If you are new to IT financial management, it can be confusing to read and hear technical terms that are unfamiliar. This is a list of IT terms that may be of help to do your job.

Agile

Agile is a project management term that means to continually improve through small and digestible increments.

Algorithm

An algorithm is a sequence of instructions used to perform a task in software.

Artificial Intelligence (AI)

Artificial intelligence (AI), is a term used to describe computers' aptitude to mimic human abilities such as reasoning, knowledge representation, planning, learning, natural language processing, perception, robotics, social intelligence and general intelligence.

Assembly Language

Assembly language is a low-level programming language that communicates with the hardware of a computer.

Attenuation

Attenuation is the loss of signal strength in networking cables or connections. It may cause signals to become distorted or indiscernible.

Augmented Reality (AR)

Augmented Reality (AR) uses a device placed between the person and their environment to provide an enhanced version of their surroundings by providing virtual elements in the field of vision.

Automation

Automation is the technique of using software or scripting to perform a specific process or task without manual input. Automation often frees up knowledge workers from routine tasks but still requires oversight to ensure proper operation.

Autonomous Vehicle

Autonomous vehicles can operate and sense their surroundings without human involvement.

Big Data

Big data is a label that typically applies to extremely large and/or unstructured data sets or data sets. Many organizations have little differentiation between their approach to big data and their approach to traditional data sets.

Biometric Authentication

Biometric authentication is using a person's unique characteristics to verify their identity, including fingerprint scanning, facial recognition and voice recognition.

Blockchain

A blockchain is a list of records linked together using special cryptographic operations across a distributed network of computers.

Blocklisting

In tech, blocklisting is the process of denying access to applications or other entities that might pose a threat to a network.

Bluetooth

Bluetooth is a technology that allows devices to connect with each other over short distances without wires or cables.

Botnet

A botnet is a system of devices that are infected with malware and is controlled by an attacker, sometimes used in DDoS attacks.

Central Processing Unit (CPU)

A central processing unit (CPU) is a piece of computer hardware that retrieves, stores, processes and executes instructions. Think of the CPU as the brains of the computer.

Cache

Caches are digital storage used to store temporary files that devices can use for future requests in order to run more efficiently.

Cloud Computing

Cloud computing is the model of providing virtual infrastructure or software via network connections in a way that allows more self-service and dynamic allocation. This can be done by working with a public cloud provider or building a private cloud implementation.

Computer Networking

Computer networking is the process of linking computers together to send and receive information from each other.

Containerization

Containerization is the process of isolating and maintaining an application. Everything that the application needs to run is placed inside that container. It can then be moved around regardless of the host operating system.

Cyberattack

A cyberattack is a set of actions aimed to infiltrate computer networks, systems and personal devices.

Cybersecurity

Cybersecurity is the practice of protecting digital assets against cybercriminals, including measures such as network security, penetration testing or workforce education.

Cybersecurity Analyst

A cybersecurity analyst (or cyber risk analyst) is someone who detects and predicts cyber threats and then implements changes to protect an organization.

Cybersecurity Compliance

Cybersecurity compliance is the practice of adhering to standards and regulatory requirements set forth by an agency, law or authority group.

Cybersecurity Specialist/Engineer

Cybersecurity engineers work to build and maintain a system that's safe against cyberattacks. They focus on fixing and protecting these systems and staying up to date on new technology so they can keep their system secure.

DDoS Attack

A distributed denial-of-service (DDoS) attack aims to disrupt normal web traffic from accessing a site by flooding a server with internet traffic.

Dark Web

The dark web is a part of the internet that isn't accessible to the general public. It can only be accessed by using special software so that users can remain anonymous.

Data Analyst

A data analyst is someone who works with an organization's data to assist in making better business decisions and provide insights that support decision-making efforts.

Database Administrator

A database administrator is someone who manages all aspects of an organized database environment.

Data Center

A data center is a physical server facility that securely houses critical applications, data and other digital assets.

Data Mining

Data mining is the process of examining and manipulating data sets to find patterns and prepare data for deeper analysis.

Data Visualization

Data visualization is the representation of data through visual elements like charts, plots, infographics, maps, etc.

DevOps Engineer

DevOps engineers is someone who combines software development and IT infrastructure operations to increase an organization's ability to gain efficiency in software production cycles.

Drone

Also known as unmanned aerial vehicles (UAV), drones are flying machines that are controlled remotely or can fly on their own.

Edge Computing

Edge computing allows data to be processed as close as possible to the point of creation.

Embedded Development

Embedded development is when manufacturers place software or code into products that consumers use every day.

Encryption

Encryption is the process of concealing private information by converting digital information into something that can only be read with a key related to the type of conversion.

Front End Developer

Front end developers use programming languages such as HTML, CSS and JavaScript to design and develop the look and feel of a website.

Graphics Processing Unit (GPU)

A graphics processing unit (GPU) is a piece of computer hardware that renders graphics on a device.

High-definition Multimedia Interface (HDMI)

Short for high-definition multimedia interface, HDMI digitally transmits video and audio data from one source to another.

Incident Response Plan

An incident response plan is a combination of people, process and technology that is documented, tested and trained toward in the event of a security breach. The purpose of the incident response plan is to prevent data and monetary loss and to resume normal operations.

Information Technology (IT)

Information technology (IT) is the development and use of computer systems and networks to store, manage or retrieve information. It also is used to refer to the organization within businesses, government agencies and universities that have responsibility for the hardware/software/network operations, system development/maintenance, and any related support.

Infrastructure as a Service (IaaS)

Infrastructure as a service (IaaS) is a type of cloud computing that provides access to storage, servers, memory, etc.

Internet of Things (IOT)

Internet of Things (IOT) refers to systems of internet-connected devices that provide computing capability. These devices are different from traditional computers and can provide intelligence to everyday objects.

IP Address

An IP address is a string of numbers used to identify devices on the internet or network.

IT Project Manager

An IT project manager is someone who sets timelines for technical projects and keeps the team on task and on budget.

IT Support Specialist

IT support specialists (or help desk technicians) are the individuals responsible for analyzing, troubleshooting and evaluating technology issues.

Local Area Network (LAN)

A local area network (LAN) consists of a series of computers linked together to form a network in a relatively contained location, such as a home or office building.

Linux

Linux is an open-source operating system used extensively in IT infrastructure. Linux is technically a family of different variations, known as distributions, all based on the same core code, known as the Linux kernel.

Machine Learning

Machine learning is a form of artificial intelligence that allows software to learn patterns based on sample data.

Malware

Malware refers to any software that is intended to threaten or compromise information or systems.

Managed Service Provider (MSP)

A managed service provider (MSP) is an IT business that has the skills, expertise and experience to implement and manage technology solutions that help their clients' businesses achieve peak performance.

Near-field Communication (NFC)

Near-field communication (NFC) is a short-range and contactless form of communication that allows devices to communicate with each other.

Network Administrator

Network administrators are IT pros that support an organization's internal servers by installing, maintaining and monitoring systems.

Network Segmentation

Network segmentation is the process of dividing a computer network into separate network zones by using devices like bridges, switches and routers.

Next-generation Firewalls (NGFWs)

Next-generation firewalls (NGFWs) are network security devices that provide complete application control and visibility and are more sophisticated than traditional firewalls.

Open-source Software

Open-source software has code that can be modified and seen by anyone. What developers are allowed to do with it afterward depends on the specific open-source license that is used.

Operating System

Operating systems connect computer hardware to applications and manages all memory and processes. Some examples include Linux, Apple macOS and Microsoft Windows.

Passive Optical Network (PON)

A passive optical network (PON) is used by telecommunications network providers to allow a single fiber from a service provider the ability to maintain an efficient broadband connection for multiple end users.

Penetration Testing

Penetration testing is the process of attacking a network in order to assess the strength of the network's cybersecurity defenses.

Phishing

Phishing attacks use email, phone or text to get someone to provide sensitive information such as passwords and credit card information.

Platform as a Service (PaaS)

Platform as a service (PaaS) is a cloud computing service that uses virtualization to offer an application-development platform to developers or organizations. This platform includes computing, memory, storage, database and other app development services. PaaS solutions can be used to develop software for internal use or offered for sale.

Programming Language

A programming language is a set of rules or instructions that are used to create software applications.

QA Analyst

A QA analyst is someone who uses quality assurance techniques to detect errors in a software product or process.

Random Access Memory (RAM)

Random access memory (RAM) is a form of computer storage that can be rewritten multiple times.

Ransomware

Ransomware is a type of malware that encrypts your data so that attackers can demand a ransom in exchange for giving your access back.

Raspberry Pi

A Raspberry Pi is a credit card sized computer that brings programming capabilities and computing power to people all over the world.

Security Architect

A security architect is someone who develops and maintains the security of an organization's network. They also collaborate with business leaders, engineers, developers and more to protect an organization from cyber threats.

Security Operations Center (SOC)

A security operations center (SOC) can refer to the team of experts that monitor an organization's ability to operate securely. It can also refer to the location of the physical equipment used for monitoring.

Social Engineering

Social engineering is the method of gaining the trust of a user so that the attacker can acquire sensitive information that can be used to access data.

Software as a Service (SaaS)

Software as a Service (SaaS) is the method of delivering applications or software via the internet so that it can be easily accessed by anyone that is connected to the internet.

Spoofing

Spoofing is when cybercriminals use deception to appear as another person or source of information.

Steganography

Steganography is the practice of hiding a secret message inside of something that is not a secret with the purpose of concealing and deceiving.

Systems Administrator

A systems administrator is someone who implements and maintains backend IT infrastructure such as servers and networks.

Threat Hunting

Threat hunting is the process of mitigating cyber threats before they attack an organization.

Threat Detection

Threat detection is the process of finding malicious activity on your network.

Troubleshooting

Troubleshooting is the process of identifying problems with a network through a rigorous and repeatable process and then solving those problems using testable methods.

UI/UX Designer

UI/UX designers are individuals who research the behavior and preferences of consumers in order to develop and test design models that make products easier for people to use.

Virtualization

Virtualization is the process of creating copies of computing resources such as servers or storage. Multiple copies can be created on a single piece of physical hardware, allowing for more flexibility in operations.

Virtual Private Network (VPN)

A virtual private network, is an extension of a private network over public resources, using dedicated hardware or software to create the extension and securely transmit data.

Virtual Reality (VR)

Virtual reality (VR) is using computer-simulated three-dimensional environments to provide the user with an immersive and interactive experience.

Vulnerability Assessment

Vulnerability assessment is the process of discovering and analyzing vulnerabilities and penetration testing is the process of exploiting those vulnerabilities to help determine the best mitigation technique.

Web Developer/Designer

Web developers are individuals responsible for both the design and look of a website as well as the site's technical aspects such as performance and capacity, which are metrics of a website's speed and traffic.

Wide Area Network (WAN)

A wide area network (WAN) is a large network of information and data that is not tied to a single location.

Zero Trust

Zero trust is an overarching model of cybersecurity that forces verification of users and data at every level rather than assuming that the source of the information can be trusted.

Source: www.comptia.org