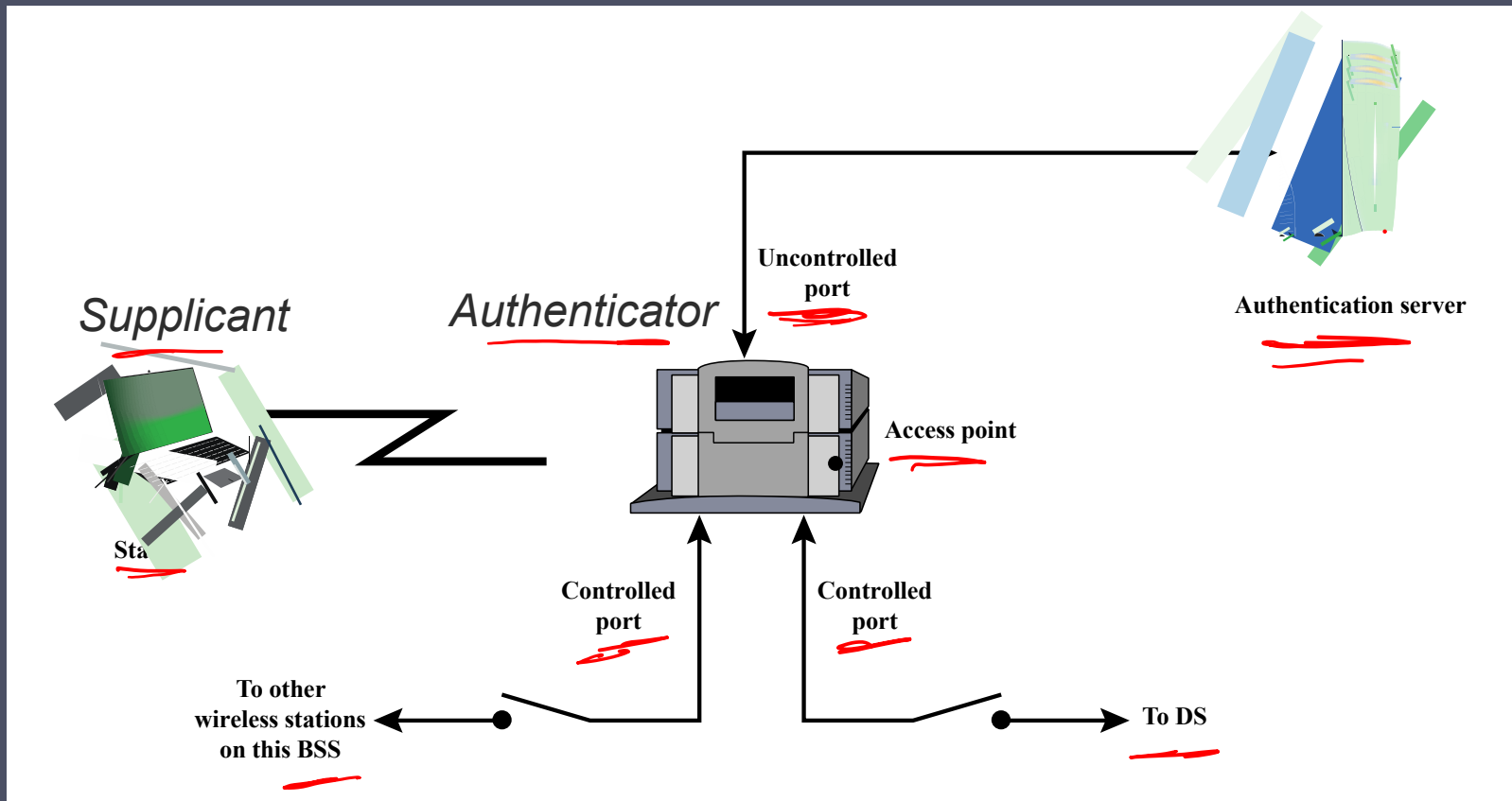
IEEE 802.1x Standard

Securing Wireless Networks

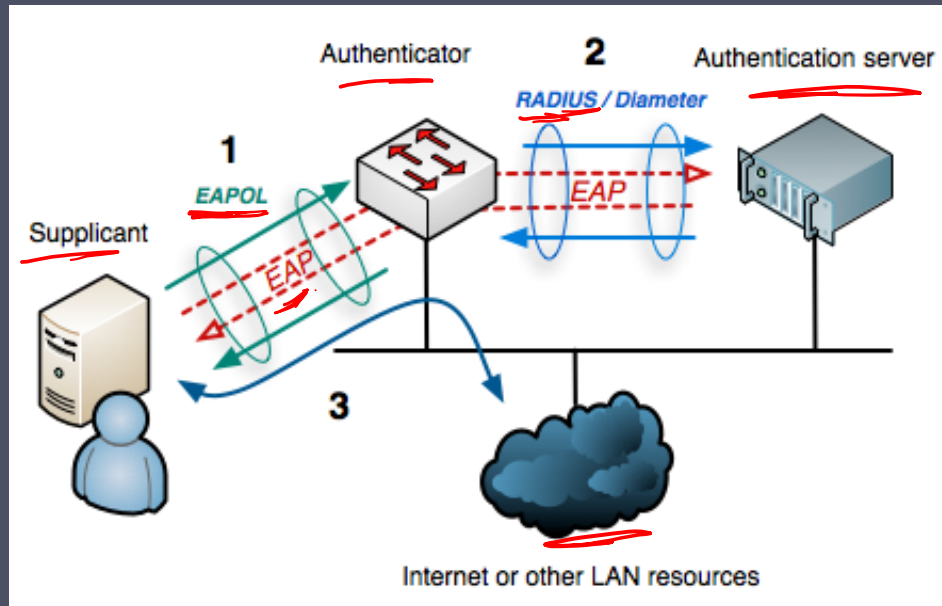
- The main threat involving wireless access points is unauthorized access to the network
- Principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control
 - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
- Use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors



802.1X Access Control



IEEE 802.1X standard for Securing Wired/Wireless Networks



Extensible Authentication Protocol (EAP) originally designed for Point-to-Point Protocol (PPP)

EAPoL (EAP over LAN)

EAPoW (EAP over Wireless)

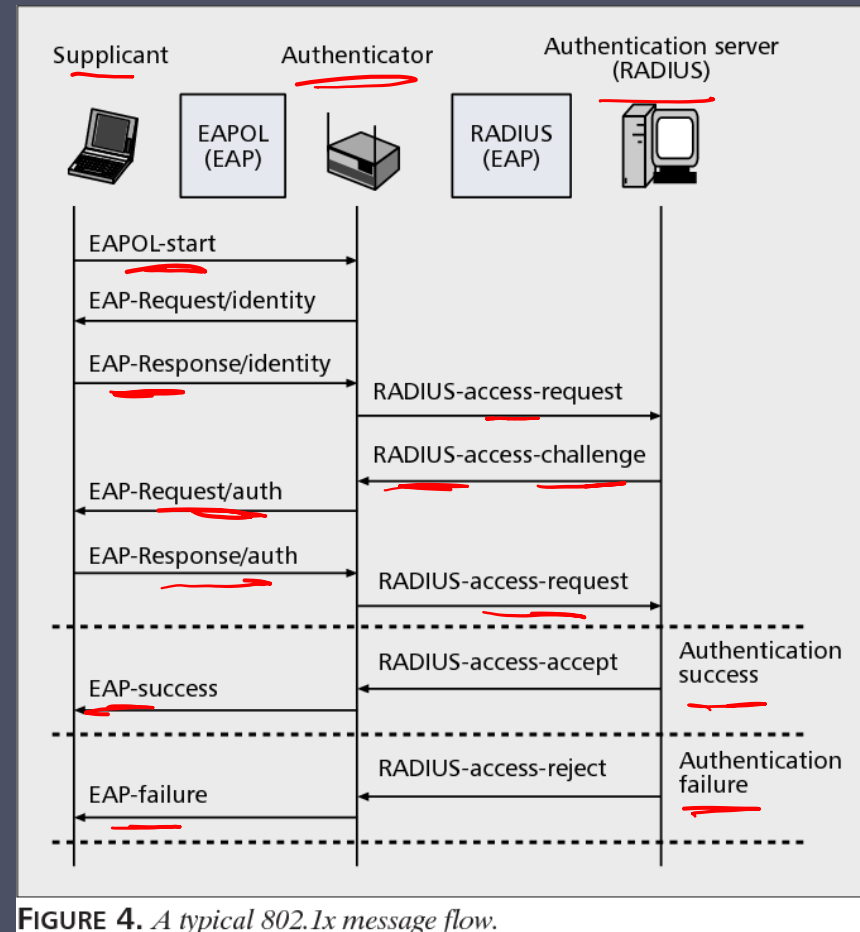


FIGURE 4. A typical 802.1x message flow.

Wireless Fidelity (Wi-Fi) Alliance

Wireless Fidelity (Wi-Fi) Alliance

<https://www.wi-fi.org/>

- The Wi-Fi Alliance is a non-profit organization that owns the Wi-Fi trademark.
 - Manufacturers may use the trademark to brand products certified for Wi-Fi interoperability.
- 802.11b
 - First 802.11 standard to gain broad industry acceptance
- Wireless Ethernet Compatibility Alliance (WECA)
 - Industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
 - Later renamed the Wi-Fi Alliance in 2002
- Term used for certified 802.11b products is Wi-Fi in 1999
- In 2018, the Wi-Fi Alliance introduced simplified Wi-Fi generational numbering to indicate supported 802.11 standard by the equipment e.g.
- Other programs
 - Wi-Fi Direct: In October 2010, the Alliance began to certify Wi-Fi Direct
 - Wi-Fi Easy Connect protocol via QR Code
 - Wi-Fi Passpoint : Wi-Fi Passpoint, alternatively known as Hotspot 2.0 and may others...



Year	WiFi Versions/Protocols	Old name	New name
1999	First Generation	<u>WiFi 802.11b</u>	<u>WiFi 1</u>
1999	Second Generation	WiFi 802.11a	WiFi 2
2003	Third Generation	WiFi 802.11g	WiFi 3
2009	Four Generation	WiFi 802.11n	WiFi 4
2014	Fifth Generation	WiFi 802.11ac	WiFi 5
2019	Sixth Generation	WiFi 802.11ax	WiFi 6



Demo Wi-Fi Info...

Wireless LAN Security

Wireless LAN Security

- There are two characteristics of a wired LAN that are not inherent in a wireless LAN.
 - In order to transmit over a wired LAN, a station must be physically connected to the LAN, which is not the case in Wireless...
 - Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN, which is not the case in Wireless...

