BR1GHT

Vision on Digital Control

Towards Continuous Monitoring

The digital transformation is reshaping organisations with an increasing pace. Digital solutions using RPA, IoT and mobile are being implemented in the business to save costs, improve business processes or to build client intimacy. But what are the risks of these new digital solutions, how do you control them and what does digital mean for your control environment? In a series of publications, we will dive deeper into these questions and take you with us in our Digital Control journey Towards Continuous Monitoring.

By Ronald Teuthof

May 2020

Companies are getting digital in a faster pace than ever, implementing new solutions, using digital drivers[1] such as data-analytics, Robotic Process Automation (RPA), Internet of Thing (IoT), and often in combination with cloud computing and mobile. Inefficiencies in mostly financial or time-consuming back-end processes are reduced, infrastructural technology components are better monitored resulting in preventive maintenance gains. New digital opportunities are being explored, such as digital twins, wearable technology, and so on. However, all these developments have two things in common. They are all adding complexity and the all cause risk and control uncertainties. And it does not stop there. Unprecedented digital areas are entered, using artificial intelligence, augmented reality, machine learning and blockchain, adding even more complexity to a level that only a small number of specialists still can comprehend. At this moment less than 30 percent of organisational transformations succeed[2].

What are the risks of these digital implementations and how do we control them? Digital Control is about 2 questions:

1. how do we control digital, and
2. what does digital mean for control?

Companies are becoming technology firms faster than the current generation can adapt to. Technology capabilities need to become part of business capabilities, and this takes time. IT will be everywhere and fully owned by business.

Everywhere innovation initiatives are stimulated and often without coordination or without any chance of success other than reinventing the wheel. Central IT departments will need to redefine their way-of-working from inflexible central owned IT towards agile managing digital transformation in terms of guiding, driving and controlling.

Companies become more and more dependable on technology vendors, a still very small number of real experts and the large consulting firms who took them on their digital journey. A digital journey full of changes, where change is the only constant.

How do you manage those third parties and how do you manage those new pieces of technology implemented in your environment? New technology, which often are software components, is critical for management, providing the information you use to steer your company, making decisions for you and initiating activities in your name.

How will you control your new digital components? Is the 2'nd and 3'rd line of defence able for the tasks ahead?

Can we stop the digital journey? No, we cannot, and neither should we want to. This paper is not written to provide a radical opinion against digitisation. However, we must find better ways to manage the risks emerging from it. Whilst we all are in our bubble of opportunism, slowly but surely, all eyes move towards the second and third line of defence in companies. Risk and compliance departments strengthen their focus on those new risk and compliance areas. Security, data and analytical specialists are added to understand the digital business activities and its risks better, focusing on denial of service attacks, hackers, fraud, unexpected deviations and compliance with GDPR and other laws and regulations.

The pace of the digital transformation is simply moving faster than we can enhance the capabilities of our current risk, compliance, and audit specialist. New generations of digital control specialists enter the market, but it is still

[1] A digital driver is a new technology area driving new opportunities for business improvement.

[2] Unlocking success in digital transformations, McKinsey & Company, October 2018.

not enough to bridge the gap. When new young digital control experts enter the market, they are not only inexperienced, but in many cases, they will start working in the business itself, the so called first line, implementing control by design. And this is how it should be done. Does this mean that the situation of risk, compliance and audit departments is hopeless? If they do not act now, I believe yes. The gap between the traditional way of risk management, compliance and audit and the level businesses become digitally, simply grows too wide. If risk and audit departments act now and become part of the digital journey, becoming digital skilled and start using technology solutions themselves, then I believe they will stay relevant. However, they will need to change their way of working drastically and fast.

The risks of digital. Let us dig a little deeper.

Looking at a company you roughly can identify 4 layers:

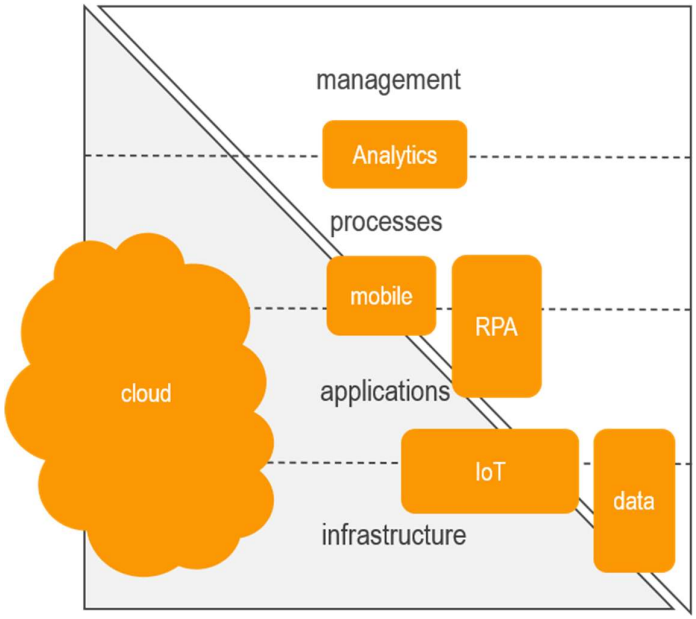


Figure 1. Four layers of a company, where many parts are sourced out to external providers (left triangle).

- Management (or governance), the organisation structures and management control domain. This is the core that makes the company what it is, where the strategy is defined, unique selling points or business purposes are established. Where decisions are made on day-to-day events and long-term visions are created.

- Processes, or the basic building blocks of how business procedures and activities are streamlined. Processes define how people are working, what they need and what they deliver. In some companies, processes are being outsourced (business process outsourcing) or brought outside the company through digitisation (e.g., customer functionalities).

- Applications are getting more and more automated and outsourced. The digital where we are referring to are basically applications, automating input, data transformation and output. At this moment we see one movement of large ERP-packages being outsourced (e.g., SAP) against new open digital platforms, where vendors work together to build autonomous applications working with each other as one via open API-sources.

- Infrastructure, technical systems, either information technology (IT), such as IT-networks and hardware, or the infrastructure of companies used in their core business, also called Other Technology (OT), such as the grid in utility companies. Whereas traditional IT is already highly outsourced, new cloud supported IoT platform are being built to monitor OT.

The digital transformation impacts all the above layers in a company and in most cases all at the same time in a context where infrastructure, applications and processes are undergoing changes and are being highly outsourced. What makes it even more complex is that digital solutions hardly ever work on their own but come together with other solutions. What makes it almost too complex, is that all those solutions come from different vendors or

suppliers and are all in a certain state of maturity and development. This initiates an unstoppable 'push' of fragmented half-fabricates growing like a virus without a predefined overall picture of the end state. In all cases they do certain things in solving a problem, however the uncertainty lies in the following questions:

- what else are they doing?
- who is changing the solutions and how do we know it is what we want?
- if one component is changed, what is the effect on the others?

In many situations, new digital solutions are 'black boxes' and it is not always clear what they exactly do. Because of that, they cause major uncertainties and pose risks to the reliability and availability of the companies' infrastructure, applications, processes, and management functions.

This brings us back to our first question; 'How do you control digital?'

How do you control digital? Control by design

When you look at all the new digital solutions, they all can connect to a system. A system is either an IT-network, a 'thing', an application or a process and they all monitor that system with the purpose to initiate an activity to improve the performance of that system.

Examples of those digital solutions are:

a. *A grid company uses 'things' such as sensors, monitors its temperature, signals for maintenance or shuts it down if it gets too hot.*
b. *An RPA application monitors another application for data, when it meets certain conditions, it signals for an activity or automatically initiates a transaction in another application, automating processes.*
c. *A security solution is monitoring an IT-network to detect unauthorised access. If it detects an intrusion, it will send a signal to the security officer, but also automatically tries to reduce the impact by for example shutting IT-ports where intruders came through.*

When you look closer at the digital solutions, they all have 3-layers in common:

1. Data collection (or warehouse function).
2. Analytical engine (for decision support purposes)
3. Smart decision unit (decision automation and robotics).

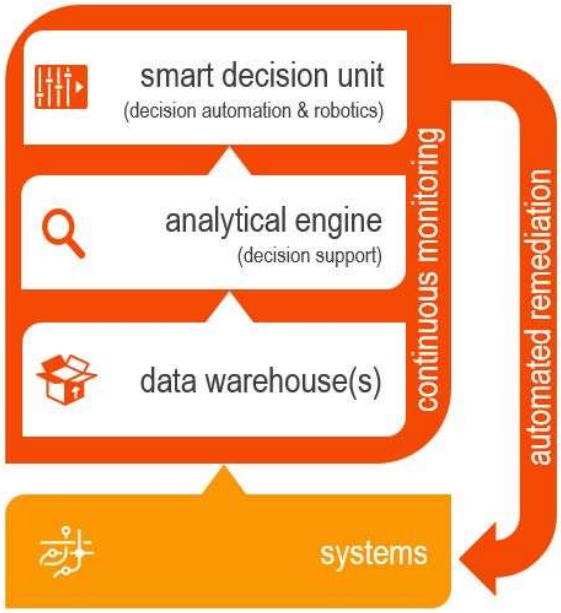


Figure 2. The 3 layers of a digital solution.

Not all digital solutions have all 3 components. Some are not storing data, while others are only built to analyse and do not have an automated remediation function. The 3 components all together are what we call the continuous monitoring 'engine' of the digital solution. They are the core which will drive current and future business improvements. All 3 components will develop themselves separately, each in its own pace.

Analytical engines will become more sophisticated from descriptive (what happened?), diagnostic (why did it happen?) to predictive (what will happen?). All triggering human assessments to decide for remediation. More and more prescriptive analytics (what should you do?) is developed where no human assessment is needed anymore. Many prescriptive analytical solutions automate

remediation fully without any human interference. Artificial intelligence further optimises automated responses and makes monitoring continuous.

Decision support now evolves from automated data processing towards technically controlling complex mechanical activities, such as stopping a car, 3D printing, and unloading container ships, all by itself without human intervention.

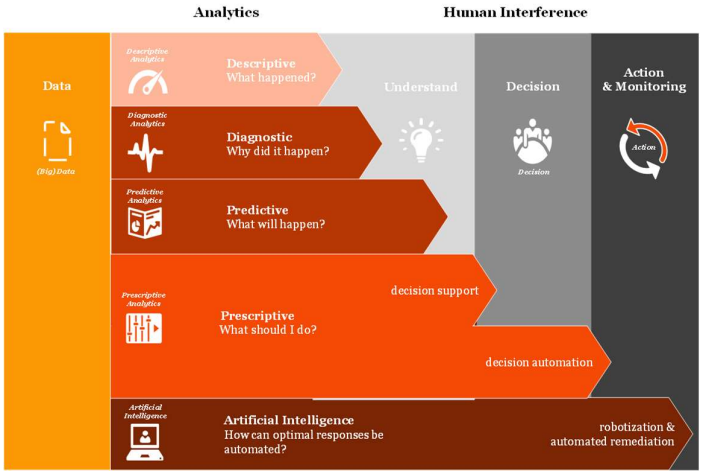


Figure 3. Developments of the 3 layers of digital solutions.

But how do we know that they only do what we think they do and nothing else, now and in the future? The answer to that question lies in 3 things:

1. **Build control by design.** When implementing new and complex digital solutions, it is important to define controls in the design phase. When a standard solution is used, it is important to understand, evaluate and decide on the risks involved. The risk can only be reviewed properly when the whole context is taken into consideration. For example, when you want to control an RPA solution, you need to have an end-to-end overview with process control objectives considering the effect on all applications. It helps to limit the number of different solutions and vendors and have more strategic relations with them. To get enough assurance that the digital solution is not doing undesired activities (like fraud), it is important to do source reviews and fully control the change management procedures over the development of the solutions. This is by far the most complex and detailed expertise that is needed.

2. **Scenario or model testing.** You cannot perform source reviews every time new

versions are implemented. To gain as much assurance as possible that no undesired activities are built in, it is important to have scenario's with specific cases available to run automatically when programs are tested. Those scenario's need to be build and operated parallel whilst the solution is programmed. We call this model testing. Those test models contain test cases around certain conditions and controls and need to be smart. They not only need to generate 'known' cases but have sufficient artificial intelligence in them to generate test cases by itself, covering unforeseen risks.

3. **Continuous controls monitoring.** During the build phase of your digital solution, it is important that you build the controls in a separate 'control repository'. After the implementation of your solution, you must continuously monitor the operating effectiveness of your solution by continuously monitoring the defined controls. In building just 'one' central controls repository over all your new digital solution, lies the answers to our first question 'how do you control digital', and the starting point for our second question 'what is the impact of digital for control'. However, before we answer the second question, let's look closer at continuous control monitoring?

Continuous Controls Monitoring (CM)

In almost all cases, digital solutions built to improve performance can at the same time be used as continuous controls monitoring to realise reliability. Digital solutions and continuous controls monitoring systems are two sides of the same coin.

When you have integrated your digital solution with your controls repository, you will have the basis to get assurance over the solution in two ways:

a. **Issues**. If your digital solution detects a deviation of the standard, it is built to automatically remediate this, but it also needs to document the issue in the controls repository. This control event leads to an issue to be reviewed by a controls expert. The controls expert will initiate remediation of the control issue (via continuous improvement). When change is constant, the scenario test results also need to automatically result in control events (thus realising control over change).

b. **Positive assurance**, when your solution performed its tasks, has analysed data and did not find deviations of the standard, it needs to document this as well in the controls repository. This results in positive assurance that the system and controls are working correctly.

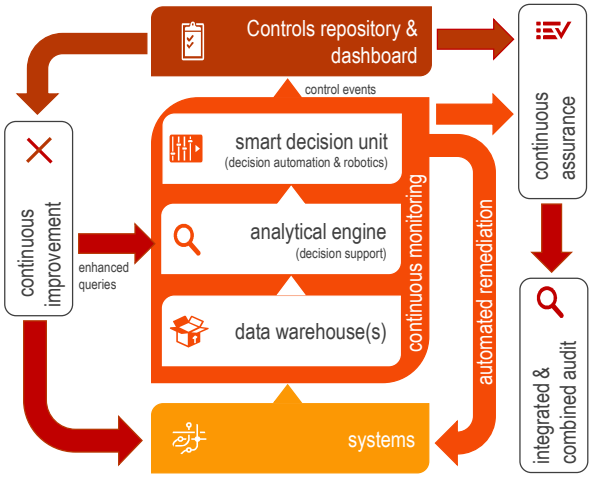


Figure 4. Developments of the 3 layers of digital solutions.

So, this is how it should be (and can) be done, but what is the current state of continuous controls monitoring? Today you see the following:

a. Many central controls repositories are part of GRC technology solutions, where risks are centrally documented, controls are identified and automatically dispatched to control owners. The control owners perform the controls and document them manually in the GRC-system. This is a time-consuming process, and in many cases GRC-systems

are costly, complex to implement and seen as an extra burden. In very limited situations I have seen that controls are automatically tested.

b. Many software solutions, whether they are new digital RPA or IoT solutions or existing ERP-systems, have controls built in them. Some controls are tested automatically, but hardly any of them are documented in a central controls repository. This causes uncertainties whether the solution only does what it should do or whether there are risks of built in unwanted functionalities (e.g. fraud or failures, trojan horses, security breaches, and so on).

c. In the marketplace we now see continuous controls solutions, monitoring infrastructure and or applications and providing insight into control deficiencies. However, they are on top of existing software solutions and not part of them. This results in two inconveniences; one, the continuous monitoring solutions don't provide automated remediation and two, when the bases systems or the control context (frameworks, regulations) are changed, the continuous monitoring systems need to change, causing an uncontrollable situation and may lead to false assurance (believing systems are monitored, when in fact they are not). Furthermore, in many cases it is unclear what those continuous monitoring systems are doing. They are the same black box we mentioned before.

There is much more to say about continuous controls monitoring, what is working already, what is the overall context of it, and so on. For more details and updated versions of our Digital Control vision, we refer to our website **www.BR1GHT.eu.**

Now we understand what Continuous Monitoring is and how it helps control digital, it brings us to our second question; 'what does digital mean for control?'.

What is the impact of digital on control

We have realised that your IT environment, including all new digital solutions with RPA and IoT, automatically feeds your central controls repository with issues and / or positive confirmation that your controls are operating effectively.

Now your central controls repository can drive your 2'nd and 3'rd line of defence and revolutionise all their activities and added value to the business.

Realtime Compliance (RTC). When laws & regulations as well as voluntary policies & procedures have been translated (designed) into controls (control framework) the compliance function, often performs labour intensive 'tick-the-box' exercises to get assurance that those controls operate effectively and that the organisation is 'overall' compliant. With the usage of a central control repository and automated controls testing, real-time insight in the status of those controls is provided. As a result, the compliance function can immediately react when deviations occur and can add value on the spot, whilst time is saved for other value adding activities.

Continuous monitoring provides organisations with the capability to be better in control and be more transparent about control. Transparent towards your stakeholders; oversight bodies, regulators, but also suppliers, business partners, clients, and third-party service providers, such as IT data centres. When you allow your partners, vendors and suppliers to document the controls they perform over the activities in under your ultimate responsibility, then you create horizontal and vertical (controls) integration. This is the bases for voluntarily oversight and the topic of our second vision document. Voluntarily oversight will reduce the need for costly external assurance engagements performed by accountants and reduce the cost of control significantly.

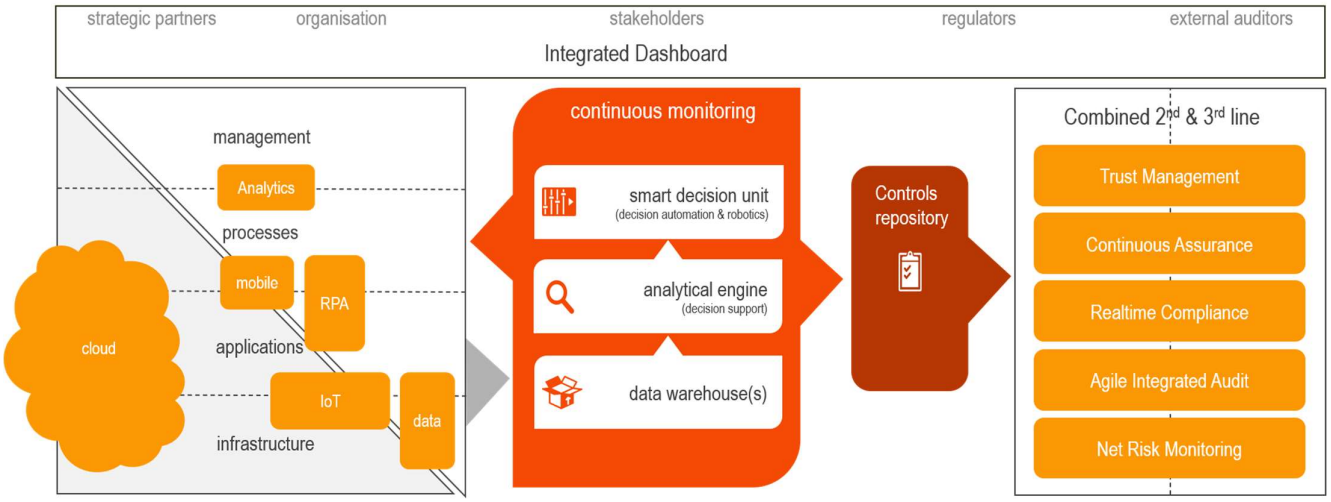


Figure 5. Continuous controls monitoring driving the 2'nd and 3'rd line of defence activities.

Net Risk Monitoring. Risk Management will still define top-down 'key controls' to manage specific risk areas, however continuous monitoring will automatically 'flag' controls as operating effectively. This will increase the total level of risk assurance, reduce manual test efforts and thus freeing-up time to use to dive into other emerging risk areas. Risk Management will have a dashboard and the capability of net risks monitoring.

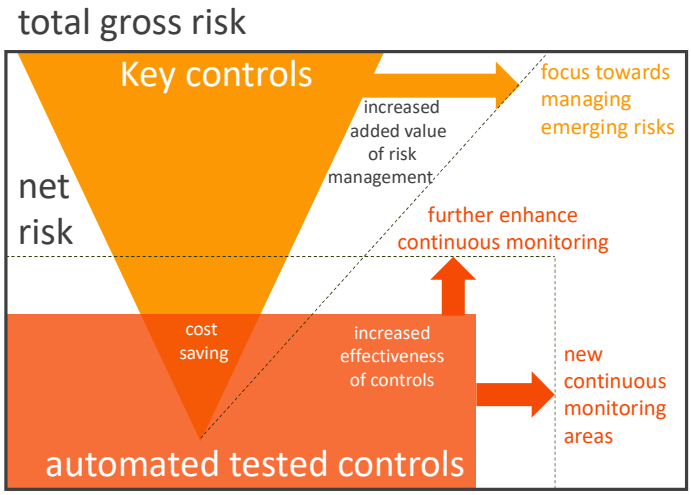


Figure 5. Risk Management net risk monitoring, cost savings and added value towards managing emerging risks.

An agile integrated audit. The Internal audit function will change from thoroughly planned annual audit programs towards agile auditing. When issues are flagged in your controls repository, internal audit will automatically receive notifications and will support risk and the business in analysing the root causes of those control failures. Agile Internal Audit allows the internal audit function to now:

- add flexibility into their programs and immediately react on controls issues,
- directly focus on stakeholder needs by interacting with the business,
- accelerate audit cycles,
- drive timely insights, and
- generate less documentation.

An integrated audit involves both the audit of financial statements and its system of controls over financial reporting. An integrated audit will likely include an extensive examination of the controls associated with a firm's transaction processing systems. Direct insight in the controls status will provide internal audit with trust over the control environment. An extra benefit is that it also reduces external auditor's effort, time and costs, because they can get

their assurance directly out of the controls repository.

Continuous Assurance. Having your new digital solutions controlled, your controls build into your central controls repository and automatically and continuously tested, you now can be transparent in your business activities. Your control environment adds value to more than your 'licence to operate' alone. You can manage your controls in the context of the execution of your strategy and value delivery to your stakeholders. Stakeholders who go beyond the border of investors, regulators or auditors. You can reach your partners, people and society and provide continuous assurance over your purpose, which goes beyond financial performance and into the realisation of our global sustainable development goals, making our world a little better.

Trust Management. Being transparent means that all issues are directly visible to a broader range of stakeholders inside and outside your company's boarders. Trust arrives on foot but leaves on horseback and needs to be protected via, amongst others, a real-time continuous monitoring system, a continuous stakeholder dialogue and integrated business dashboard.

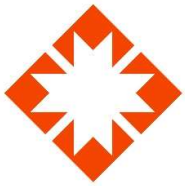
The Digital Control playbook

We developed a playbook on Digital Control and will update and produce a series of publications about the following subjects:

- The technology behind Continuous Monitoring, practical client cases.
- Maturity modelling. Making the step from compliance towards trust.
- Risk Management redefined.
- Realtime compliance towards horizontal and vertical controls integration.
- Voluntary oversight; moving away from external third-party assurance. Taking control ourselves.
- World class Internal Audit. Adding maximum value.
- How to audit and control new emerging technologies driven bij the digital transformation.
- Trust Management; focusing on value in a world of digital transparency.
- Building new digital capabilities in the 2'nd and 3'rd line of defence.

If you want to know more about BR1GHT, please follow us on LinkedIn, Facebook, Youtube or via our website www.BR1GHT.eu.

If you have questions related to this publication, please contact us on info@BR1GHT.eu. To discuss the content, please leave your thoughts, suggestions, or comments on our blog at our website.



'Let us help you to use the right technology to build your future on and to enhance & protect your business value.'

Drs Ronald Teuthof RE CISA worked for 28 years for PwC The Netherlands of which 13 years as a partner responsible for IT and (internal) audit & risk assurance related topics. In 2019 Ronald established BR1GHT with the purpose to add more value to clients, together with clients and with partners using best practice technology. BR1GHT now provides services to over 50 clients in 12 countries and works closely together with large communities of clients and technology experts.

Appendix definitions

Robotic process automation (**RPA**) is the use of software with artificial intelligence (AI) and machine learning capabilities to handle high-volume, repeatable tasks that previously required humans to perform. These tasks can include queries, calculations and maintenance of records and transactions.

The Internet of Things (**IoT),** a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Analytics is the discovery, interpretation, and communication of meaningful patterns in data. It also entails applying data patterns towards effective decision making. In other words, analytics can be understood as the connection between data and effective decision making within an organisation. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming and operations research to quantify performance.

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server. Clouds may be limited to a single organisation (enterprise clouds) or be available to many organisations (public cloud).

In computer science, **artificial intelligence** (**AI**), sometimes called machine intelligence, is intelligence demonstrated by machines. Leading AI textbooks define the field as the study of "intelligent agents": any device that perceives its environment and takes actions that maximise its chance of successfully achieving its goals. Colloquially, the term "artificial intelligence" is often used to describe machines (or computers) that mimic "cognitive" functions that humans associate with the human mind, such as "learning" and "problem solving".

Augmented reality (**AR**) is an interactive experience of a real-world environment where the objects that reside in the real world are enhanced by computer-generated perceptual information, sometimes across multiple sensory modalities, including visual, auditory, haptic, somatosensory and olfactory. AR can be defined as a system that fulfils three basic features: a combination of real and virtual worlds, real-time interaction, and accurate 3D registration of virtual and real objects. The overlaid sensory information can be constructive (i.e. additive to the natural environment), or destructive (i.e. masking of the natural environment). This experience is seamlessly interwoven with the physical world such that it is perceived as an immersive aspect of the real environment. In this way, augmented reality alters one's ongoing perception of a real-world environment, whereas virtual reality completely replaces the user's real-world environment with a simulated one.

A **blockchain** is a growing list of records, called *blocks*, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). By design, a blockchain is resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

Machine learning (**ML**) is the study of computer algorithms that improve automatically through experience. It is seen as a subset of artificial intelligence. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without

being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of applications, such as email filtering and computer vision, where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks.

A **digital twin** is a digital replica of a living or non-living physical entity. Digital twin refers to a digital replica of potential and actual physical assets (physical twin), processes, people, places, systems and devices that can be used for various purposes. The digital representation provides both the elements and the dynamics of how an Internet of things device operates and lives throughout its life cycle. Definitions of digital twin technology used in prior research emphasise two important characteristics. Firstly, each definition emphasises the connection between the physical model and the corresponding virtual model or virtual counterpart. Secondly, this connection is established by generating real time data using sensors. The concept of the digital twin can be compared to other concepts such as cross-reality environments or co-spaces and mirror models, which aim to, by and large, synchronise part of the physical world (e.g., an object or place) with its cyber representation (which can be an abstraction of some aspects of the physical world).

Wearable technology, are smart electronic devices (electronic device with micro-controllers) that are worn close to and/or on the surface of the skin, where they detect, analyse, and transmit information concerning e.g. body signals such as vital signs, and/or ambient data and which allow in some cases immediate biofeedback to the wearer. Wearable devices such as activity trackers are an example of the Internet of Things, since "things" such as electronics, software, sensors, and connectivity are effectors that enable objects to exchange data (including data quality) through the internet with a manufacturer, operator, and/or other connected devices, without requiring human intervention. Wearable technology has a variety of applications which grows as the field itself expands. It appears prominently in consumer electronics with the popularisation of the smartwatch and activity tracker. Apart from commercial uses, wearable technology is being incorporated into navigation systems, advanced textiles, and healthcare.

Continuous Controls Monitoring (CCM), refers to the use of automated tools and various technologies to ensure the continuous monitoring of business and financial transactions and transactional applications to reduce the costs involved for audits and to improve the level of trust of a company. CCM helps reduce business losses by using effective continuous auditing mechanisms and control monitoring of various aspects of the applications involved. It is mostly considered to be part of auditing where a set of automated procedures monitor the internal controls. Some of the controls monitored by CCM include authorisations, access, system configurations, business process settings and new digital solutions.