Cybersecurity Hyperglossary

DR. GARY HINSON, MBA

CRC Press
Taylor & Francis Group

Cybersecurity Hyperglossary

Precise and consistent communication is vital in the complex and ever-expanding field of cybersecurity and its related domains. This hyperglossary offers more than just plain English definitions of 5,555 terms and abbreviations; it's a meticulously crafted resource designed to foster a shared understanding across a diverse audience, from seasoned professionals to newcomers. By providing clear definitions and an innovative network of hyperlinked references, it enhances communication in critical areas, reduces misunderstandings, and facilitates a more engaging and interconnected learning experience across the broad landscape of information risk and security, privacy, governance, compliance, business continuity, ethics, and more.

Beyond basic definitions, this book delves into the nuances and origins of cybersecurity language, promoting vocabulary standardisation and reducing misinterpretations in various professional contexts. Furthermore, it bridges the communication gap between technical experts and non-technical stakeholders, empowering effective collaboration and informed decision-making. This book is a key tool for education and professional development, supported by a vibrant online community where experts collaborate to refine and evolve our terms of art. Ultimately, this comprehensive hyperglossary, coupled with community insights, offers an unparalleled advantage in navigating and shaping the future of cybersecurity understanding.

Gary Hinson, PhD, MBA, is an information security specialist with a particular interest in the human and business aspects of both protecting and exploiting information. His career stretches back to the mid-1980s as a practitioner, manager, and consultant in the fields of IT system administration, information security, and IT auditing for multinationals in several industries. For more than a decade until COVID, Gary created monthly packages of security awareness materials for subscribers. These days, Gary consults and teaches on the ISO/IEC 27000-series "ISO27k" information security management standards and information security metrics.

Cybersecurity Hyperglossary

Dr. Gary Hinson, MBA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Designed cover image: Shutterstock Image ID 2007809843

First edition published 2026
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 978-1-041-09552-1 (hbk)
ISBN: 978-1-041-09553-8 (pbk)
ISBN: 978-1-003-65067-6 (ebk)

DOI: 10.1201/9781003650676

Typeset in Calibri
by codeMantra

Contents

Foreword

Language, usually meant to communicate, often leads to misunderstandings. Even in the same country speaking the same language, different disciplines, trades, and professions often use different words to mean more or less the same thing often rendering clear communication the victim. This issue becomes even more pronounced in technology, where rapid innovation collides with deep specialisation. Within a single domain – take security, for example – terminology between, say, risk management and incident response can vary dramatically. Between civilian activity and the military, the differences in terms can be even more stark. What's referred to as a *data breach* in the civilian sector is called *spillage* by the U.S. Department of Defense. While one group will talk about *vulnerabilities*, others will discuss *attack surface*. What IT professionals might say is *data normalisation*; an epidemiologist will call *harmonisation*. This plethora of terms often creates confusion, slows collaboration, and makes interdisciplinary efforts more complex than they need to be.

This extraordinary glossary was created to meet that challenge head-on. With over 5,000 clearly defined tech terms and over 700 acronyms decoded, it offers a unified language for professionals working across IT management and operations, cybersecurity, risk management, artificial intelligence, and related fields. More than just definitions, it provides rich explanations and real-world context – clarifying not just what a term means, but *how* and *where* it's used. The goal is not only to reduce ambiguity but also to foster better understanding between technologists, managers, policymakers, and users.

What makes this work truly exceptional, and what sets it apart from typical glossaries, is its completeness. Thanks to the years of meticulous research and dedication by Dr. Gary Hinson, this volume captures virtually every significant term in the modern digital ecosystem. But it goes further still – unlike many reference tools, this glossary often includes full descriptions, nuanced usage notes, and, where relevant, quick links to external resources for deeper exploration.

This monumental tome will prove invaluable for anyone navigating today's tech landscape. For managers encountering unfamiliar jargon, for editors striving for clarity and consistency, and for professionals and students alike who need a trustworthy source of meaning, this glossary will become the go-to standard when clear, concise terminology is important. Whether in textbooks or RFPs, work orders or product or engineering specifications, or legal documents, the right words are paramount. Quite literally, this monumental work gets everyone on the same page.

Kudos to Dr. Hinson for this major contribution to just about anyone dealing with the digital universe – which these days, is pretty much all of us.

Krag Brotby
CISM, CGEIT, GRC guru

Language shapes how we think. In security, it shapes how we act, how we collaborate, and how we fail.

Cybersecurity, as a field, has suffered for years from a fragmented vocabulary. We borrow terms from engineering, risk management, military doctrine, academia, and marketing. We invent new ones at a breakneck pace, often without checking if they already exist elsewhere. Worse, we use the same words to mean different things depending on our background, our role, or our latest framework of choice.

And people get very protective over those words. Some of the biggest arguments I've seen are over whether or not cybersecurity should have a space or not. Really. I've had hate mail and harassment over it.

The result is confusion, chaos, and a lack of holistic thinking.

This matters. Cybersecurity is not a standalone discipline. It is a domain of security, sitting alongside physical, personnel, and technical domains. It intersects with safety, governance, operations, and culture. If we're going to respond to the complex, dynamic threats we face, we have to be able to work together.

That requires a shared language.

This hyperglossary is a starting point. Not a definitive guide, and not an attempt to impose a single top-down doctrine. Instead, it's an effort to bring some coherence to the words we use every day. To make it possible to understand one another, spot patterns and align our work. It won't be exhaustive or final. Language evolves, and so must this.

I've lost count of the meetings I've sat in where people thought they disagreed, but were speaking different security dialects. Where decisions got delayed because two teams were using different definitions for "threat" or "control." These moments add friction. At scale, they cause real harm.

More fundamentally, we need this clarity to make progress. It's hard to build shared models, improve resilience, or even teach effectively if we can't agree on what basic terms mean. Whether you're writing policy, engineering a system, running an incident, or trying to explain a risk to a boardroom, having a consistent, plain-language vocabulary makes life easier.

This isn't about dumbing things down. It's about raising the standard of thinking. Clear language doesn't just improve communication. It forces us to be precise. It makes hidden assumptions visible. It helps identify gaps in understanding and practice. And it makes space for genuine collaboration across disciplines.

We're at a point where the complexity of our systems, the capabilities of our threats, and the interconnectedness of everything demand better cooperation. That can't happen if we're all talking past each other.

Take this glossary as a tool. Use it, challenge it, add to it. Let it be something we build together, rather than something we argue over. Because the sooner we can speak the same language, the sooner we can get on with solving the problems that matter.

James Bore
Chartered Security Professional

Preface

This hyperglossary is the result of a personal quest to make sense of the rich language of cybersecurity. This book's size is a testament to the breadth and complexity of the subject, coupled with an extraordinary rate of change. I started this writing project back for my own benefit in the 1990s, at about the time that a group coordinated by the UK Department of Trade and Industry adopted a corporate security manual, becoming BS 7799 "Code of Practice for Information Security Management" in 1995.

Cybersecurity: in common use, this primarily refers to technological/IT security controls protecting computer systems, networks, and the associated data against attacks from the Internet. There's more to it, though.

Information security was a novelty back then, one that intrigued me with its focus on protecting and exploiting information. Since then, we've seen the rise of IT security and lately **cybersecurity** as computing and the Internet have become integral parts of modern life. Nevertheless, I appreciate that original focus on protecting and exploiting the valuable information content: to me, the computer systems and technologies are merely tools for data processing (now *there's* an historic term!).

Hyperglossary: contraction of **hyper**-linked **glossary**, an intuitive reference combining the best features of a glossary, dictionary, wiki, thesaurus, and encyclopaedia with specialist inputs, plain English definitions, and extensive cross-referencing.

The field can appear fragmented and scattered, with experts in various areas naturally developing their own jargon and specialised meanings. To address the challenge, I developed the **hyperglossary** format in 2001, making a reference resource even more valuable. I find the combination of clear plain-English definitions with embedded links to further information a powerful and intuitive way to capture and utilise the details. What's more, it's *fun* to release my inner geek, following my nose from term-to-term, rediscovering and reconnecting with concepts I'd almost forgotten much as I enjoyed browsing Roget's Thesaurus and encyclopaedias when I was a teen.

In recent years, I've incorporated terms relating to the risk and security aspects of **I**nternet **o**f **T**hings and **A**rtificial **I**ntelligence, with quantum computing just around the corner. While the pace of change in technology and cybersecurity keeps us professionals on our toes, it makes things tricky for business people and others struggling to keep up. Being left behind presents significant information risks in its own right; for example, unpatched IT systems are more vulnerable to ransomware, and mis- or dis-information is threatening democracy and personal freedoms, both real and present dangers as we see from the news headlines.

By publishing this book, I hope to foster greater consistency in our language, not only for those immersed in the field but also for technology and other professionals, business leaders, regulatory authorities, standards bodies, and others. Given that English is a foreign language for some of you, I have tried hard to create reasonably simple and accessible definitions, although the technical complexities and conceptual aspects sometimes frustrate that aim. I tried, honestly I tried.

Beyond simply a curated collection of terms and definitions, this book supports a vibrant online community through which cybersecurity professionals, from students to seasoned experts, share their knowledge and collectively enhance our understanding of the field. Ultimately, the

hyperglossary *plus* the global community of readers makes an unbeatable combination. Read on for opportunities to play your part in moving things forward.

PURPOSE

The primary purpose of this hyperglossary is to provide a comprehensive, user-friendly reference for anyone seeking to understand and use the terminology of cybersecurity and related domains.

Specifically, it aims to:

- Provide reasonably clear and concise definitions of about 5,000 key terms-of-art plus expansions of about 700 abbreviations, acronyms, and initialisms. Pragmatic explanations complement the formal definitions. Clearer communication improves understanding, enabling us to engage more productively in daily work, debate, research, policy-making, and decision-making.
- Acknowledge the origins of the concepts and terms we use today, while appreciating the subtleties of different meanings, emphases, and interpretations as the field matures.
- Standardise our vocabulary where appropriate, encouraging consistency and reducing misinterpretation across laws, regulations, standards, policies, procedures, guidelines, advertisements, job descriptions, management and audit reports, emails, presentations, articles, conversations, and more. Language issues present information risks in this area, worth avoiding or mitigating I feel. Greater linguistic alignment should reduce unnecessary fragmentation and divergence within the field, presenting a more unified front.
- Bridge the communication gaps between technical experts and non-technical individuals such as business leaders and industry regulators – a common problem arising from limited familiarity and fluency in each other's languages, perspectives, and worlds.
- Facilitate teaching, training, knowledge sharing, learning, and personal development within the cybersecurity profession, reducing barriers to entry and progression.
- Enable and support transnational discussion, collaboration, innovation, and technical development. Cybersecurity is most certainly a *global* concern.
- Lead the way in aligning terminology, especially concerning core terms such as 'threat,' 'vulnerability,' 'impact,' and 'risk.' If we wish to be taken seriously as professional experts, we really ought to agree on the fundamentals and be consistent in how we put things across.

SCOPE

This hyperglossary encompasses a broad spectrum of cybersecurity-related areas, including the following:

- Risk, particularly the proactive management of information risk as a business imperative.
- Information security, protecting all forms of information (not just digital data).
- Risk and security aspects of **I**nformation, **O**perational, **C**ommunications, **V**irtual, and **S**mart **T**echnologies (**IT**, **OT**, **CT**, **VT**, and **ST**) – and perhaps others.
- Privacy and data protection.
- Governance, accountability, rôles, and responsibilities.
- Compliance and conformity – similar but distinct concerns.
- Ethics and morality, navigating conflicts in ways that demonstrate integrity and foster trust.

- Business continuity, including resilience, **D**isaster **R**ecovery, and contingency planning.
- Various forms of assurance such as testing, reviewing, assessing, and auditing, including supply chain assurance, a substantial issue with cloud computing and globalisation.
- The intersection of technological areas such as **A**rtificial **I**ntelligence and **I**nternet **o**f **T**hings, plus other concerns such as environmental sustainability and climate change, with cybersecurity.

While striving for comprehensive coverage, the field continues to expand rapidly. Therefore, ever since its inception decades ago, the hyperglossary has been and remains a dynamic product, evolving and maturing with ongoing research and input from the global community as the language itself changes. The book you are reading is merely a snapshot in time.

Language can be misused or misunderstood and, despite writing this hyperglossary, I am not immune. While I have made every effort to research and define terms carefully, they often have 'flexible' meanings in practice and my interpretations may not always align with or capture the original authors' intentions. Context is crucial.

Many definitions include quoted text from authoritative sources such as international standards, but the quotes may not always be complete or perfectly up-to-date. *Please* refer to the original sources using the provided 'More info' links if it matters to you, especially if you plan to develop and share variant definitions.

Finally, to be absolutely clear, I am *not* a lawyer. This hyperglossary does not constitute legal advice. In some jurisdictions and circumstances, certain terms may have specific legal interpretations that differ significantly from those presented here. Do not rely on this glossary for anything critical or vital: it is intended solely for educational purposes. Always seek advice from competent, trustworthy, qualified, and experienced professional advisors and carefully evaluate their guidance.

AUTHOR PERSPECTIVE

With a career spanning several decades in the information risk and security domain, I have come to appreciate the value of global alignment and coordination within the field, particularly concerning the language we share.

My journey began after transitioning from a microbiology/genetics post-doc in the early 1980s to an initial role as a DEC system/network administrator at a UK pharmaceuticals R&D division. For two decades, primarily in the UK and Europe, I gained extensive, multi-faceted experience in information risk management, technology audit, and information security management within major power generation, defence and financial services companies, providing me with a broad understanding of the challenges and nuances across diverse sectors.

Throughout my career, I have not only witnessed but also contributed, in a small way, to the evolution and maturity of this critical field. Long-term involvement with the committee behind the ISO/IEC 27000 standards has instilled in me a strong preference for pragmatic, real-world solutions in cybersecurity.

Since completing an MBA in 2000 and emigrating to NZ, my focus shifted more towards the governance, management, and strategic aspects, consulting for **S**mall and **M**edium-sized **B**usinesses and running my own micro-business. The challenges of applying security principles in resource-constrained environments have become increasingly evident. Coupled with ever-changing information risks, cybersecurity requires frequent realignment with both overarching business objectives and technology capabilities.

METHODS AND SOURCES

The definitions provided in the hyperglossary represent a synthesis of my professional experience since the 80s, with authoritative sources such as:

- Industry standards and publications (*e.g.* ISO27k and the NIST Cybersecurity Framework).
- Assorted conceptual models and approaches (*e.g.* COBIT and DVMS).
- A bulging home office library with getting on for 200 cybersecurity books to hand and a dozen more in the 'read me' pile for this bookworm.
- Academic research and scholarly articles, plus pieces by professionals in the industry journals.
- Reputable vendor documentation plus marketing materials and market analyst reports.
- Insightful and sometimes provocative contributions from fellow experts through various professional social media platforms (*e.g.* LinkedIn, ISACA Engage, the ISO27k Forum, various blogs plus the SANS, RISKS and CRYPTO-GRAM newsletters).
- Relevant laws and regulations (*e.g.* GDPR and SOC2).
- Practical experience gained through decades of real-world application.

Despite my high ideals and grand expectations, I consider myself a realist and pragmatist. As you will soon see, I favour commonsense explanations reflecting commonplace usage within the field, while also acknowledging the context of more formal definitions where relevant. My aim is to provide definitions that are both accurate and readily understandable for a diverse audience. Please accept my apologies in advance for any misinterpretations: I am entirely human.

STRUCTURE AND USE

By convention, the glossary is organised alphabetically from A to Z, with a few numeric entries (such as 2FA) appearing at the beginning. A typical entry consists of the following:

- Term:
  - The singular cybersecurity-related word, phrase, abbreviation, acronym, or initialism being defined, along with common variants and abbreviations (picked out in **bold**).
  - For the sake of brevity, different word forms of essentially the same term are normally combined under a single entry rather than being listed separately.
- Definition:
  - A reasonably clear and concise plain-English explanation of the term, with links to the definitions of words and phrases elsewhere within the hyperglossary (these are functional hyperlinks in the eBook version). Alternative definitions are provided for terms with distinct meanings, depending on the context in which they are used.
  - Pragmatic guidance, examples, and notes covering various nuances.
  - In *italics*, cited content quoted from definitive references (such as standards) with minor editorial changes in some cases. Rather than citing every term from every reference, I have selected the most appropriate, well-phrased, or definitive ones, sometimes incorporating different interpretations to emphasise other perspectives.
  - 'See also' links to related or similar terms.
  - *'Cf.'* links to distinct, complementary, contrasting, or often-confused terms.
  - 'More info' links to more information on the web.

Check the hyperglossary whenever you encounter unfamiliar cybersecurity terminology. The hyperglossary format is designed for easy browsing with ~39,000 hyperlinks, 99% of which are internal cross-references while the remaining 1% are external/Internet URLs. At times, you will find yourself exploring related concepts at length, flowing intuitively between terms and definitions in the eBook. You may prefer the printed book for ready reference, quiet reflection/self-study, and note-taking.

The uncited definitions and explanations in this hyperglossary (*i.e.* my inputs) are generally valid and applicable within the context of information risk, information security, and related areas. Having *tried* to define terms generically and straightforwardly, based on my knowledge and experience as well as any cited references, I would be flattered if you find my definitions useful enough to share or circulate further. However, if you do, ***please*** **cite this cybersecurity hyperglossary** (with a hyperlink to hyperglossary.com if appropriate), just as I have openly acknowledged my sources.

It is evident from the reference sources that some definitions have been doing the rounds for years, with successive authors adding their spin and occasionally taking off at tangents. With this book, I hope to guide us all gently back in line.

YOUR PART IN THIS UNDERTAKING

To foster a dynamic and collaborative approach to cybersecurity terminology, I have established an online hub for the global community of reader. Our discussion forum (a Google group) is specifically intended to debate the terms and definitions, suggest additions or clarifications, point out errors that ought to be corrected, and offer alternative interpretations. We are keen to share insights into the terminology and its practical application. Connect with your peers and contribute to the collective understanding of cybersecurity language.

Please join us at Hyperglossary.com We are a diverse global group of information risk and security professionals, students, academics, technologists and language experts, standardisers, and others. Participation is free: this is your opportunity to participate and contribute your wisdom to the *next* edition of the hyperglossary.

Future updates to both the print and eBook versions will be informed by the active participation of this community. Working together, I believe we can clarify the jargon, bridge communication gaps, reduce ambiguity (risk!), and foster a more consistent lexicon.

CONCLUDING REMARKS

I invite you to explore this Cybersecurity hyperglossary, engage with the online community, and contribute to its ongoing development. Working together, we can achieve greater clarity and understanding in this vital field. Browse around, think, learn, and join in the debate.

OK, that's more than enough preamble from me.

Go!

Acknowledgements

I am very grateful to the following:

- Everyone who has coined, defined, used, discussed, and refined the *thousands* of terms of art in this book.
- The academics, gurus, practitioners, innovators, and creatives who built and continue driving the field forward.
- My long-suffering wife, family, and friends patiently looking on as I became utterly immersed in this project.
- Colleagues and acquaintances who encouraged me to keep going when the task seemed endless.
- The editorial and production teams from Taylor & Francis who made the dream a reality.
- You, dear reader, in the hope that you will provide constructive feedback via Hyperglossary.com, putting me straight where I got things wrong, suggesting terms and alternative definitions and most of all *using* these terms as defined in your work, edging us ever closer to consensus, productive communications, and genuine understanding.

Thank you one and all.

Dr. Gary Hinson, MBA

The beginning of wisdom
is the definition of terms.

Socrates

Define your terms,
you will permit me again to say,
or we shall never understand one another.

Voltaire

Author Biography

Dr. Gary Hinson, **MBA** is an information security specialist with a particular interest in the human and business aspects of both protecting and exploiting information.

Following an honours degree in genetics at the University of York in 1983, then a PhD and postdoctoral research in molecular biology/microbial genetics at the University of Leicester, I transitioned into my first proper job in 1987. Thanks to some IT experience in connection with the development of DNA fingerprinting, I became a DEC VAX systems and network administrator ('sysmgr') for the research and development arm of Beecham Pharmaceuticals. The commercial value of research information was very evident with heavy investment to develop and protect intellectual property, primarily by legal means (drug patents). At the time, however, the vulnerabilities associated with 'knowledge workers' and the early networks were barely understood and not fully appreciated by management. Management concerns regarding protection of medical, personal and business data were not obvious, at least not to me. As a privileged user deep in the bowels of IT, I had ready access to the databases, applications, drug designs plus medical safety and efficacy studies, even executive emails, with essentially no auditing or oversight. Looking back, we were quite naïve and trusting.

By 1990, I had developed a professional interest in the information risk and security field when it was more commonly known as computer or IT security (pre-dating 'cyber'!). It seemed odd to me that systems and network security was such a low strategic priority with no obvious intent to improve. The research staff and managers had been physically threatened by animal liberation/anti-vivisection activists, indicating (to me) an increased threat elevating the information risks. Management, however, were mostly thinking in terms of perimeter fences and security guards and there were problems there too!

When Beecham was taken over by SmithKline – a much larger US-based pharmaceutical company – we were instructed by senior management simply to join and merge the two sprawling DECnet networks without regard to the information risks that I believed were substantial. Network node *addressing* was a concern but information security was barely an afterthought.

Time to move on.

For more than a decade I learned the ropes in corporate security and audit positions, mostly in the UK and Europe. My work for an electricity company, initially in IT security, was an opportunity to implement BS 7799 protecting both **I**nformation **T**echnology and **O**perational **T**echnology (real-time process control systems, then known as SCADA/ICS) in a critical infrastructure context. I was shoulder-tapped for a move into Internal Audit and an excellent grounding in assurance, governance, strategy and senior management, with an 'executive' (part-time) MBA from the University of Bath in 2000. Leading the UK/European technology audit functions for BAE SYSTEMS and Siemens exposed me to defence, aeroospace and high-tech industries facing their own unique risk, security, governance, compliance and cultural challenges.

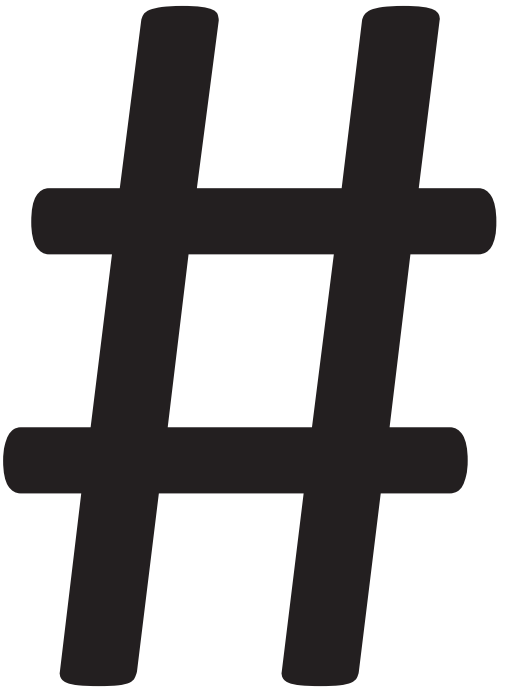
Since 2000, I have been consulting, writing and selling *gigabytes* of information risk and security awareness and training content, policies *etc.,* supporting clients implementing the ISO/IEC 27000 standards and nurturing from scratch the vibrant 5,500-strong "ISO27k Forum". I emigrated to New Zealand in 2005.

As a member of ISO/IEC JTC 1/SC 27, I enjoy contributing to the information security management standards and interacting with hundreds of professional peers. It's good to give something back to the community and stay in touch with innovative approaches.

Now living on a rural farm block near Napier in New Zealand, I have ample opportunity to cogitate on infosec and AI while repairing fences, installing a backup generator, tending to our animals or trout fishing. I love the natural beauty of the NZ countryside, spoilt only by the roar of heavy machinery and chainsaws as the surrounding pine forest is being harvested. Oh and the occasional earthquake or flood - harsh lessons in resilience and the perils of underinvestment in infrastructure being all too evident down here on the Far Side!

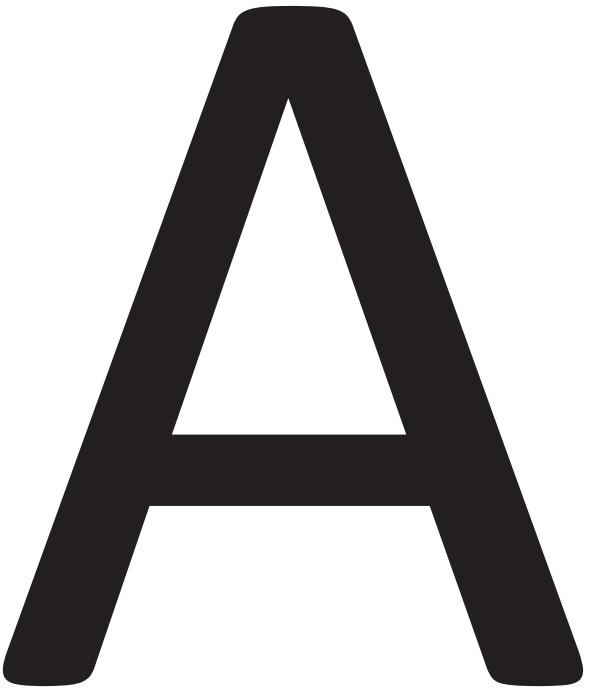
Disclaimer

The information provided within this cybersecurity hyperglossary is intended for general knowledge and informational purposes only. While every effort has been made to ensure accuracy and completeness, the dynamic nature of the cybersecurity field and the potential for differing interpretations mean that errors and omissions are inevitable. The content of this book should not be considered professional advice. You are *strongly* encouraged to verify critical information with authoritative sources and consult with qualified professionals for specific guidance related to your particular circumstances. The author and publisher disclaim any liability for errors or omissions in the content of this hyperglossary or for any actions taken based on the information provided herein.



DOI: 10.1201/9781003650676-1

TERM	MEANING
0-day	*Abbrev:* zero-day.
2FA	*Abbrev:* **two**-**F**actor **A**uthentication.
2G/GSM, 3G/UMTS, 3½G/HSDPA, 4G/LTE, 5G, 6G,…	Second and successive **G**enerations of the cellular digital networks used by devices such as cellphones/smartphones, SMS/TXT messaging, and data communications including mobile Internet access. Defined by the ITU under IMT-2000 and later standards. The 5G standards were introduced in 2017. The 6G standards are under development, with 6G products expected to emerge in 2030–2032. **H**igh-**S**peed **D**ownlink **P**acket **A**ccess (3½G) and earlier services are deprecated with limited use. See also **G**lobal **S**ystem for **M**obile communications, **U**niversal **M**obile **T**elecommunications **S**ystem, **L**ong **T**erm **E**volution.
3DES	*Abbrev:* **triple D**ata **E**ncryption **S**tandard.
3-D Secure	Datacommunications security protocol developed for VISA to protect online transactions involving credit cards. Covers three domains (hence "3-D"): (1) acquirer (bank or credit card company), (2) card issuer, and (3) interoperability (infrastructure). Supersedes **S**ecure **E**lectronic **T**ransaction.
419	Section number of the Nigerian penal code criminalising advance fee frauds. May refer to other social engineering scams as well; hence, email scammers are known colloquially as 419ers.



TERM	MEANING
AAA	*Abbrev:* **A**uthentication, **A**uthorisation, and **A**ccounting.
AAL	*Abbrev:* **A**uthenticator **A**ssurance **L**evel.
A/B testing	Systematic comparison. "A statistical way of comparing two (or more) techniques, typically an incumbent against a new rival. A/B testing aims to determine not only which technique performs better but also whether the difference is statistically significant. A/B testing usually considers only two techniques using one measurement but can be applied to any finite number of techniques and measures" *(ISACA glossary).*
ABAC	*Abbrev:* **A**ttribute-**B**ased **A**ccess **C**ontrol.
***Abbrev*:**	Abbreviation of 'Abbreviation of.' Click any underlined definitions for their entries. Strictly speaking, some are acronyms (such as infosec) or initialisms (such as IT and USB) but for simplicity, *Abbrev:* covers them all.
Abend (abnormal end)	See crash.
Absolute assurance	*Total* certainty, *utter* confidence – a practically unattainable objective. "A level of assurance that is impossible to achieve" (*OCEG GRC Glossary*).
ABUEA	*Abbrev:* **A**ttribute-**B**ased **U**nlinkable **E**ntity **A**uthentication.
Abuse case	Description of unwelcome, inappropriate and potentially malicious computer user interactions with an application, developed to explore the risks and controls. "Describes the intentional and unintentional misuses of the software. Abuse cases should challenge the assumptions of the system design" *(SCP QRG).*
Acceptable **[**or **A**llowable**]** **I**nterruption **W**indow **(AIW)**	Organisation-defined term, *e.g.* this could be the daily time slot during which management accepts the need to suspend locally provided (non-cloud) information services for essential administrative activities such as backups and patching. "The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives" *(ISACA glossary).* See also **M**aximum **T**olerable **O**utage.
Acceptable **U**se **P**olicy **(AUP)**	Policy or guideline laying out and contrasting acceptable against unacceptable use of information, **I**nformation **T**echnology services, systems, networks, *etc.* in plain English for a general audience. "A policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet" *(ISACA glossary).*

TERM	MEANING
Acceptance criteria	Stakeholders' requirements or conditions for taking delivery of and starting to use something, such as a new or modified computer system or information services. Suggests formally specified functional and/or nonfunctional requirements and some form of acceptance test to gain assurance. "Criteria that a solution must satisfy to be accepted by customers" *(ISACA glossary).*
Acceptance statement	"Formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk" *(ISO/IEC 29134:2024).*
Acceptance test	Category/class of tests towards the end of the development phase of the **S**oftware **D**evelopment **L**ife**C**ycle, marking the critical control point as products are handed over from the design and development team to operations and the users or customers. Primarily applies to computer systems, bespoke applications and cloud services, plus other important/valuable products, devices, equipment, facilities, *etc*. Intended to provide assurance to customers, users, or other stakeholders that their requirements, specifications, and expectations have been and will be adequately satisfied or exceeded; hence, the products can be accepted, whether conditionally (*e.g.* subject to any remaining issues being resolved) or unconditionally. "Test of a system or functional unit usually performed by the purchaser on his premises after installation with the participation of the vendor to ensure that the contractual requirements are met" *(ISO/IEC 2382).* "Testing performed to determine whether a customer, acquirer, user, or their designee should accept a solution" *(ISACA glossary).* See also **U**ser **A**cceptance **T**est, **P**roduction **A**cceptance **T**est, **S**ecurity **A**cceptance **T**est.
Accept design option	See risk acceptance. "An intentional design decision to embrace, or concede to the current level of risk, reward, and compliance" *(OCEG GRC Glossary).*
Access, accessible	Capability of a person, computer program, agent, organisation, *etc.* to enter, interact with, and so use (if not misuse and abuse!) a controlled asset such as information, data, a site, building, facility, room, person, system, network, **D**ata**B**ase, file, filing cabinet, folder, disk, other device, or storage media. "Obtain the use of a resource" *(ISO/IEC 2382).* "Ability of the rights holders to use or benefit from a certain service or product. Note: Restrictions can be caused by distance to the source (*e.g.* water supply network does not reach a certain neighbourhood) or unaffordability (*e.g.* service is too costly for a certain household or group of people), among other reasons" *(ISO 22300).* See also accessibility.

TERM	MEANING
Access authority	Organisation, department, person, system, program, or function that determines whether to grant (permit) or deny (refuse) access to one or more controlled information assets such as personal information. "An entity responsible for monitoring and granting access privileges for other authorized entities" *(CNSSI 4009).*
Access card, proximity card, pass card, access badge, staff pass, ID card, RFID (Radio Frequency IDentification) tag, …	Authentication device that (normally) communicates wirelessly with a card reader (normally) located at an access-controlled door or gate to determine whether the expected cardholder is authorised to proceed. Vulnerable to being lost, stolen, or handed to someone else, and perhaps cloned or hacked. Often carries the authorised holder's photograph as well, giving vigilant and diligent security guards, receptionists, and other workers the chance to determine at a glance whether the person presenting, wearing, or using the card resembles the mugshot (assuming they have not simply replaced the photo or faked the entire pass).
Access control, access-control	Control designed to mitigate unacceptable risks by restricting access to one or more assets, permitting authorised and appropriate access whilst preventing unauthorised or inappropriate access. May be physical (such as a lock), electronic/digital (such as encryption), or procedural (such as a nightclub bouncer checking the VIP guest list). Often critically or vitally important, implying the need for strong assurance that the control is correctly specified, designed, implemented, configured, operating, managed, maintained, and governed. "Means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways" *(ISO/IEC 2382).* "Means to ensure that physical and logical access to assets is authorized and restricted based on business and information security requirements" *(ISO/IEC 27002).* "The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises" *(ISACA glossary).* "The process of granting or denying requests for access to systems, applications and information. It can also refer to the process of granting or denying requests for access to facilities" *(NZISM).* "Ensures that resources are only granted to those users who are entitled to them" *(SANS glossary).*
Access Control Facility № 2 (ACF2)	Mainframe user authentication, access control, and auditing application for IBM z/OS and z/VM **O**perating **S**ystems. See also RACF.

TERM	MEANING
Access **C**ontrol **L**ist **(ACL), access control table**	Security metadata associated with a computer file, folder, disk, port, *etc.* typically specifying which users may or may not access or change the object's security settings, in what manner, under what conditions, and whether successful and/or unsuccessful attempts to do so are logged. ACL capabilities and functions vary between **O**perating **S**ystems. "An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals" *(ISACA glossary).* "A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource" *(SANS glossary).* See also access list.
Access **C**ross **D**omain **S**olution **(ACDS)**	"A system permitting access to multiple security domains from a single client device" *(AusISM).*
Access gateway	"An architectural construct that provides the system user access to multiple security domains from a single device, typically a workstation" *(NZISM).*
Accessibility	Ease of use, particularly for people coping with disabilities. Physical and mental issues (such as poor or no vision or hearing, dyslexia, illiteracy, Parkinsonism, cerebral palsy, weakness, loss or inability to control limbs, dementia, colour blindness, and epilepsy) can make interacting with, controlling and using computer systems more challenging than for able-bodied people.
Access list	In conjunction with access controls, specifies who or what can or cannot access a controlled resource, possibly with additional criteria such as time and type of access permitted or denied, *e.g.* the nightclub doorman's VIP guest list. "List of entities, together with their access rights, that are authorized to access a resource" *(ISO/IEC 2382).* See also **A**ccess **C**ontrol **L**ist, access policy.
Access management	Directing, planning, organising, leading, and controlling activities involved in determining who is permitted or forbidden specified modes and means of access to information, systems, facilities, *etc.* May include defining and/or applying access rules and control requirements, dealing with conflicts and changes, analysing logs, monitoring and responding to issues, alarms or alerts, testing and maintaining the controls. "Maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation" *(SANS glossary).*

TERM	MEANING
Access matrix	Table relating individual computer users or rôles (on one axis) to the computer systems, application functions, and/or classes of data (on the other axis), showing the types of access permitted and/or denied (within the body of the table). "Uses rows to represent subjects and columns to represent objects with privileges listed in each cell" *(SANS glossary).*
Access method	How access to a controlled resource is obtained, *e.g.* physical, online, illicit, official. "The technique used for selecting records in a file, one at a time, for processing, retrieval or storage. The access method is related to, but distinct from, the file organization, which determines how the records are stored" *(ISACA glossary).*
Access path	"The logical route that an end user takes to access computerized information. Note: Typically includes a route through the operating system, telecommunications software, selected application software and the access control system" *(ISACA glossary).*
Access permission	"All of a subject's access rights with respect to some object" *(ISO/IEC 2382).* See also access right.
Access Point **(AP), W**ireless **A**ccess **P**oint**, Wi-Fi A**ccess **P**oint **(WAP)**	Network router providing Wi-Fi services. "A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network" *(NIST SP 800-48 and SP 800-121).* "Device or piece of equipment that allows wireless devices to connect to a wired network. Note: The connection uses a wireless local area network (WLAN) or related standard" *(ISO/IEC 27033-6).* "A point that accesses the network" *(ISACA glossary) (!).*
Access **P**oint **N**ame **(APN)**	Gateway linking a mobile network to the Internet or another network. Malware may surreptitiously alter the APN on mobile devices, redirecting users to access points monitored and controlled by hackers.
Access policy, access control policy	Security policy or a set of defined rules determining authorised and controlled access to information assets such as functions, tables, or records in a **D**ata**B**ase, or programs, files, and folders on a computer system on a network, or the facilities housing such assets. Typically used to develop an access list and configure access controls to achieve appropriate access rights (*e.g.* read, write, delete, and/or control) for user rôles which are then assigned to individual users authorised to perform those rôles. See also **R**ôle-**B**ased **A**ccess **C**ontrol, access matrix.

TERM	MEANING
Access right	Individual people, systems, programs, organisations, *etc.* may be granted or denied access to controlled assets such as data, transactions/functions, or physical locations according to whether the access is authorised, *i.e.* their logical access rights, permissions, or attributes match the access rules or criteria associated with those assets according to the access policy. May be documented in the form of an access matrix or permit. "Permission for a subject to access a particular object for a specific type of operation. Example: Permission for a process to read a file but not write to it" *(ISO/IEC 2382).* "The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy" *(ISACA glossary).* See also right, access permission.
Access risk	Uncertain possibility and consequences of access to information assets, particularly unauthorised or inappropriate access. "The risk that information may be divulged or made available to recipients without authorized access from the information owner, reflecting a loss of confidentiality" *(ISACA glossary).*
Access to personal information	Access to personal information. "The ability to view personal information held by an organization. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals need to be able to find out what personal information an entity has on file about them and how the information is being used. Individuals need to be able to correct erroneous information in such records" *(**T**rust **S**ervices **C**riteria).*
Accident	While information security incidents may result from deliberate acts by hackers, malware, fraudsters, spies, *etc.,* the greater proportion by number are in fact the result of inadvertent or unintentional acts, natural or chance events, or errors. Physical accidents (health and safety failures) and illnesses that befall workers may qualify as information security incidents since people are information assets.
Accommodation address	Mail drop postal address used for convenience and sometimes to conceal the true location/identity of a fraudster by giving the appearance of belonging to a legitimate business or an innocuous member of the public.

TERM	MEANING
Account	a. *[Noun]* Computer user profile or userID. b. *[Noun]* Financial ledger. c. *[Noun]* Descriptive report or story (as in 'an account of the proceedings'). d. *[Noun]* Something to be considered or borne in mind (as in 'taken into account'). e. *[Verb]* To explain, justify or excuse something (as in 'call to account' in accountability). f. *[Verb]* To record something in the books (as in 'account for' in accounting).
Account harvesting	"Process of collecting all the legitimate account names on a system" *(SANS glossary).*
Account hijack, account takeover	Taking control of a target's bank, credit card, email, computer, or other account by means of hacking, social engineering, malware, or coercion*,* typically as part of identity fraud or some other attack.
Account number	See **P**rimary **A**ccount **N**umber.
Accountability	Being accountable. In contrast to responsibility and authority, this sticky property cannot be unilaterally delegated or passed by the accountable person or organisation to another; in other words, **the buck stops here**. "Property that ensures that the actions of an entity may be traced uniquely to that entity" *(ISO/IEC 2382).* "State of being accountable. Notes: Accountability relates to an allocated responsibility. The responsibility can be based on regulation or agreement or through assignment as part of delegation. For systems, accountability is a property that ensures that actions of an entity can be traced uniquely to the entity. In a governance context, accountability is the obligation of an individual or organization to account for its activities, for completion of a deliverable or task, accept the responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner" *(ISO/IEC TS 5723).* "State of being accountable. Notes: Accountability relates to an allocated responsibility. The responsibility can be based on regulation or agreement or through assignment as part of delegation. Accountability involves a person or entity being accountable for something to another person or entity, through particular means and according to particular criteria" *(ISO/IEC 22989).* "The ability to map a given activity or event back to the responsible party" *(ISACA glossary).*

TERM	MEANING
Accountability of governance	"The ability of governance to ensure that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritization and decision making; and monitoring performance, compliance and progress against plans. In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson" *(ISACA glossary).*
Accountable	Someone (a person or organisation) who is held/called to account by an authority for a failure (such as a privacy breach or some other incident) is formally required to explain their part in the failure. They may be sanctioned or penalised in some way (disciplinary action, dismissal, prosecution, fine, restriction or withdrawal of privileges, additional oversight, *etc.*), if the authority determines that they did not adequately fulfil their obligations. "Required or expected to justify actions or decisions; being answerable and responsible for those actions & decisions" *(NZISM).* "Answerable for actions, decisions and performance" *(ISO/IEC 22989)*.
Accountable material	"Requires the strictest control over its access and movement. Includes TOP SECRET data, some types of caveated data and any data designated as accountable material by its originator" *(AusISM).*
Accountable party	The person or organisation held to account. "The individual, group or entity that is ultimately responsible for a subject matter, process or scope" *(ISACA glossary)*.
Accounting	Principles and practices of systematically, formally, and thoroughly recording and cross-checking various details such that relevant parties can be held to account for their activities. Most **I**nformation **T**echnology systems, for instance, can automatically record information about user logons, use of privileges and overrides, alerts, alarms and other potentially significant events in their logs or accounting files, with utilities to search and report on them, even if these days the details are no longer needed to recharge users for their use of the computers (common practice prior to the 1990s).
Accreditation	Process of verifying that an organisation or individual is competent to check/audit and certify others, to a level of assurance required by a trusted authority acting on behalf of stakeholders. "A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system and issues a formal approval to operate the system" *(NZISM)*. *Cf.* certification.

TERM	MEANING
Accreditation authority	"The authoritative body or individual responsible for systems accreditation" *(NZISM)*.
Accuracy, accurate	Truthful and valid, faithfully representing factual objective reality. An integrity property. "Measure of closeness of results of observations, computations, or estimates to the true values or the values accepted as being true" *(ISO 17572-1)*. "Quality of that which is free of error [and/or] qualitative assessment of freedom from error, a high assessment corresponding to a small error [and/or] quantative measure of the magnitude of error, preferably expressed as a function of the relative error, a high value of this measure corresponding to a small error" *(ISO/IEC 2382)*. "The fraction of predictions that a classification model predicted correctly. In multiclass classification, accuracy is defined as correct predictions divided by total number of examples. In binary classification, accuracy is defined as true positives plus true negatives divided by total number of examples" *(ISACA glossary)*. "Ability to get the true result. For quantitative tests, the accuracy expresses the closeness of agreement between the true value and the value obtained by applying the test procedure a number of times" *(FSRCoP)*. *Cf*. precision.
ACD	*Abbrev:* **A**ctive **C**yber **D**efence.
ACF2	*Abbrev:* **A**ccess **C**ontrol **F**acility № **2**.
ACKnowledgement **(ACK)**	Positively recognise and accept/agree that something is valid, true, legitimate, authentic, *etc*. "Affirmative response, by a receiver, to a sender, indicating that transmitted data have been received" *(ISO/IEC 2382)*. "A flag set in a packet to indicate to the sender that the previously sent packet was accepted correctly by the receiver without error or that the receiver is now ready to accept a transmission" *(ISACA glossary)*.
ACL	*Abbrev:* **A**ccess **C**ontrol **L**ist.
ACME	*Abbrev:* **A**utomated **C**ertificate **M**anagement **E**nvironment.
ACPO guidelines	Influential ACPO Good Practice Guide for Digital Evidence offered succinct, pragmatic guidance for UK police gathering digital forensic evidence, last updated by the **A**ssociation of **C**hief **P**olice **O**fficers in 2011. Built on four basic principles: "(1) No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court; (2) In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions; (3) An audit trail or

TERM	MEANING
	other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result; (4) The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to." Superseded by the **F**orensic **S**cience **R**egulator's **C**ode **o**f **P**ractice. See also ISO/IEC 27050 standards.
Acquirer	Person or organisation that purchases, obtains, receives, or is given something. "Stakeholder that procures a product or service from another party. Note: Procurement may or may not involve the exchange of monetary funds" *(ISO/IEC 27036-1)*. "The stakeholder who obtains a solution from a supplier" *(ISACA glossary)*.
Acquisition	Initial phase or activity in the process of gathering, analysing, and presenting forensic evidence, or the act of acquiring something. "Process of creating a copy of data within a defined set. Note: The product of an acquisition is a potential digital evidence copy" *(ISO/IEC 27037)*. "A process by which digital evidence is duplicated, copied, or imaged" *(NIST SP 800-101)*. "Process for obtaining a product or service" *(ISO/IEC 27036-1)*. "The process of obtaining solutions by establishing and executing supplier agreements" *(ISACA glossary)*.
ACS	*Abbrev:* **A**utomation and **C**ontrol **S**ystem.
ACSC	*Abbrev:* **A**ustralian **C**yber **S**ecurity **C**entre.
Action	Activity, act, movement, reactions, response, *etc*. "The mechanism by which the agent transitions between states of the environment in reinforcement learning. The agent chooses the action by using a policy" *(ISACA glossary)*. "An act taken against an Asset by a Threat Agent. Requires first that contact occurs between the Asset and Threat Agent" (*O-RT*).
Actions & control	"A specific way, usually used in combination, that an organization addresses risk, reward, and compliance" *(OCEG GRC Glossary)*.
Activation function	"Function applied to the weighted combination of all inputs to a neuron. Note: Activation functions allow neural networks to learn complicated features in the data. They are typically non-linear" *(ISO/IEC 22989)*.
Active code	"Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)" *(SANS glossary)*.

TERM	MEANING
Active **C**yber **D**efence **(ACD)**	Adaptive mechanisms defending against network security threats. "Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities" *(CNSSI 4009)*. "Helps organisations to find and fix vulnerabilities, manage incidents or automate disruption of cyber-attacks. Some services are designed primarily for the public sector, whereas others are made available more broadly to private sector or citizens, depending on their applicability and viability" *(UK National Cyber Security Strategy 2022)*.
Active **D**irectory **(AD)**	Microsoft's architecture to administer and control network resources (computers, user IDentities, groups, *etc*.) through a hierarchical directory structure. Resource collections are organised into domains under **D**omain **C**ontrollers. Domains can be associated into trees, and large organisations may have forests of trees. AD authenticates and authorises access to resources in the directory, using several protocols and sets of rules called **G**roup **P**olicy **O**bjects. See also **AD D**omain **S**ervices, **AD L**ightweight **D**irectory **S**ervices, **AD F**ederation **S**ervices, **AD C**ertificate **S**ervices, Microsoft Entra ID.
Active **D**irectory **C**ertificate **S**ervices **(AD CS)**	Digital certificate management services provided by a Windows server for **A**ctive **D**irectory.
Active **D**irectory **D**omain **S**ervices **(AD DS)**	Directory services associated with a Microsoft **A**ctive **D**irectory network, used to locate resources within the local domain and other domains through the global catalogue. Automatically replicated across **D**omain **C**ontrollers for resilience. Critically important domain-related data (such as passwords) are stored in a **D**irectory **I**nformation **T**ree file called, by default, %SystemRoot%\NTDS\ntds.dit. This is obviously enough a bullseye triple-word-score lottery-win diamond-studded flag for hackers actively targeting an organisation's Microsoft network, with hacking and administrative tools available to facilitate compromise.
Active **D**irectory **F**ederation **S**ervices **(AD FS)**	Proprietary Microsoft technology blending **L**ightweight **D**irectory **A**ccess **P**rotocol with **S**ecurity **A**ssertion **M**arkup **L**anguage for **I**dentification **& A**uthentication, authorisation, and access control purposes including **S**ingle **S**ign **O**n within **A**ctive **D**irectory. See also Microsoft Entra ID.
Active **D**irectory **L**ightweight **D**irectory **S**ervices **(AD LDS)**	Described by Microsoft as an 'independent mode of **A**ctive **D**irectory' providing directory services for networked applications, based on **L**ightweight **D**irectory **A**ccess **P**rotocol.
Actively exploited vulnerability	"A vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner" *(EU CRA)*.

TERM	MEANING
Active **M**anagement **T**echnology **(AMT)**	Hardware subsystem incorporated into some Intel **C**entral **P**rocessing **U**nit chips to facilitate low-level system management. In 2017, Intel disclosed a design flaw in AMT with severe vulnerability allowing hackers to gain privileged access to systems using the "Q series" chipset, either locally or through the network. Begs questions about the wisdom of allowing low-level privileged system management in this way, through hardware that bypasses normal **U**nified **E**xtensible **F**irmware **I**nterface and **O**perating **S**ystem security (a backdoor), and why this design was ever approved.
Active recovery site (mirrored)	"A recovery strategy that involves two active sites, each capable of taking over the other's workload in the event of a disaster. Note: Each site will have enough idle processing power to restore data from the other site and to accommodate the excess workload in the event of a disaster" *(ISACA glossary)*.
Active response	"A response in which the system either automatically, or in concert with the user, blocks or otherwise affects the progress of a detected attack. Note: Takes one of three forms: amending the environment, collecting more information or striking back against the user" *(ISACA glossary)*.
Active shooter, active killer	Well-armed suicidal terrorist or brutally unhinged nutcase who indiscriminately and violently attacks innocent people with intent to injure or kill as many as possible before being arrested, disarmed, disabled, or killed. An extreme safety threat (danger) to everyone in the vicinity.
ActiveX	Deprecated Microsoft technology for interactive web pages. Malicious ActiveX controls (a form of malware) may potentially compromise the users' systems, *e.g.* if the browser security settings allow, even unauthenticated ('unsigned') ActiveX controls may access files on the user's hard drive. Microsoft dropped Active X support from its browsers in 2016.
Activist	Relatively mild extremist.
Activity monitor	"Aims to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible" *(SANS glossary)*.
Actor	a. Performer in stage plays, films, and TV shows, *e.g*. Arnold Schwarzenegger, Anthony Hopkins, Greta Garbo, … b. "Entity that fills a thematic role in a script. Examples: An agent, a co-agent, a beneficiary, a patient" *(ISO/IEC 2382)*. "Organization or individual that fulfils a role" *(ISO 23234)*. See also bad actor.

TERM	MEANING
Actuary	Insurance professional who uses probability theory and advanced mathematical/statistical techniques to analyse data and so quantify, and hence manage risk with scientific rigour.
Actuating function	Functional part of an application, system, or organisation which can command an actuator.
Actuator	Mechanical device that acts (moves, applies force) when commanded, such as a solenoid, stepper motor, or motorised arm that opens or closes a valve. "A device component responsible for enacting physical changes within an environment, *e.g.*, relays, solenoids, switches" *(ISACA glossary)*.
Acunetix	Commercial penetration testing/hacking tool. An example of dual-use technology, popular with black, grey, and white hats. More info: https://www.acunetix.com/
Acute risk	"Time-bound, discrete events, for example a major fire or a terrorist attack. Contrast with chronic risks" *(UK Resilience Lessons Digest 2023)*. *Cf.* chronic risk.
AD	*Abbrev:* **A**ctive **D**irectory.
Adaptive **Grad**ient **(AdaGrad)**	**A**rtificial **I**ntelligence/**M**achine **L**earning algorithm that dynamically adjusts the learning rate for each parameter. "A sophisticated gradient descent algorithm that rescales the gradients of each parameter, effectively giving each parameter an independent learning rate" *(ISACA glossary)*.
Adaptive authentication	"This varies the level or degree of authentication required where unusual login requests occur. For example, out of normal hours, from an unusual geolocation, from an unknown device and so on. When an unusual authentication request is received, Adaptive Authentication may request additional credentials such as a one-time code provided to a known mobile phone number" *(NZISM)*.
ADCON	Military term meaning the combination of manual control with management control. *Cf.* administrative control.
AD CS	*Abbrev:* **A**ctive **D**irectory **C**ertificate **S**ervices.

TERM	MEANING
Address	a. *[Verb]* To take account of, work on, deal appropriately with, tackle, fix, *etc*. b. *[Noun]* Identifies the source and destination of datacommunications messages (see network address) or the physical place on Earth where a person lives or a premises is located (postal address), allowing messages, letters, and parcels to be routed accordingly and delivered. c. *[Noun]* Specified location in computer memory, a specific cell in a spreadsheet, *etc*. d. *[Noun]* Speech, monologue, soliloquy, lecture, or sermon.
Addressing	a. Assigning/allocating or using an address. "The method used to identify the location of a participant in a network. Note: Ideally, specifies where the participant is located rather than who they are (name) or how to get there (routing)" *(ISACA glossary)*. b. The act of taking account of, working on, dealing appropriately with, tackling, fixing, *etc*.
Addressing exception	Addressing exception. "An exception that occurs when a program calculates an address that is outside the bounds of the storage that is available to the program" *(ISACA glossary)*.
Address **R**esolution **P**rotocol **(ARP)**	"A protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions" *(SANS glossary)*.
Address space	The maximum number of addresses that can be uniquely identified with a given addressing protocol, *e.g.* an 8-bit computer processor with an 8-bit addressing bus can natively address just 2^8 (*i.e*. 256) memory locations, each containing an 8-bit byte, without special technical arrangements to extend or concatenate registers and thus address additional memory locations. "The number of distinct locations that may be referred to with the machine address. Note: For most binary machines, it is equal to 2^n, where n is the number of bits in the machine address" *(ISACA glossary)*.

TERM	MEANING
Address **S**pace **L**ayout **R**andomisation **(ASLR)**	Security technique that pseudorandomises memory addressing for processes, function calls, *etc.,* frustrating hacking attempts to invoke or replace privileged functions occupying fixed and hence predictable addresses through buffer overflows and similar exploits. See also **K**ernel **A**ddress **S**pace **L**ayout **R**andomisation.
AD DS	*Abbrev:* **A**ctive **D**irectory **D**omain **S**ervices.
Adequate security	Control arrangements deemed or believed sufficient to achieve and maintain an acceptable level of risk. May yet turn out to be inadequate or excessive under various circumstances. "Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls" *(OMB Circular A-130)*.
AD FS	*Abbrev:* **A**ctive **D**irectory **F**ederation **S**ervices.
Ad hoc test	See unstructured test.
Ad injection	Browser malware that displays advertisements and (in some cases) steals personal information from infected systems. See also adware, Cross-Site Scripting, HTML injection.
AD LDS	*Abbrev:* **A**ctive **D**irectory **L**ightweight **D**irectory **S**ervices.
Administration **(admin), administrator, administrative, administer**	The operational donkey-work of management involving network, systems, security, project, team, group, department, and other technology and business administration. Keeping things in good order, running smoothly, is an essential yet often undervalued and thankless rôle, without which entropy rules, routine processes soon fall apart and chaos reigns.
Administrative access	Privileged account or access right allowing administrators to perform administrative activities. "Elevated or increased privileges granted to an account for that account to manage systems, networks and/or applications. Administrative access can be assigned to an individual's account or a built-in system account" *(ISACA glossary)*.

TERM	MEANING
Administrative account	Administrative userID, usually a privileged user account, sometimes a privileged non-interactive ID to perform autonomous activities such as routine backups. "A user account with full privileges on a computer. Such an account is intended to be used only when performing personal computer (PC) management tasks, such as installing updates and application software, managing user accounts, and modifying operating system (OS) and application settings" *(NIST SP 800-114)*. "Dedicated accounts with escalated privileges and used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Common administrator account subtypes include root accounts, local administrator and domain administrator accounts, and network or security appliance administrator accounts" *(CIS Controls)*.
Administrative control	Control associated with, involving or integral to administrative activities such as computer system, network, or application management, *e.g.* the account administration processes for authorising and assigning applicable access rights to rôles, then allocating relevant rôles to the users. "The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies" *(ISACA glossary)*. *Cf.* ADCON.
Admissible	Forensic evidence including analytical findings and expert witness testimony *must* be trustworthy if it is to be presented in court. Dubious evidence (*e.g.* if there is good reason to suspect or believe that it was *not* in fact properly collected, stored, and analysed in full accordance with applicable laws/regulations and standards of good forensic practice) may be ruled inadmissible by the judge, in which case it cannot be used in court to support or refute a case.
ADP	*Abbrev:* **A**dvanced **D**ata **P**rotection.
ADS	*Abbrev:* **A**lternate **D**ata **S**tream.
Advanced **D**ata **P**rotection **(ADP)**	Apple's proprietary end-to-end encryption scheme.
Advanced **E**ncryption **S**tandard **(AES), AES-128, AES-256**	**N**ational **S**ecurity **A**gency-approved cryptographic algorithm replaced **D**ata **E**ncryption **S**tandard. Specified in the standard FIPS 197 with 128- or 256-bit keys. A symmetric cryptography block cipher strong enough for TOP SECRET classified information, although widespread distrust of the NSA following Ed Snowden's revelations casts doubt on that assertion/belief, and there are even stronger algorithms for US military/governmental use. "A public algorithm that supports keys from 128 bits to 256 bits in size" *(ISACA glossary)*.

TERM	MEANING
Advanced **K**ey **P**rocessor **(AKP)**	"A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to 1) exchange information with a client platform, 2) interact with fill devices, and 3) connect a client platform securely to the primary services node (PRSN)" (*CNSSI 4009*).
Advanced **P**ersistent **T**hreat **(APT)**	Highly sophisticated, sustained, and ultimately damaging cyberattack, or a campaign involving a series of attacks, by a very resourceful, determined, and capable adversary, typically cyber-spooks. Generally involves a combination of methods and tools, such as custom malware, social engineering, hacking (including hacked hardware, software, or firmware, including *things*), and/or physical intrusion. Aside from the extreme technical challenges of characterising and understanding APTs, tracing and attributing their sources and even consistently naming the variants and the associated originators is tricky (something a crowdsourced APT spreadsheet addresses). "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (*e.g.*, cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives" *(NIST SP 800-39)*. See also APT#.
Advance fee fraud	Type of fraud/social engineering in which the fraudster fools a naïve and vulnerable victim into sending money as 'advance fees' supposedly in order to secure a substantial pay-out (such as an inheritance or lottery win) or other benefit (such as an immigration visa) which, strangely enough, gets tantalizingly close but never quite materialises. Commonly known as a 419 scam. Originally perpetrated by letter, Telex, and FAX, latterly by email, SMS/TXT messaging, social media, *etc*.
Adversarial **E**xample **(AE)**	Image constructed specifically to mislead or deceive an **A**rtificial **I**ntelligence machine vision system into misclassifying the subject (such as mis-identifying a camouflaged enemy tank as a bush).

TERM	MEANING
Adversary, adversarial, enemy, malicious actor	Deliberate threat agent, *i.e*. a malicious organisation, people, or person (such as hackers, cybercriminal gangs, competitors, workers, fraudsters, VXers, lobbyists, rumour-mongers, saboteurs/cyberteurs, pressure groups, snoops, spooks, or terrorists) intent on attacking, compromising, exploiting, and perhaps harming the target in some way. "A threat agent" *(ISACA glossary)*.
Advisory service, consulting service	Provision of advice and guidance to clients by specialists. "Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes, systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls" *(IIA GIAS)*.
Adware	Annoying, distracting software that displays advertisements, *etc*. Considered by some to be malware since it is often covert, seldom knowingly authorised, consumes storage and processing capabilities, and may have undesirable side-effects. "A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used. Note: In most cases, this is done without any notification to the user or without the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and it provides the user with a specific service" *(ISACA glossary)*. See also ad injection, ransomware, crimeware, scareware, spouseware, stalkerware, spyware.
Adwind, AlienSpy, Frutas, Unrecom, Sockrat, JSocket, jRat	Heavily obfuscated species of **R**emote **A**ccess **T**rojan malware available to rent on the black market (**M**alware-**a**s-**a**-**S**ervice). Java-based, hence capable of executing on many **I**nformation **T**echnology platforms. Frutas emerged in 2012 and variants were still in the wild 6 years later.
AE	*Abbrev:* **A**dversarial **E**xample.
AES	*Abbrev:* **A**dvanced **E**ncryption **S**tandard.

TERM	MEANING
Affirmation	Formal attestation, statement, or claim confirming something. "A written or oral statement confirming implementation, or lack of implementation, of processes that meet the intent and value of one or more model practices. Affirmations must be provided: By people who have a process role that involves implementing, following, or supporting processes; In an interactive forum where the appraisal team has control over the interaction Examples of affirmations: Oral affirmations include: interview responses, presentations, and demonstrations, and can include responses to questions on white boards, Skype/Instant Message chat boards, *etc*. Written affirmations include: emails, instant messages, and data contained in systems, documents" *(ISACA glossary)*.
Affirmative cyber risk	Cyber incidents *explicitly* covered in cyberinsurance or other forms of insurance. *Cf.* non-affirmative cyber risk.
After-action report, final exercise report	"Document that records, describes and analyses the actual disruption or exercise, drawing on debriefs and reports from observers, and derives lessons from it. Note: The after-action report documents the results from the after-action review" *(ISO 22300)*.
After **F**irst **U**nlock **(AFU)**	State of a mobile phone after the user has authenticated and unlocked it at least once by entering a PIN code, pattern, or biometric. In this state, the device **O**perating **S**ystem dynamically decrypts files and enables functions and features (such as the camera) that were automatically disabled **B**efore **F**irst **U**nlock, facilitating extensive data access by the user … and potentially by forensic analysts or hackers.
Agency	a. *[Adjective]* Self-determination, the capability of a person or organisation to act independently in their own interest, controlling their own activities, decisions, and environment, free of undue influence or constraint. *Cf.* agent. b. *[Noun]* Part of government. "Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency" *(NIST SP 800-171)*. "New Zealand Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the Public Service Act" *(NZISM)*.
Agency control	Agency control. "This description applies where an Agency has direct control of agency information systems and data. It follows that Non-Agency Control occurs where direct control is impaired or does not or cannot exist" *(NZISM)*. *Cf.* non-agency control.
Agency head	"The government employee with ultimate responsibility for the secure operation of agency functions, whether performed inhouse or outsourced" *(NZISM)*.

TERM	MEANING
Agent	a. Person who somehow (usually covertly, hence 'secret agent') obtains legitimate access to confidential proprietary or personal information but betrays their position of trust by disclosing or permitting access to the information by an unauthorised third party, typically through a collector. See also spy. b. Benign or malicious program, person or organisation acting on behalf of or representing another, *e.g.* gathering and passing on data from one system or network for collation and analysis centrally in conjunction with data fed by agents elsewhere, a custodian or steward holding and protecting information assets, or a 'go-between' facilitating recruitment, property sales, or business deals. "In artificial intelligence (AI), an autonomous program or system designed to perceive and interact with its environment to make decisions and take actions to achieve specific goals. Also referred to as an intelligent agent" *(ISACA glossary)*. *Cf*. agency.
Agentic Artificial **I**ntelligence **(Agentic AI), intelligent agent**	**A**rtificial **I**ntelligence architecture involving distributed intelligent semi- or fully autonomous, self-learning agents, taking rational decisions and acting on behalf and in the interests of their owners/controllers according to their local circumstances.
Agent provocateur	French term literally translated as 'agent who provokes,' such as a secret agent (spy, mole) who infiltrates an organisation and incites or causes them to act illegally or inappropriately in such a way that they are likely to be caught in the act. A cyberteur.
AGI	*Abbrev:* **A**rtificial **G**eneral **I**ntelligence.
Agile, agile development	Software engineering approach involving making frequent small/incremental/evolutionary changes (iterations or sprints) to a production system, with rapid user/customer feedback after each release directing the next round. "A development methodology that uses an iterative approach to deliver solutions incrementally through close collaboration and frequent reassessment" *(OMB Circular A-130)*. "A methodology of adopting flexible, adaptable and iterative processes" *(ISACA glossary)*. "Evidence that the organization can respond quickly and positively to changes and stress" (*OCEG GRC Glossary*). See also **R**apid **A**pplication **D**evelopment, **C**ontinuous **D**evelopment, DevOps.
Aggregation	Collection and collation of information from disparate sources. Due to explicit and/or inferred relationships between aggregated items, analysis can reveal structures and new knowledge; hence, **D**ata**B**ases are usually more valuable than the data items they contain: the whole is greater than the sum of the parts. "Acquisition of sensitive information by collecting and correlating information of lesser sensitivity" *(ISO/IEC 2382)*. "A term used to describe compilations of data that may require a higher level of protection than their component parts" *(AusISM)*.

TERM	MEANING
Agreement	Joint commitment of two or more parties to a common objective. "Mutual acknowledgement of terms and conditions under which a working relationship is conducted" *(ISO/IEC 27036-1)*.
AgriTech, AgroTech, AgTech	Contractions of **agri**cultural **tech**nology, particularly the development and exploitation of innovative **I**nformation **T**echnology within farming and the agricultural industry/sector. See also Biotech, EdTech, FinTech, FoodTech, GovTech, EcoTech/GreenTech, HealthTech, LegalTech, RegTech, RetailTech, and other tech neologisms.
AH	*Abbrev:* **A**uthentication **H**eader.
AI	*Abbrev:* **A**rtificial **I**ntelligence.
AI agent	**A**rtificial **I**ntelligence agent. "Automated entity that senses and responds to its environment and takes actions to achieve its goals" *(ISO/IEC 22989)*.
AI Auditor	ISACA's qualification for **I**nformation **T**echnology auditors, risk and compliance analysts auditing **A**rtificial **I**ntelligence systems. More info: https://www.isaca.org/credentialing/aaia
AI component	Component of an **A**rtificial **I**ntelligence system. "Functional element that constructs an AI system" *(ISO/IEC 22989)*.
AICPA	*Abbrev:* **A**merican **I**nstitute of **C**ertified **P**ublic **A**ccountants.
AIGP	*Abbrev:* **A**rtificial **I**ntelligence **G**overnance **P**rofessional.
Aircrack ng	Wi-Fi network hacking and penetration testing tool, capable of cracking WEP, WPA, and WPA2/PSK.
AirCyber	Initiative from BoostAeroSpace SAS spreading security awareness and good practices through the aerospace and defence industry, with conformity assessments and certification aimed at small to medium-sized suppliers for Airbus and its European partners. More info: https://boostaerospace.com/aircyber/
Air gap	Complete physical and logical separation between entities, *e.g.* isolating highly secure networks from less-secure ones by prohibiting any connections or information transfers between them. Tends to fail-insecure; in other words, if the air gap is somehow breached, the construct may be highly vulnerable if excessive trust (faith) or reliance was placed on the air gap. See also data diode.
Air lock, air-lock, airlock	See man-trap.
AI system impact assessment	Analysis of the potential effects, consequences, or value of an **A**rtificial **I**ntelligence system. "Formal, documented process by which the impacts on individuals, groups of individuals, or both, and societies are identified, evaluated and addressed by an organization developing, providing or using products or services utilizing artificial intelligence" *(ISO/IEC 42001)*.

TERM	MEANING
AKP	*Abbrev:* **A**dvanced **K**ey **P**rocessor.
Alarm	Audio/visual warning of the occurrence of a critical security and/or vital safety condition or incident requiring an urgent, high-priority response (*e.g.* fire/smoke, intruder, flood, or a gross system integrity, brake or control failure). See also alert.
Alarm system	System comprising one or more types of alarms/alerts, *e.g.* intruder/security alarms, fire/smoke alarms, industrial process alarms, electrical alarms. May interface with building management or other systems for coordinated/consolidated monitoring and control, particularly in complex safety-critical environments such as factories and prisons.
Alert	a. *[Noun]* Warning indication that a security event (*e.g.* audit or security log file full, system shutdown initiated, user authentication failure, access-controlled door held open) has occurred. While definitions vary, alerts *generally* signal important warnings but not necessarily critical or vital conditions requiring less urgent responses than alarms. They are usually logged for analysis and follow-up action when convenient. However, a particular flurry, sequence or cascade of alerts may itself be cause for alarm. "Part of public warning that captures attention of first responders and people at risk in a developing emergency situation" *(ISO 22300)*. "'Instant' indication that an information system and network may be under attack, or in danger because of accident, failure or human error" *(ISO/IEC 27033-1)*. b. *[Adjective]* Security aware, vigilant, and primed to react quickly and appropriately to threats, events, and incidents as they unfold. Think: meercats and other prey species.
Alerting system	a. System for alerting. May refer specifically to the computer element, whereas the overall system potentially includes the definition of various alert and alarm criteria and situations, design and implementation, testing, monitoring, maintenance, response plans, escalation, *etc.*, as part of the process and safety engineering. "Provides real-time information about security issues, including vulnerabilities and exploits that are currently happening" *(ISACA glossary)*. b. Whichever computer system raised an alert – not always immediately obvious in, say, a busy process control room.
Alert situation	The particular circumstances or conditions intended to trigger an alert, *e.g.* if a chemical manufacturing process exceeds a temperature or pressure warning setpoint, alerting the human or automated controllers to a potential concern. "The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The enterprise entering into an alert situation initiates a series of escalation steps" *(ISACA glossary)*.

TERM	MEANING
Algorithm, cipher, cypher	Logical function, process, and/or protocol at the heart of an information system such as a cryptosystem or **A**rtificial **I**ntelligence system, *e.g.* determines the calculations, actions, or operations necessary to encrypt plaintext and decrypt ciphertext, or to make real-time decisions when controlling a robotic machine tool. "Finite ordered set of well-defined rules for the solution of a problem" *(ISO/IEC 2382)*. "A finite set of well-defined, unambiguous rules for the solution of a problem in a finite number of steps. It is a sequence of operational actions that lead to a desired goal and is the basic building block of a program" *(ISACA glossary)*. "A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer [and] An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms" *(SANS glossary)*.
Algorithm analysis	Algorithm analysis. "A software verification and validation (V&V) task to ensure that the algorithms selected are correct, appropriate and stable, and meet all accuracy, timing and sizing requirements" *(ISACA glossary)*.
Algorithmic justice	"Actively identifying and dismantling harmful biases within algorithms, promoting fairer development and deployment, and promoting accountability and transparency" *(ISACA glossary)*.
All-hazards	Risk management objective to identify and address a wide variety of potential events, incidents, disasters, emergencies, *etc*. "Naturally occurring event, human induced event (both intentional and unintentional) and technology caused event with potential impact on an organization, community or society and the environment on which it depends" *(ISO 22300)*.
Allocated requirement	"Requirement that results from levying all or part of a higher-level requirement on a solution's lower-level design component. Requirements can be assigned to logical or physical components, including people, consumables, delivery increments and architecture" *(ISACA glossary)*.
All-of-government	"Refers to the entire New Zealand state sector" *(NZISM)*.
Allocated space	"Area on digital media, including primary memory, which is in use for the storage of data, including metadata" *(ISO/IEC 27037)*.
Allow list	Politically correct form of whitelist. "A list that confirms items being analysed are acceptable … the opposite of a deny or block list" *(NZISM)*.

TERM	MEANING
Alpha test	Software self-assessment performed by its developer, a peer, or the development team, the first phase of testing by humans as opposed to, say, automated source code syntax/typo checks by the compiler. Being so closely involved in the process, developers *may* fail to recognise inherent logical errors and misinterpreted functional or nonfunctional requirements that beta testers *may* spot. Or not.
Alternate **D**ata **S**tream **(ADS)**	For interoperability with the Macintosh **H**ierarchical **F**ile **S**ystem, Windows **N**ew **T**echnology **F**ile **S**ystem can associate additional 'streams' of information with files (other than the details normally shown in folder listings), each of which can contain additional data, even executable programs with malware implications. A legitimate use for ADS is the zone.identifier "**M**ark **O**f [**T**he] **W**eb" metadata stream indicating if the file arrived from trusted or untrusted local or remote (Internet) sources, optionally including the source **U**niform **R**esource **L**ocator.
Alternate facilities, alternate site	"Alternate operating location selected to be used by an organization when normal business operations cannot be carried out using the normal location after a disruption has occurred" *(ISO/IEC 27031)*. "Locations and infrastructures from which emergency or backup processes are executed when the main premises are unavailable or destroyed. Note: Includes other buildings, offices or data processing centers" *(ISACA glossary)*.
Alternate process	Different approach or way of doing things. "An automatic or manual process designed and established to continue critical business processes from point-of-failure to return-to-normal" *(ISACA glossary)*.
Alternative routing	"A service that allows the option of having an alternate route to complete a call when the marked destination is not available. Note: In signaling, alternate routing is the process of allocating substitute routes for a given signaling traffic stream in case of failure(s) affecting the normal signaling links or routes of that traffic stream" *(ISACA glossary)*.
Amazon **W**eb **S**ervices **(AWS)**	Brand name for Amazon's global cloud infrastructure. See also Azure, **G**oogle **C**loud **P**latform.
American **I**nstitute of **C**ertified **P**ublic **A**ccountants **(AICPA)**	US trade body for **C**ertified **P**ublic **A**ccountants, merged in 2017 with the **C**hartered **I**nstitute of **M**anagement **A**ccountants. More info: https://www.aicpa-cima.com/home

TERM	MEANING
American **N**ational **S**tandards **I**nstitute **(ANSI)**	Private non-profit organisation promoting voluntary standards and conformity assessment in the US. Mission: "To enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity." See also **N**ational **I**nstitute of **S**cience and **T**echnology. More info: https://www.ansi.org/
Ambiguous	Uncertain/unclear and potentially risky situation, definition, or meaning increasing the possibility of misinterpretation and misunderstanding. "A property that refers to the presence of multiple, unclear, or conflicting interpretations of conditions, events, or behaviors in a system" *(OCEG GRC Glossary)*.
Amplification attack, reflection attack	Type of attack in which servers are tricked into transmitting a large volume of network traffic to a target system, potentially overloading it, causing a **D**enial-**o**f-**S**ervice. **N**etwork **T**ime **P**rotocol, **D**omain **N**ame **S**ystem, or other request packets with spoofed source **I**nternet **P**rotocol addresses matching the target are sent to one or more servers which then forward their responses to the target instead of the originator. See also **D**istributed **R**eflective **D**enial-**o**f-**S**ervice.
AMT	*Abbrev:* **A**ctive **M**anagement **T**echnology.
Analogue	a. *[Adjective]* Continuously variable as opposed to a step function such as digital. b. *[Noun]* Artificial model representing and simulating something real, such as a virtual assistant.
Analysis, analytics	Process of systematically exploring, examining, investigating, and evaluating information relating to risks, incidents, forensic evidence, *etc*. in some depth. "Evaluation of potential digital evidence in order to assess its relevance to the investigation. Note: Potential digital evidence, which is determined to be relevant, becomes digital evidence" *(ISO/IEC 27042-2)*. "The examination of acquired data for its significance and probative value to the case" *(NIST SP 800-101)*. "1. To separate into elemental parts or basic principles to determine the nature of the whole. 2. A course of reasoning showing that a certain result is a consequence of assumed premises. 3. The methodical investigation of a problem and the separation of that problem into smaller related units for further detailed study (Source: ANSI)" *(ISACA glossary)*. "Any form of test, comparison or analytical method performed on an item/exhibit or relevant material recovered from an item/exhibit" *(FSRCoP)*.

TERM	MEANING
Analysis criteria	Analysis criteria. "The criteria used to analyze, quantify and select ways to address risk, reward, and compliance" *(OCEG GRC Glossary)*.
Analytical model	Mathematical formula for generating metrics (such as a trend in a relevant security parameter) from measurements (normally a time series of values of the parameter), giving meaning to the numbers ("See, I told you things *are* getting better!"). "Algorithm or calculation combining one or more base measures and/or derived measures with associated decision criteria" *(ISO/IEC 27000)*.
Analytical technique	Systematic method or approach for analysis, *e.g.* a classic 'scientific' technique is to study current knowledge and generate a credible theoretical hypothesis, then test it against reality using experimental data and so advance the state of knowledge. "The examination of ratios, trends and changes in balances and other values between periods to obtain a broad understanding of the enterprise's financial or operational position and to identify areas that may require further or closer investigation. Note: Often used when planning the assurance assignment" *(ISACA glossary)*.
Anarchy, anarchism, anarchist	For ideological or other reasons, anarchists typically seek to overthrow the government and disrupt civil society by (among other things) sabotaging vulnerable parts of the **C**ritical **N**ational **I**nfrastructure.
Angler	Modular crimeware kit, in the wild in 2016, used for phishing.
Angry IP Scanner, ipscan	Network security administration/penetration testing tool like nmap. It scans (queries) **I**nternet **P**rotocol address and port ranges to identify nodes.
Annotate, annotation	Prepare pertinent 'margin' notes to accompany a particular document, topic, or activity, *e.g.* explaining the content in more detail, commenting on and critiquing it, raising queries and concerns, elaborating or suggesting alternative interpretations and conclusions. "The process of labeling or tagging data to provide examples from which a machine learning (ML) algorithm can develop a model" *(ISACA glossary)*.
Annual audit, statutory audit	Financial audit conducted by external auditors to confirm that the information in the organisation's annual report and accounts is accurate and truthful. This involves checking the integrity of any financial or other systems on which the accounts are based, and testing the organisation's compliance with applicable laws and regulations, *e.g.* concerning accounting practices and tax treatments.

TERM	MEANING
Anomaly, anomalous	Something markedly different, unusual, abnormal, unexpected, or exceptional, hence intriguing and perhaps of concern. While large data anomalies (such as numerous data values completely missing for a significant period) may be easily spotted by eye (provided someone is looking!), small anomalies in large data sets or **D**ata**B**ases can be identified much more easily and reliably by systematic statistical analysis, *e.g.* applying Benford's law. Such anomalies are inherently interesting, hinting at the possibility of unexpected relationships, biases, or events, perhaps even information security incidents such as bugs, flaws, frauds, malware, or hacks in progress. Anomalous data communications (*e.g.* an unusual surge or dip in network traffic volume, or unusual senders and recipients) and activities (*e.g.* unusual out-of-hours working) may indicate issues worthy of investigation (*e.g.* 'technical issues,' misconfiguration, fraud, information theft/spying, malware). "Unusual or statistically rare" *(ISACA glossary)*.
Anomaly detection	The process of identifying anomalous conditions, outliers or spurious items, *etc.* in a data set or sequence. Naturally implies the ability to distinguish anomalous from normal if extreme values, potentially indicating a genuine discontinuity or flaw in the model, a subjective or arbitrary determination based on an accurate understanding of the data variability and (often) statistical analysis of objective evidence. "Detection on the basis of whether the system activity matches that defined as abnormal" *(ISACA glossary)*.
Anonymity	Someone's right to go about their life and business without unnecessarily revealing their identity, *e.g.* whistleblowers or for privacy reasons. Typically achieved through discretion, sometimes through a trusted third party or using techniques such as anonymisation, tokenisation, or redaction. With careful design, the systematic process of identifying and authenticating messages, instructions, data, *etc.* can be logically and practically separated from identifying and authenticating the originating people, organisations, systems, *etc*. May conflict with law enforcement and other sociological or ethical expectations, objectives, requirements, or obligations such as personal accountability. "Characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly" *(ISO/IEC 29100)*. "The quality or state of not being named or identified" *(ISACA glossary)*.

TERM	MEANING
Anonymisation	Permanent and complete removal of the personal information necessary to identify specific individuals in a **D**ata**B**ase, document, *etc.,* normally for privacy reasons. "Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" *(ISO/IEC 29100*). "Irreversible severance of a data set from the identity of the data contributor to prevent any future reidentification, even by the organization collecting the data under any condition" *(ISACA glossary)*. *Cf.* pseudonymisation.
Anonymous	a. Information of unstated origin that is not and cannot be linked unambiguously to a specific, identifiable person, subject, originator, or source. b. Name of a 'hacker collective' – a loosely organised and indistinct group of pranksters, hackers, digital vigilantes, and subversive hacktivists active for two decades from about 2004. Their proclamations famously included the line "We are legion" spoken in a synthetic voice emanating from a stylised mask. See also LulzSec.
ANSI	*Abbrev:* **A**merican **N**ational **S**tandards **I**nstitute.
Anti-pass-back	Physical security access control arrangement such as a man trap designed to prevent someone presenting their access card to open a one-person-at-a-time controlled entrance for themselves, then handing their card back to someone else (typically an unauthorised visitor) permitting them also to access the controlled area. Electronic access control systems may keep track of individuals, preventing them from re-accessing an area unless they have previously exited it, requiring them to present their access cards at *both* entry *and* exit points. "A security mechanism preventing an access card or similar device from being used to enter an area a second time without first leaving it (so that the card cannot be passed back to a second person who wants to enter)" *(PCI Card Production and Provisioning Physical Security Requirements)*.
Antiphishing, anti-phishing	Cluster of information risk and security management techniques and controls to mitigate the risks associated with phishing. "Software that identifies phishing content and attempts to block the content or warn the user about the suspicious nature of the content" *(ISACA glossary)*.

TERM	MEANING
Antivirus, antimalware	Software application/program/package/system and associated services and controls to mitigate the risk of malware by avoiding, detecting, preventing, and/or removing infections with viruses, worms, Trojans, spyware, ransomware, rootkits, *etc*. "A widely used technology to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware [and] An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected" *(ISACA glossary)*.
AP	*Abbrev:* **A**ccess **P**oint.
API	*Abbrev:* **A**pplication **P**rogramming **I**nterface.
APN	*Abbrev:* **A**ccess **P**oint **N**ame.
app	*Abbrev:* **app**lication.
Appearance	How or what something *appears* to be – a subjective impression. "The act of giving the idea or impression of being or doing something" *(ISACA glossary)*.
Appearance of independence	For an auditor, scientist, judge or similar professional rôle, the *appearance* of being independent is almost as important as the actuality. It affects the nature and quality of interactions with stakeholders, including aspects such as access to sensitive information, tolerance, influence, and mutual respect (trust). "The behavior that is appropriate of an IS auditor to meet the situations occurring during audit work (interviews, meetings, reporting, *etc*.). Note: An IS auditor should be aware that appearance of independence depends on the perceptions of others and can be influenced by improper actions or associations" *(ISACA glossary)*.
Appetite	Hunger or desire, *e.g*. risk appetite. "A range for the value of an indicator that defines a preferred or expected level of variation around a target" *(OCEG GRC Glossary)*. *Cf*. tolerance.
Applet	A cute little application program. "A program written in a portable, platform-independent computer language, such as Java, JavaScript, or Visual Basic. Notes: An applet is usually embedded in an HyperText Markup Language (HTML) page downloaded from web servers. Applets can only perform a restricted set of operations, thus preventing, or at least minimizing, the possible security compromise of the host computers. However, applets expose the user's machine to risk if not properly controlled by the browser, which should not allow an applet to access a machine's information without prior authorization of the user" *(ISACA glossary)*.

TERM	MEANING
Appliance	Computer system or device dedicated to a specific purpose, ready to use straight out of the box ('plug and play'), requiring little if any configuration or management. Home networking and entertainment devices and smart 'white goods' (washing machines, refrigerators, *etc*.) are appliances with embedded systems. See also **I**nternet **o**f ***T****hings*.
Application (app), application program, application software	a. Computer program or suite of programs providing useful functions. Applications on smartphones, tablet and portable PCs, social media or (supposed) security apps downloaded from the web and installed by naïve users, may be Trojans, spyware, or other malware, especially on jailbroken devices. "A program, or group of programs, hosted on enterprise assets and designed for end-users. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications" *(CIS Controls)*. "The use of information resources (information and information technology) to satisfy a specific set of user requirements" *(OMB Circular A-130 Appendix III)*. "A computer program or set of programs that performs the processing of records for a specific function. Notes: Applications contrast with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort. [and] A program that processes business data through activities such as data entry, update or query. Notes: Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort. [and] A software designed to fill the specific needs of a user; for example, software for navigation, payroll or process control. Contrasts with support software and system software" *(ISACA glossary)*. b. Situation in which something might be usefully and gainfully employed or utilised (applied). c. Process and form for applying for a job, grant, loan, permission, network access, *etc*.
Application acquisition review	"An evaluation of an application system being acquired or evaluated, that considers matters such as: appropriate controls being designed into the system, the processing of information in a complete, accurate and reliable manner; the application will function as intended; the application will application functionality in compliance with any applicable statutory provisions and compliance with the established system acquisition process" *(ISACA glossary)*. See also system development audit.
Application architecture	Architecture and design of an application program or system. "A description of the logical grouping of capabilities that manage the objects necessary to process information and support the enterprise's objectives" *(ISACA glossary)*.

TERM	MEANING
Application benchmarking	Application benchmark. "The process of establishing the design and operation of automated controls within an application" *(ISACA glossary)*.
Application component	Component part of an application such as a function or subroutine.
Application containerisation	"A mechanism that is used to isolate applications from each other within the context of a running operating system instance. In much the same way that a logical partition (LPAR) provides segmentation of system resources in mainframes, a computing environment — employing containers — segments and isolates the underlying system services so that they are logically sequestered from each other" *(ISACA glossary)*.
Application control, application security	Security control over, or within, an application, such as access controls, backups, **D**ata**B**ase security, and the associated administrative controls, *e.g.* change control. "The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved" *(ISACA glossary)*. "An approach in which only an explicitly defined set of trusted applications are allowed to execute on systems" *(AusISM)*.
Application development, software development, systems development, development, application programming	Process, method, approach, phase, or stage within which new or updated software is coded (*i.e.* source code is written). Sometimes broadened to include the preceding specification and architecture/design phases, and perhaps the subsequent software testing, version control, change and configuration management, and implementation activities. "The act or function of developing and maintaining application programs in production" *(ISACA glossary)*.
Application development review	"An evaluation of an application system under development that considers matters such as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions and in compliance with the established system development life cycle process" *(ISACA glossary)*. See also system development audit.
Application development sandbox	See development environment. "A standalone computer, virtual machine or virtual environment used to conduct software development removed from production infrastructure" *(ISACA glossary)*.
Application implementation review	"An evaluation of any part of an implementation project. Note: Examples include project management, test plans and user acceptance testing (UAT) procedures" *(ISACA glossary)*. See also system development audit, testing, implementation.
Application maintenance review	"An evaluation of any part of a project to perform maintenance on an application system. Note: Examples include project management, test plans and user acceptance testing (UAT) procedures" *(ISACA glossary)*. See also system development audit.

TERM	MEANING
Application **P**rogramming **I**nterface **(API)**	In a **S**ervice-**O**riented **A**rchitecture, complete applications can be assembled Lego-style from building blocks – essentially subroutines, subsystems, or functions providing discrete information services accessed through APIs. While individual services or microservices and APIs may be securely specified, designed, and implemented, ensuring overall system security can be challenging due to numerous interfaces and issues such as scope, context, dynamics, and complexity, plus the almost inevitable flaws and bugs. "Set of functions, protocols, parameters, and objects of different formats, used to create software that interfaces with the features or data of an external system or service" *(ISO/IEC/IEEE 26531)*. "A set of routines, protocols and tools referred to as building blocks used in business application software development" *(ISACA glossary)*.
Application proxy	Network service mediating the data flowing to and from applications running on a server. "A service that connects programs running on internal networks to services on exterior networks by creating two connections, one from the requesting client and another to the destination service" *(ISACA glossary)*.
Application security	See application control. "The security aspects supported by the application, primarily with regard to the roles or responsibilities and audit trails within the applications" *(ISACA glossary)*.
Application **S**ervice **P**rovider **(ASP)**	Organisation offering applications via the Internet, *i.e.* **S**oftware-**a**s-**a**-**S**ervice. "A managed service provider (MSP) that deploys, hosts and manages access to a packaged application to multiple parties from a centrally managed facility. Note: The applications are delivered over networks on a subscription basis" *(ISACA glossary)*. See also **C**loud **S**ervice **P**rovider.
Application software tracing and mapping	"A specialized tool that can be used to analyze the flow of data through the processing logic of the application software and document the logic, paths, control conditions and processing sequences. Notes: Both the command language or job control statements and programming language can be analyzed. This technique includes program/system: mapping, tracing, snapshots, parallel simulations and code comparisons" *(ISACA glossary)*.
Application-**S**pecific **I**ntegrated **C**ircuit **(ASIC)**	**I**ntegrated **C**ircuit designed, preprogrammed, and dedicated to perform a particular function with high efficiency/performance and reliability such as **R**ead-**O**nly **M**emory chips storing firmware and **F**ield-**P**rogrammable **G**ate **A**rrays used for **D**igital **S**ignal **P**rocessing, industrial automation, **A**rtificial **I**ntelligence/**D**eep **L**earning, cryptography, *etc*. "Integrated circuit customized for a particular use" *(ISO/IEC 22989)*. "A solid-state device designed to perform a single or small group of functions" *(ISACA glossary)*.

TERM	MEANING
Application system	Either just an application program itself, or the broader system potentially including the computer server; the **O**perating **S**ystem and middleware (*e.g.* a **D**ata**B**ase **M**anagement **S**ystem); the network, administrative, and business services; the data; and various groups of people or organisations involved in designing, developing, providing, using, supporting, maintaining, managing, and benefiting from the app. "An integrated set of computer programs designed to serve a particular function that has specific input, processing and output activities. Note: Examples include general ledger, manufacturing resource planning and human resource (HR) management" *(ISACA glossary)*.
Application whitelist	Application of whitelisting to applications. "An approach in which all executables and applications are prevented from executing by default, with an explicitly defined set of allowed executables" *(NZISM)*.
Appraisal	Formal or official assessment. "An examination of one or more processes by a trained team using an appraisal reference model as the basis for determining, at a minimum, strengths and weaknesses" *(ISACA glossary)*.
Appropriate evidence	"The measure of the quality of the evidence" *(ISACA glossary)*.
Approval	See authorisation.
Approved Destruction Facility	"The status of 'approved facility' for the destruction of media and equipment, applies to a specific installation/site, and is granted by the Director-General GCSB under the NZISM [if deemed] capable of securely destroying IT equipment, devices and media to the standard required under the NZISM and related policies and that procedural security meets the required standards" *(NZISM)*.
APT	*Abbrev:* **A**dvanced **P**ersistent **T**hreat.
APT#	Identifier for a state-sponsored (spooky) hacker group such as the North Korean APT38 (also known as Lazarus Group) using **A**dvanced **P**ersistent **T**hreat malware. Identification is difficult due to the groups evolving, actively evading detection and misleading analysts working independently. Likewise, attribution to specific countries is problematic due to false flag operations, disinformation, and global politics.
Arbitrary	Subjective, according to someone's preference. Vulnerabilities that reportedly allow 'arbitrary commands' are a cybersecurity red flag since adversaries who exploit them can effectively take full control of a compromised system.

TERM	MEANING
Architecture	Overall grand design or blueprint for an organisation's information systems, networks, and business processes, linking even higher-level objectives from various strategies to lower-level designs for individual systems, subsystems, domains, and processes. May incorporate the information security architecture. In the physical security context, the architectural design of a facility can help or hinder security and safety. "Fundamental organisation of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution" *(ISO/IEC 27033-1)*. "The design of the structure of a system, including logical components, and the logical interrelationships of a computer, its operating system, a network, or other elements" *(**T**rust **S**ervices **C**riteria)*. "Description of the fundamental underlying design of the components of the business system, or of one element of the business system (*e.g.*, technology), the relationships among them and the manner in which they support enterprise objectives" *(ISACA glossary)*.
Archive, archival	Secure long-term storage of valuable information, designed to ensure its integrity, availability, and often (but not necessarily) its confidentiality and so maintain its value. May be required for compliance reasons, *e.g.* organisations are obliged by applicable laws/regulations to provide certain types of business record several years after they were created. In a few cases, the retention period is indefinite. Since only valuable information is archived, assurance that it can in fact be restored when needed is a non-negotiable requirement, so prove it! "Store backup files and any associated journals, usually for a given period of time" *(ISO/IEC 2382)*. "A lasting collection of computer system data or other records that are in long-term storage" *(ISACA glossary)*.
Area	a. Region, place, location, site, facility, domain, zone, concept, *etc*., within some sort of physical or notional boundary, not necessarily sharply or explicitly declared. b. Two-dimensional measure of the extent of a surface, plane, or layer.
Armour	Strong protective plates, typically comprising layers of leather, steel, Kevlar/carbon-fibre/composite materials and ceramics that absorb and spread the energy, resisting penetration by weapons such as swords, daggers/knives, shrapnel, and bullets. The physical security version of hardening.

TERM	MEANING
Arms-length	Indicates a notional separation between parties, giving a degree of independence and plausible deniability of their collusion or involvement in nefarious activities such as **O**ffensive **C**yberspace **O**perations, anti-competitive behaviours such as price fixing, cabal, or *coup d'etat*.
ARP	*Abbrev:* **A**ddress **R**esolution **P**rotocol.
ARPANET (Advanced Research Projects Agency Network)	"A pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990" *(SANS glossary)*.
Arson	Deliberately setting fire to or burning something without its owner's permission, or with intent to defraud another (such as an insurance company). A form of sabotage. A threat to many tangible assets.
Artefact, artifact	a. Glitch, interruption, error, problem, unnatural occurrence. "A form of objective evidence that is an output of the work being performed and the process being followed. It must demonstrate the extent of implementing, performing or supporting the organizational or project processes that can be mapped to one or more model practices. Artifacts must be provided by people with a process role to implement, perform, follow or support processes" *(ISACA glossary)*. "Something observed in an examination or analysis that was not originally present but occurs as a result of the procedures employed for examination or analysis" *(FSRCoP)*. b. Object such as an item of evidence or a record.
Artificial **G**eneral **I**ntelligence **(AGI), General AI, strong AI, full AI, superintelligence**	Generic/adaptable form of **A**rtificial **I**ntelligence, far closer to human intelligence and sentience than today's limited AI approaches such as generative AI. "Type of AI system that addresses a broad range of tasks with a satisfactory level of performance. Notes: Compared to narrow AI; AGI is often used in a stronger sense, meaning systems that not only can perform a wide variety of tasks, but all tasks that a human can perform" *(ISO/IEC 22989)*. "Systems that demonstrate broad capabilities of intelligence, including reasoning, planning, and the ability to learn from experience, and with these capabilities at or above human-level" (Microsoft researchers, cited by Ada Lovelace Institute). *Cf.* **Gen**erative **A**rtificial **I**ntelligence.
Artificial **I**ntelligence **(AI), cognitive system**	**I**nformation **T**echnology system based on neural networks employing **D**eep **L**earning, **M**achine **L**earning, **L**arge **L**anguage **M**odels, and/or **N**atural **L**anguage **P**rocessing techniques, having been trained on big data sets to simulate or emulate the rational reasoning, cognitive, and decision-making capabilities of intelligent humans. AI-related terms, concepts, and practices are emerging from a rapidly evolving cluster of complex and

TERM	MEANING
	disruptive technologies with significant information risk, information security, privacy, compliance, business, and societal implications. While the information risks and ethical concerns associated with AI are challenging and potentially disturbing, AI systems show promise in the cybersecurity field, *e.g.* automated network/system intrusion, phishing, malware and fraud detection, prevention and response, and the intelligent design of business processes and systems. "Interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning" *(ISO/IEC 2382)*. "Research and development of mechanisms and applications of AI systems. Note: Research and development can take place across any number of fields such as computer science, data science, humanities, mathematics and natural sciences" *(ISO/IEC 22989)*. "Discipline concerned with the building of computer systems that perform tasks requiring intelligence when performed by humans" *(ISO/IEC 39794-16)*. "An advanced computer system that can simulate human capabilities, such as analysis, based on a predetermined set of rules" *(ISACA glossary)*. "A technology in which a computing system is coded to 'think for itself', adapting and operating autonomously. AI is increasingly used in more complex tasks, such as medical diagnosis, drug discovery, and predictive maintenance" *(UK National Cyber Security Strategy 2022)*.
Artificial **I**ntelligence **G**overnance **P**rofessional **(AIGP)**	IAPP's professional qualification concerning technological foundations and the **A**rtificial **I**ntelligence **S**oftware **D**evelopment **L**ife**C**ycle, AI's effects on people and principles, applicability of laws, responsible AI governance and risk management, and ongoing issues and concerns. More info: https://store.iapp.org/ai-governance-professional-aigp-online-training/
Artificial **I**ntelligence **(AI) system**	**I**nformation **T**echnology system (hardware and software) plus the associated data, network infrastructure, people, *etc*. involved in providing **A**rtificial **I**ntelligence services. "Engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives. Notes: The engineered system can use various techniques and approaches related to artificial intelligence to develop a model to represent data, knowledge, processes, *etc*. which can be used to conduct tasks; AI systems are designed to operate with varying levels of automation" *(ISO/IEC 22989)*.

TERM	MEANING
Artificial **S**uper**I**ntelligence **(ASI)**	Concept of an **A**rtificial **I**ntelligence system that substantially exceeds human levels of intelligence, reasoning, *etc*. in general, rather than just in specific areas (narrow AI).
ASI	*Abbrev:* **A**rtificial **S**uper**I**ntelligence.
ASIC	*Abbrev:* **A**pplication-**S**pecific **I**ntegrated **C**ircuit.
ASLR	*Abbrev:* **A**ddress **S**pace **L**ayout **R**andomisation.
ASP	*Abbrev:* **A**pplication **S**ervice **P**rovider.
Assembler	Program that translates assembly language into machine code instructions appropriate for the particular **C**entral **P**rocessing **U**nit on which the code is to execute.
Assembly language	Any low-level programming language using symbolic representations of machine code – similar to shorthand.
Assert, assertion	Unilaterally state or claim something to be true, without *necessarily* having or providing the evidence to prove it, *e.g.* trust centre. "Any formal declaration, or set of declarations, about a subject matter made by management. Note: Assertions should usually be made in writing and commonly contain a list of specific attributes about the subject matter or about a process involving the subject matter" *(ISACA glossary)*.
Assertive	Dominant, coercive, overbearing, or authoritarian, able to exert strong influence on another without resorting to overt aggression or violence. A powerful technique in many social engineering attacks as well as legitimate controlling activities ("Hands up! You're nicked!" for instance).
Assessment, assess	Process of analysing, reviewing, testing, examining, and/or evaluating something to reach an opinion, decision, or judgement. "A broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative. Note: May include opportunities for reducing the costs of poor quality, employee perceptions of quality aspects, proposals to senior management on policy, goals, *etc*." *(ISACA glossary)*. "The action of evaluating, estimating, or judging against defined criteria. Different types of assessment (*i.e*., qualitative, quantitative, and semi-quantitative) are used to assess risk. Some types of assessment yield measures [or results]" *(NIST SP 800-55v1)*. "The application of expert judgement to devise an examination strategy (see Examination strategy) based upon a framework of circumstances in the form of written submission details, photographs, 'preview' examinations of items, discussions with submitting officers *etc*., that addresses in an effective way the identified key issues in the case" *(FSRCoP)*.

TERM	MEANING
Assessment result	"The output or outcome of an assessment" *(SP 800-55v1)*.
Assessor	Competent person who conducts an assessment, evaluation, or examination. "Person who leads and conducts a privacy impact assessment. Notes: The assessor may be supported by one or more other internal and/or external experts as part of their team; The assessor may be an expert internal or external to the organization" *(ISO/IEC 29134)*. See also evaluator.
Asset	Something of value to its owner, a resource. May be tangible (*e.g.* a building, hardware, executed contract or licence/approval, person – possibly an agent, cash, or padlock), intangible (*e.g.* knowledge, experience, know-how, skill, capability, competence, tradecraft, information, software, creative idea, concept, relationship, virtual organisation, brand, reputation, trust, loyalty, goodwill, bank credit, application or service, right or permission, understanding, verbal contract, obligation), or indeterminate (*e.g.* trademark, patent, firmware, data, **D**ata**B**ase, system, security). "Legal right or organisational resource which is controllable by an entity and has the capacity to generate economic benefits" *(ISO 10668)*. "Anything that has value to the organization" *(ISO/IEC 27002)*. "Anything of value to an agency, such as IT equipment and software, information, personnel, documentation, reputation and public confidence" *(NZISM)*. "Anything of value, such as ICT equipment, software or data" *(AusISM)*. "Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation" *(ISACA glossary)*. "The information, information system, or information system component that is breached or impaired by the Threat Agent in a manner whereby its value is diminished or the act introduces liability to the Primary Stakeholder" *(O-RT)*. "Things that have value to anyone involved in the processing of personally identifiable information (PII). Note: In the context of a privacy risk management process, an asset is either PII or a supporting asset" *(ISO/IEC 29134)*. "Item, thing or entity that has potential or actual value to an organization. Notes: Value can be tangible or intangible, financial, or non-financial, and includes consideration of risks and liabilities. It can be positive or negative at different stages of the asset life. Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation, or agreements. A grouping of assets referred to as an asset system could also be considered as an asset. Life, health and welfare of humans and other living beings can also be an asset" *(ISO 23234)*. See also information asset. *Cf.* liability.

TERM	MEANING
Asset management	Systematic, professional management of one or more types/classes of assets (such as buildings/properties, financial, computing hardware and software, or information) to achieve objectives specified by their owners, custodians, and other stakeholders.
Asset operator	Person or organisation operating (using, controlling) an asset such as a computer system. *Cf*. asset owner.
Asset owner, liability owner	Organisation, rôle, or person who literally/legally or notionally owns an asset or liability, along with any associated property rights and obligations, responsibilities, or social expectations. May be a custodian, steward, or agent acting on behalf of the legal owner. May be accountable for its protection/security and legitimate exploitation to optimise its value. See also information owner, data owner, file owner, network owner, domain owner, process owner, product owner, risk owner, service owner, system owner.
Asset value	A measure of the worth of an asset to someone, usually its legal owner or possessor. "The value of an asset to both the business and to competitors" *(ISACA glossary)*.
Assignment	Allocation or appointment of someone (usually an employee) to a particular task, rôle, position, project, *etc*., or the engagement itself – the work package.
Assurance	Provision of a certain level of trust, confidence, confirmation, or proof of something, normally as a result of competently reviewing, checking, testing, or auditing it against relevant specifications, expectations, or objectives, *e.g.* a 'security-assured' program has *presumably* been tested to confirm that it satisfies information security requirements. "The act of objectively and competently evaluating subject matter to provide conclusions and confidence that statements and beliefs about the subject matter are justified and true" *(OCEG GRC Glossary)*. "Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria" *(IIA GIAS)*. "An IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort regarding the subject matter. Note: Assurance engagements could include support for audited financial statements, reviews of controls, compliance with required standards and practices, and compliance with agreements, licenses, legislation and regulation" *(ISACA glossary)*.
Assurance actions & controls	"Actions & controls that primarily serve assurance activities" *(OCEG GRC Glossary)*.

TERM	MEANING
Assurance control	Control designed to mitigate unacceptable assurance risks. While assurance is itself a form of detective control (*e.g.* examinations identifying and disclosing issues to management), various controls can strengthen assurance processes, *e.g.* recruitment, training, and oversight to ensure that technology auditors are sufficiently competent, diligent, trustworthy, experienced, *etc*. for their audit engagements.
Assurance engagement, assurance initiative	Assurance engagement. "An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise. Note: Examples may include financial, performance, compliance and system security engagements" *(ISACA glossary)*.
Assurance provider	"Someone who conducts assurance activities" *(OCEG GRC Glossary)*.
Assurance risk	Uncertainty relating to the assurance required and provided, *e.g.* whether the particular sampling approach proposed for an audit will or will not discover issues, what kinds of issues it might or might not reveal, and hence whether the approach is appropriate or needs to be reconsidered in a particular situation.
Assurance service	Service providing or relating to some form of assurance, *e.g.* testing, reviewing, inspecting, assessing, auditing. "Services through which internal auditors perform objective assessments to provide assurance. Examples of assurance services include compliance, financial, operational/performance, and technology engagements. Internal auditors may provide limited or reasonable assurance, depending on the nature, timing, and extent of procedures performed" *(IIA GIAS)*.
Asymmetric cryptography, asymmetric encryption/ decryption, public key cryptography	Type of cryptosystem that uses pairs of mathematically related but quite different public and private keys to either encrypt or decrypt. Although the pairs of keys are relatively simple and quick to generate on a computer, it is infeasible to guess or calculate either key from the other without additional information due to the complex mathematics and long key lengths involved. "Cryptography in which a public key and a corresponding private key are used for encryption and decryption. Note: If a public key is used for encryption, the corresponding private key must be used for decryption, and vice versa" *(ISO/IEC 2382)*. See also **P**ublic **K**ey **I**nfrastructure. *Cf.* symmetric cryptography.
Asymmetric cryptography algorithm, asymmetric cipher	Cryptographic algorithm for asymmetric cryptography. "A type of cipher that combines a widely distributed public key and a closely held, protected private key. A message that is encrypted by the public key can only be decrypted by its mathematically related counterpart" *(ISACA glossary)*.

TERM	MEANING
Asynchronous **T**ransfer **M**ode **(ATM)**	"A high-bandwidth, low-delay switching and multiplexing technology that allows integration of real-time voice, video and data. It is a data-link layer protocol. Note: ATM is a protocol-independent transport mechanism. It allows high-speed data transfer rates of up to 155 Mbit/s." *(ISACA glossary) Cf.* **A**utomated **T**eller **M**achine.
Asynchronous transmission	Type of digital datacommunications protocol or modulation method in which each character of a message is preceded by a start bit and followed by one or two stop bits (and, often, a parity bit) to distinguish it from the unmodulated carrier. "A transmission method where characters are sent one at a time" *(ISACA glossary)*. *Cf.* synchronous transmission.
ATM	*Abbrev:* **A**synchronous **T**ransfer **M**ode or **A**utomated **T**eller **M**achine or **A**t **T**he **M**oment, depending on context.
AtomBombing	Code injection exploit that alters the atom tables used internally by Windows to store and communicate strings during program execution.
Atomic	"A condition of smart contracts where one or more conditions defined by the smart contract must be met for the transaction to execute in its entirety" *(ISACA glossary)*. See also smart contract.
Atomic swap	"A peer-to-peer exchange of assets across separate blockchains triggered by predetermined rules, without the use of a third-party service and through the use of self-enforced smart contracts. It requires an exchange of assets on both sides or the transaction will not occur" *(ISACA glossary)*. See also smart contract.
ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge)	MITRE's taxonomy/**D**ata**B**ase of cyber-attack tactics and techniques, first published in 2015. Contrived name complements D3FEND. "ATT&CK is a knowledge base of cyber adversary behavior and taxonomy for adversarial actions across their lifecycle. ATT&CK has two parts: ATT&CK for Enterprise, which covers behavior against enterprise IT networks and cloud, and ATT&CK for Mobile, which focuses on behavior against mobile devices" *(MITRE ATT&CK FAQ)*. More info: https://attack.mitre.org/
Attack	Type of information security incident actively and deliberately perpetrated by someone (the attacker or adversary) on one or more victims (people and/or organisations) without their permission. *Cf.* accident or natural event. Taking control of more than half the mining power of a cryptocurrency blockchain network may be called a "51% attack." "Attempt to violate computer security. Examples: Malicious logic, wiretapping" *(ISO/IEC 2382)*. "Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset" *(ISO/IEC 27000)*. "Successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset" *(ISO/IEC 27002)*. "An actual occurrence of an adverse event" *(ISACA glossary)*.

TERM	MEANING
Attacker	Adversary who deliberately mounts an attack. "Person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources" *(ISO/IEC 27033-1)*.
Attack mechanism	The method and means by which an attack is perpetrated. "A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target" *(ISACA glossary)*.
Attack surface	Notional 3-dimensional representation of the organisation's information assets, risks, *etc.* where one axis in some way represents vulnerabilities and/or their exposure by various parts of the organisation, forming a complex and dynamic 'surface' that might be actively attacked or exploited by hackers, malware, *etc.* to the corresponding extent. Implies that improving the protection of information assets and/or reducing the exposure or extent of vulnerabilities will somehow improve the organisation's information security and reduce the area … without necessarily stating how that might be achieved. A security metric. "The IT equipment and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability" *(NZISM)*. "The amount of ICT equipment and software used in a system. The greater the attack surface the greater the chances of an adversary finding an exploitable security vulnerability" *(AusISM)*. See also security landscape, risk universe, risk profile, heatmap.
Attack toolkit	See crimeware.
Attack vector	Path, process, or mechanism by which a vulnerable network, system, device, application, organisation, building, site, model, *etc*. might be actively compromised and exploited by an adversary. "Path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome [such as] IoT devices [and] smart phones" *(ISO/IEC 27032)*. "A path or route used by the adversary to gain access to the target (asset). Note: There are two types of attack vectors: ingress and egress (also known as data exfiltration)" *(ISACA glossary)*.
Attagging	Use of **Q**uick **R**esponse codes (perhaps stuck on top of legitimate QR codes) containing malicious JavaScript or **U**niform **R**esource **L**ocators linking to infectious or phishing websites. Exploits victims' naïveté regarding the threat and inability to interpret the codes by eye.

TERM	MEANING
Attention mechanism	Facility for an **A**rtificial **I**ntelligence system to focus on (pay extra attention to) heavily weighted parts of the content during the training process. "In artificial intelligence (AI), a powerful feature used in machine learning (ML) and deep learning (DL) that weights the importance of different inputs, thus enhancing the model's ability to process and interpret complex data patterns, leading to more accurate and relevant outcomes" *(ISACA glossary)*.
Attest, attestation	Formally documented assertion by a duly authorised and accountable person that the organisation complies with (fulfils the requirements of) particular laws/regulations or professional practices such as relevant governance, accounting, and audit standards. Although highly stylised and carefully worded to exclude other liabilities, the signatories are personally accountable for the veracity of such statements; hence, attestation is usually taken very seriously, making it a surprisingly powerful administrative control, akin to taking an oath. "An engagement in which an IT auditor is engaged to either examine management's assertion regarding a particular subject matter or the subject matter directly" *(ISACA glossary)*.
Attribute	a. *[Noun]* Measurable or observable characteristic, quality, or parameter. "Property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means" *(ISO/IEC 27000)*. b. *[Verb]* To ascribe the source, origin, or ownership of something. See also provenance.
Attribute-**B**ased **A**ccess **C**ontrol **(ABAC)**	"An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions" *(NIST SP 800-162)*. *Cf.* **R**ule-**B**ased **A**ccess **C**ontrol, **R**ôle-**B**ased **A**ccess **C**ontrol, **R**ealm-**B**ased **A**ccess **C**ontrol.
Attribute-**B**ased **U**nlinkable **E**ntity **A**uthentication **(ABUEA)**	Means for people to authenticate themselves anonymously, without revealing so much personal information that their identity can be 'linked' (inferred or determined) from other information, thereby compromising their privacy. See ISO/IEC 27551.

TERM	MEANING
Attribute sample	**Q**uality **C**ontrol/audit sampling method that compares the rate of occurrence of item characteristics (*e.g.* visible defects in goods on a production line, inaccurate or dubious financial figures in a ledger, suspicious entries in a log or evidence of noncompliance) to determine whether a response is justified (*e.g.* reject the entire batch or investigate further). Can also be used for **Q**uality **A**ssurance and process improvement, *e.g.* to identify adverse trends worthy of management attention, hopefully forestalling the occurrence of quality failures or other incidents. "A method to select a portion of a population based on the presence or absence of a certain characteristic" *(ISACA glossary)*. See also stratified sample, random sample, systematic stratified sample, time series analysis, convenience sample, discovery sample.
Attribute value	"Specific occurrence of an attribute. Example: 'Blue' is an attribute value for the attribute 'color'" *(ISO/IEC 2382)*.
Attribution	a. Acknowledgement referencing or citing the attributed source, originator, and/or owner of **I**ntellectual **P**roperty being reproduced elsewhere in order to thank them and (hopefully) reduce the risk of being accused of plagiarism or copyright abuse. Although legally speaking attribution *may* be irrelevant to copyright infringement, it is generally considered ethical, polite, helpful, and valuable. Be nice! b. Cybersecurity incidents are often blamed on (attributed to) certain perpetrators according to someone's evaluation of evidence in the malware or hacking tools used, or other clues such as the demands and claims made. However, perpetrators of illegal acts are (for obvious reasons) keen to remain undercover and may deliberately mislead analysts (false-flags). Furthermore, attacks often involve a blend of code, tools, and techniques from disparate sources, obtained through the hacking underground scene. "Process of attempting to assign a device to an individual and may be progressed through a number of different methods, each method having different risks. Cell site analysis may be one method by which patterns of usage may be assessed against what would be expected if a given device was used by a specific person, as opposed to if it was not used by that person" *(FSRCoP)*.
Audience	People who are the *intended* recipients of one or more communicated messages, as distinct from those who actually receive them (*e.g.* by interception or surveillance). "The person or group that is intended to receive a message" *(OCEG GRC Glossary)*.

TERM	MEANING
Audit	Structured, formal, and disciplined assurance process of systematic examination, review, assessment, testing, consideration, evaluation, and reporting by one or more competent and trusted people who – crucially – are independent of the subject area or matters being audited. In many organisations, 'audit' also refers to the business department or function (usually Internal Audit, Quality Audit, *etc.*) and/or third party organisation (External Audit) responsible for auditing. Derived from the Latin *audio* (to listen). "Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. Notes: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). 'Audit evidence' and 'audit criteria' are defined in ISO 19011" *(ISO/IEC 27000)*. [Additional note] "An internal audit is conducted by the organization itself, or by an external party on its behalf" *(ISO/IEC 42001)*. "A formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate or efficiency and effectiveness targets are being met. Note: May be carried out by internal or external groups" *(ISACA glossary)*. "A structured process of examination, review, assessment, testing and reporting against defined requirements or objectives. Auditors should be independent of any IT system, business process, agency, function, site, supplier or other subject area being audited" *(NZISM)*. "Information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities" *(SANS glossary)*. "A systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which specified criteria are fulfilled. In forensic science an audit usually involves determining whether the forensic unit's quality procedures have been complied with" *(FSRCoP)*.
Auditability	Measure of the capability of being audited. This assurance objective for important systems, processes, business relationships, *etc.* implies the need to generate and retain high-integrity records of relevant events and activities (*e.g.* security logs) that can be independently reviewed if and when required, along with transparency and trustworthiness. A significant challenge for **A**rtificial **I**ntelligence systems. "The level to which transactions can be traced and audited through a system" *(ISACA glossary)*.

TERM	MEANING
Auditable unit	See audit universe. "The subjects, units or systems that are capable of being defined and evaluated. Notes: Auditable units may include: Policies, procedures and practices; Cost centers, profit centers and investment centers; General ledger account balances; Information systems (manual and computerized); Major contracts and programs; Organizational units, such as product or service lines; Functions, such as information technology (IT), purchasing, marketing, production, finance, accounting and human resources (HR); Transaction systems for activities, such as sales, collection, purchasing, disbursement, inventory and cost accounting, production, treasury, payroll, and capital assets; Financial statements; Laws and regulations" *(ISACA glossary)*.
Audit accountability	The audit function and individual auditors can be held to account by an authority (typically the Board of Directors or Audit Committee) for failing to achieve specified objectives and expectations, as can every other business function or person. "A performance measurement of service delivery including cost, timeliness and quality against agreed service levels" *(ISACA glossary)*.
Audit authority	Authority formally assigned to an audit function, team, or individual through applicable statutes, policies, and contracts by stakeholders such as senior management, permitting their access to relevant information necessary to perform their duties. "A statement of an employee's position within the enterprise, including lines of reporting and the rights of access" *(ISACA glossary)*.
Audit charter	High-level scope and purpose or mission statement for the audit function. "A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity. Notes: The charter should: Establish the internal audit function's position within the enterprise; Authorize access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements; Define the scope of audit function's activities" *(ISACA glossary)*. See also internal audit charter.
Audit checklist	Aspects of concern or items of evidence that an auditor intends to gather, investigate, and evaluate during an audit engagement. The document format reflects the auditor's personal preferences and style, *e.g.* **I**nternal **C**ontrols **Q**uestionnaire, mind map, or 'shopping list.'
Auditee	Person, function, department, or organisation being audited.

TERM	MEANING
Audit engagement	A specific audit with its authorised scope and purpose or objectives (*e.g.* plan and resources, and in due course the findings, evidence, analysis, and report arising). "A specific audit assignment, task or review activity, such as an audit, control self-assessment review, fraud examination or consultancy. An audit engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives" *(ISACA glossary)*.
Audit evidence	The evidence gathered and analysed in the course of an audit engagement, typically consisting of copies of pertinent documentation, the auditors' contemporaneous notes or transcripts from interviews, meetings and observations, and digital content retrieved from computer systems. "The information used to support the audit opinion" *(ISACA glossary)*.
Audit expert system	"The expert or decision support systems that can be used to assist IS auditors in the decision-making process by automating the knowledge of experts in the field. Note: This technique includes automated risk analysis, systems software and control objectives software packages" *(ISACA glossary)*.
Audit file	a. Hardcopy and/or digital file/s containing information relating to an audit engagement, such as the scope and objectives, plan, working papers (*e.g.* audit checklist), audit evidence, findings, analysis, and report. Constitutes the formal, definitive record of a completed audit. Generally valuable and confidential; hence must be adequately secured. b. Audit log.
Audit independence, auditor independence	Capability, opportunity, and resolute determination of an auditor to gather evidence and analyse information dispassionately, deciding, acting, and reporting independently, free of undue influence, interference, constraint, or pressure from auditees. Implies or involves detached impartiality and objectivity without bias and prejudice, acting with absolute integrity, fairness, neutrality, balance, even-handedness, *etc.* An *essential* factor and unique driver of value in auditing, particularly a competent, diligent, and trustworthy auditor's state of mind and attitudes, regardless of their employment status or reporting line. "1. Self-governance. 2. The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organizational levels. Independence includes Independence of mind and Independence in appearance" *(ITAF)*. "The state of being free from structural or functional conditions that threaten the ability of the assurance provider to perform assurance activities with objectivity and without any undue influence. It includes the independence of the assurance provider from those who own, manage, operate,

TERM	MEANING
	or support the activity being assured" *(OCEG GRC Glossary)*. "The freedom from conditions that may impair the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner" *(IIA GIAS)*. See also agency.
Audit log	Formally documented historical sequence (a data file) of significant security events such as logons, authorisations, bypasses/overrides, alerts, and security/audit configuration changes, defined according to system configuration parameters, securely recorded in real time primarily for subsequent audit and forensic purposes. "A chronological record of system activities, including records of system accesses and operations performed in a given period" *(NIST SP 800-171)*. *Cf*. audit trail.
Audit logging	Privileged process/act of generating and appending audit records to an audit log. "Recording of data on information security events for the purpose of review and analysis, and ongoing monitoring" *(ISO/IEC 27033-1)*.
Audit objective	Objective, purpose, or goal/s of an audit engagement – what it was expected or required to achieve. "The specific goal(s) of an audit. Note: These often center on substantiating the existence of internal controls to minimize business risk" *(ISACA glossary)*.
Auditor	Person performing an audit. An independent specialist with a challenging vocation. "Person who conducts an audit" *(ISO/IEC 17021-1)*.
Auditor's opinion	"A formal statement expressed by the IS audit or assurance professional that describes the scope of the audit, the procedures used to produce the report and whether or not the findings support that the audit criteria have been met. Notes: The types of opinions are: Unqualified opinion—Notes no exceptions or none of the exceptions noted aggregate to a significant deficiency; Qualified opinion—Notes exceptions aggregated to a significant deficiency (but not a material weakness); Adverse opinion—Notes one or more significant deficiencies aggregating to a material weakness" *(ISACA glossary)*.
Audit plan	Given finite resources (*e.g.* auditors, auditees, time, money, management support), audit engagements are prioritised, scoped, and scheduled to optimise the value generated by satisfying audit objectives, *e.g.* providing assurance regarding the organisation's management of significant risks or compliance. "1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion. Notes: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work. 2. A high-level description of the audit work to be performed in a certain period of time" *(ISACA glossary)*.

TERM	MEANING
Audit program	Plan for an individual audit engagement. "A step-by-step set of audit procedures and instructions that should be performed to complete an audit" *(ISACA glossary)*.
Audit record	Record in an audit log or trail, or pertinent evidence obtained by auditors during the course of an audit engagement. "An individual entry in an audit log related to an audited event" *(NIST SP 800-171)*.
Audit responsibility	Responsibility associated with auditing, such as considering the evidence dispassionately, without bias, prejudice, fear, or favour. "The roles, scope and objectives documented in the service level agreement (SLA) between management and audit" *(ISACA glossary)*.
Audit risk	Risk affecting or arising from audit engagements such as misinformation, disinformation, deception, collusion, coercion, social engineering, bribery, fraud, false or misleading accusations; management interference, pressure, diversion or misdirection, inappropriate restriction or exploitation of privileged access; accidental damage to the information security of information systems, data or information; noncompliance, nonconformity; inappropriate/undue reliance on ineffective, inaccurate, or unreliable information, controls, people, organisations, systems, processes, reports, plans, promises, *etc*.; scope, budget or timescale blowouts, inordinate delays, untimely reporting; incompetent, inept or plain lazy auditing, poor planning, inadequate resourcing, failing to identify, correctly diagnose or disclose relevant matters, inadequate, inaccurate, incomplete or misleading assurance; undue stress, intimidation, threats, physical violence, *etc*. "The risk of reaching an incorrect conclusion based upon audit findings. Notes: The three components of audit risk are: Control risk; Detection risk; Inherent risk" *(ISACA glossary)*. See also audit subject matter risk.
Audit sampling	It unusual to be able to analyse *all* data points in depth during an audit engagement, so most audits involve a representative subset of the data selected by the auditor/s using an appropriate sampling method. "The application of audit procedures to less than 100 percent of the items within a population to obtain evidence about a particular characteristic of the population" *(ISACA glossary)*. See also data sample, random sample, stratified sample, systematic stratified sample, time series analysis, attribute sample, discovery sample.
Audit scope	Scope (intended and authorised coverage, less any explicit exclusions) of an individual audit or of the audit function as a whole. "Extent and boundaries of an audit. Notes: The audit scope generally includes a description of the physical and virtual-locations, functions, organizational units, activities and processes, as well as the time period covered; A virtual location is where an organization performs work or provides a service using an on-line environment allowing individuals irrespective of physical locations to execute processes" *(ISO 19011)*.

TERM	MEANING
Audit subject matter risk	Risk associated with whatever is being audited. "The risk relevant to the area under review: Business risk (customer capability to pay, credit worthiness, market factors, *etc*.); Contract risk (liability, price, type, penalties, *etc*.); Country risk (political, environment, security, *etc*.); Project risk (resources, skill set, methodology, product stability, *etc*.); Technology risk (solution, architecture, hardware and software infrastructure network, delivery channels, *etc*.)" *(ISACA glossary)*.
Audit time	The allotted hour, day, week, period or eternity in which audits take place. Strangely, the clock runs slower for auditees than for auditors, a phenomenon known as audit relativity. "Time needed to plan and accomplish a complete and effective audit of the client organization's management system" *(ISO/IEC 17021-1)*.
Audit tools	"Automated tools to aid the analysis of the contents of audit logs" *(ISO/IEC 27033-1)*.
Audit trail	Chronological records of important transactions or stages in a business or computer process, which may be used to reconstruct the exact sequence of events, *e.g.* an **I**nformation **T**echnology system security log is typically configured to record important information such as successful and failed system logons, and security alarms and alerts with timestamps. "A logical path linking a sequence of events, in the form of data, used to trace the transactions that have affected the contents of a record" *(ISACA glossary)*. "Data collected for the potential use in a security audit" *(ISO/IEC 2382)*. *Cf*. audit log.
Audit universe	Expansive view of all the in-scope areas or aspects (auditable units) that might potentially be audited at some point. "An inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process. Notes: Traditionally, the list includes all financial and key operational systems and other units that would be audited as part of the overall cycle of planned work. The audit universe serves as the source from which the annual audit schedule is prepared. The universe will be periodically revised to reflect changes in the overall risk profile" *(ISACA glossary)*. See also audit plan.
Augmented intelligence	Combination or supplementation of natural human intelligence with **A**rtificial **I**ntelligence.

TERM	MEANING
Augmented reality	Real-time computer analysis of a scene to provide supplementary information, *e.g.* a 'head-up display' with a computer-generated visual overlay superimposed on the real scene, or 'force feedback' giving a pilot or driver physical cues through the vehicle controls about potentially dangerous operating conditions. "A computer-generated simulation that adds enhancements to existing reality enabling a user to interact with reality in a more meaningful way. It is often accessed through mobile applications that blend digital enhancements with the real world while ensuring that the user can easily distinguish between the two" *(ISACA glossary)*.
AUP	*Abbrev:* **A**cceptable **U**se **P**olicy.
Australia **I**nformation **S**ecurity **M**anual **(AusISM)**	"A cybersecurity framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems, applications and data from cyberthreats. The ISM is intended for chief information security officers, chief information officers, cybersecurity professionals and information technology managers." More info: https://www.cyber.gov.au/business-and-government/cyber-security-frameworks/ism
Australian **C**yber **S**ecurity **C**entre **(ACSC)**	Australian government's cybersecurity agency. Part of the **A**ustralian **S**ignals **D**irectorate, based at the **A**ustralian **S**ignals **I**ntelligence **O**rganisation in Canberra. Spooky. More info: https://www.cyber.gov.au/about-us
Authentic, authenticity	Verifiably genuine, not counterfeit or fake. "Property that an entity is what it claims to be" *(ISO/IEC 27002)*. "The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator" *(NIST SP 800-39)*.
Authentication, authentication control, authenticate	Control process or mechanism in which a specific individual user, system, message, block of data, *etc.* is positively identified and confirmed authentic, typically on the basis of something they know (*e.g.* a secret password) and sometimes something they have (credentials), something they are (meaning biometrics), and/or where they are (their virtual/network or physical location). Usually involves cryptography. Authentication is a critical and hence inherently risky control: if the process fails, is bypassed, undermined, spoofed, or disabled, dependent security controls (such as access controls, audit trails, logging, and alerting) are also rendered ineffective, often with no indication initially of anything amiss. "Act of verifying the claimed identity of an entity" *(ISO/IEC 2382)*. "Provision of assurance that a claimed characteristic of an entity is correct" *(ISO/IEC 27002)*. "1. The act of verifying identity, *i.e.*, user, system. Note: Can also refer to the verification of the correctness of a piece of data. [or] 2. The act of verifying the identity of a user or the user's eligibility to access computerized information.

TERM	MEANING
	Note: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data" *(ISACA glossary)*. "The process of identifying an individual, device or system before granting access to system resources or data. Usually based on a set of credentials such as an identifier (such as a user or device name) and an authenticator (such as a password or some other authentication factor). Authentication is distinct from Authorisation" *(NZISM)*. "Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system" *(AusISM)*. "Process of confirming the correctness of the claimed identity" *(SANS glossary)*. "A set of controls that are used to verify the identity of a user, or other entity, interacting with the software" *(SCP QRG)*. "The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data" *(**T**rust **S**ervices **C**riteria)*. "The process of verifying the identity, or other attributes of a user, process or device" *(UK National Cyber Security Strategy 2022)*. "Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system" *(NIST SP 800-171)*. See also authorisation, validation, verification.
Authentication**,** **A**uthorisation**,** and **A**ccounting **(AAA)**	Important computer security controls associated with the logon process, *i.e.* authentication to verify the user's claimed identity, authorisation or allocation of the user's defined access rights and permissions, and logging relevant details concerning the user's logon and subsequent activities for accounting, accountability, and auditing purposes. See also **I**dentification **& A**uthentication.
Authentication **H**eader **(AH)**	"The protocol used to provide connectionless integrity and data-origin authentication for Internet Protocol (IP) datagrams and to provide protection against replays (RFC 4302). Notes: AH ensures data integrity with a checksum that a message authentication code, such as MD5, generates. To ensure data-origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the IP authentication header" *(ISACA glossary)*. "Part of the protocol used for authentication within IPSec, it provides authentication, integrity and anti-replay for the entire packet (both the header and data payload)" *(NZISM)*. "A protocol used in Internet Protocol Security (IPsec) that provides data integrity and data origin authenticity but not confidentiality" *(AusISM)*.
Authentication mechanism	Means of authenticating something or someone's asserted identity, validity, *etc*. "Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device" *(NIST SP 800-101)*.

TERM	MEANING
Authentication system	"A system or mechanism used to identify a user through associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system, user directory service, or within an authentication server. Examples of authentication systems can include active directory, MultiFactor Authentication (MFA), biometrics, and tokens" *(CIS Controls)*.
Authenticator	See token. "Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was previously referred to as a token" *(NIST SP 800-63-4)*.
Authenticator **A**ssurance **L**evel **(AAL)**	"A category describing the strength of the authentication process" *(NIST SP 800-63-3)*.
Authenticity	Measure of truth, authenticity, and veracity. "Property that an entity is what it claims to be" *(ISO/IEC 27000)*. "The concept of undisputed authorship" *(ISACA glossary)*. "Validity and conformance of the original information" *(SANS glossary)*.
Authorisation, authorise, approval	Permitted, accepted, and/or agreed by management or some other authority as being in the best interests of the organisation, the workforce, the stakeholders, or society at large. "Granting of rights, which includes the granting of access based on access rights" *(ISO/IEC 2382)*. "The process of determining if the end user is permitted to have access to an information asset or the information system containing the asset" *(ISACA glossary)*. "The process of granting (or revoking) access privileges to an individual, device or system" *(NZISM)*. "Approval, permission, or empowerment for someone or something to do something" *(SANS glossary)*. "The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls" *(NIST SP 800-39)*. "A set of controls that grant or deny a user, or other entity, access to a system resource. This is usually based on hierarchical roles and individual privileges within a role, but also includes system to system interactions" *(SCP QRG)*. "The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access" *(**T**rust **S**ervices **C**riteria)*. *Cf.* unauthorised.

TERM	MEANING
Authorisation system	"A system or mechanism used to determine access levels or user/client privileges related to system resources including files, services, computer programs, data, and application features. An authorization system grants or denies access to a resource based on the user's identity. Examples of authorization systems can include active directory, access control lists, and role-based access control lists" *(CIS Controls)*.
Authorised representative	"A natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks" *(EU CRA)*.
Authorising officer	"An executive with the authority to formally accept the security risks associated with the operation of a system and to authorise it to operate" *(AusISM)*.
Authority	a. Person, rôle, organisation, *etc.* of high status or seniority (such as a manager, regulator, government agency, tribal elder, or significant other) or a stakeholder that commands respect, compliance, and/or obedience, thus exerting influence or control over subordinates by the threat or action of calling them to account. b. Power to make decisions, allocate resources, determine priorities, *etc*.
Autodiscovery	Some servers advertise their information services (such as multimedia or printing) by routinely broadcasting network messages, allowing them to be 'discovered' (contacted, used) by other nodes on the network.
Automated application control	Application control that operates automatically, without contemporaneous human intervention. "The controls that have been programmed and embedded within an application" *(ISACA glossary)*.
Automated **C**ertificate **M**anagement **E**nvironment **(ACME)**	Protocol for administering digital certificates, defined in RFC 8555. More info: https://www.rfc-editor.org/info/rfc8555
Automated control	Control embedded in an electronic or mechanical system, capable of operating automatically or autonomously, without contemporaneous human intervention, *e.g.* the governor on a steam engine. See also automated application control. *Cf.* manual control.
Automated decision-making	"Process of making a decision by automated means without any human involvement" *(ISO/IEC 27562)*.

TERM	MEANING
Automated testing	Many forms of testing can be partially if not fully automated, ranging from simply recording and replaying manual tests (*e.g.* for regression testing and multiple-choice tests for professional qualifications) to systematically applying varying loads in stress testing or checking the quality and security of complex source code. Testing tools or suites can help by: generating and managing test data and environments (*e.g.* virtual systems); planning, orchestrating, and executing tests; dynamically modifying, curtailing, or extending tests depending on findings; measuring and recording, analysing, evaluating, and reporting test results.
Automatic, automation, automated	Works independently and mechanistically, without contemporaneous and deliberate human involvement or action. "Pertaining to a process or system that, under specified conditions, functions without human intervention" *(ISO/IEC 22989)*. See also autonomous.
Automatic summarisation	"Task of shortening a portion of natural language content or text while retaining important semantic information" *(ISO/IEC 22989)*.
Automation and control solution	Product allegedly able to satisfy customer requirements for automation and control, thereby 'solving' their problems.
Automation and **C**ontrol **S**ystem **(ACS), automation system**	**O**perational **T**echnology system.
Autonomous, autonomy	Self-determined and self-controlled, capable of operating independently, receiving and analysing sensory inputs, making smart decisions and taking appropriate actions without contemporaneous human intervention, *e.g.* self-driving/driverless cars, drones, and robots. "Characteristic of a system that is capable of modifying its intended domain of use or goal without external intervention, control or oversight" *(ISO/IEC 22989)*. See also automatic.
Autonomous system	Autonomous system. "One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN)" *(SANS glossary)*. "A collection of IP networks for which the routing is under the control of a specific entity or domain" *(UK National Cyber Security Strategy 2022)*.
Autonomous weapon	'Fire-and-forget' cyberweapon capable of acting autonomously using **A**rtificial **I**ntelligence to complete complex reconnaissance, surveillance, and/or combat missions with little if any direct involvement and real-time control by human operators, in contrast to remote-controlled or dumb weapons. May be a physical device or malware.
Autorooter	Software tool (malware) that gives hackers or script kiddies highly privileged 'root' access to vulnerable systems.

TERM	MEANING
Availability	Core objective of information security, along with confidentiality and integrity comprising the CIA triad. Availability primarily concerns the requirement for information, systems, people, and processes to be operational and accessible when needed, implying the use of resilience and/or recovery controls to guard against unacceptable disruption or interruption of necessary services. "Ability of a functional unit to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided. Note: The availability defined here is an intrinsic availability where external resources other than maintenance resources do not affect the availability of the functional unit. Operational availability, on the other hand, requires that the external resources be provided. [and] property of data or of resources being accessible and usable on demand by an authorized entity" *(ISO/IEC 2382)*. "Property of being accessible and usable upon demand by an authorized entity" *(ISO/IEC 27000)*. "The ability to ensure timely and reliable access to, and use of, information" *(ISACA glossary)*. "The assurance that systems and data are accessible and useable by authorised entities when required" *(AusISM)*. "The need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it" *(SANS glossary)*. "A measure of a system's accessibility and usability" *(SCP QRG)*. "Ensuring timely and reliable access to and use of information" *(NIST SP 800-171)*.
Availability control	Control designed to mitigate unacceptable availability risks. Its main purpose is to maintain availability of information and information services at a desired or necessary level (resilience and performance), or to regain availability following an incident or outage (recovery). See also integrity control, confidentiality control.
Availability risk	Risk involving or affecting the availability of information, such as uncertainty as to whether it will or will not be accessible when actually required for some purpose, leading to unclear consequences. "The risk that service may be lost or data are not accessible when needed" *(ISACA glossary)*. See also information risk, information security risk, confidentiality risk, integrity risk.
Avalanche	Global cybercriminal botnet infrastructure used for phishing, malware distribution, and money mule recruitment.
Average precision	Measurement function used to improve the quality of **A**rtificial **I**ntelligence models. "A metric for summarizing the performance of a ranked sequence of results. Average precision is calculated by taking the average of the precision values for each relevant result in a ranked list (each result in the ranked list where the recall increases relative to the previous result)" *(ISACA glossary)*.

TERM	MEANING
Avoid design option	See risk avoidance. "A design option to cease all activity or terminate sources that give rise to the opportunity, obstacle, or obligation" *(OCEG GRC Glossary)*.
Aware, awareness	Vigilant and alert, with a heightened capability to recognise, appreciate, and respond appropriately and promptly to changing circumstances. "The idea of being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly" *(ISACA glossary)*. See also security awareness.
AWS	*Abbrev:* **A**mazon **W**eb **S**ervices.
Axiom	Fundamental information security policy requirement, architectural principle, or rule. Axioms may be derived from first principles, and/or from sources such as the control objectives originally defined in BS 7799 to justify and underpin the organisation's information security policy statements, standards, procedures, guidelines, and controls.
Azure	Brand name for Microsoft's global cloud infrastructure. See also **A**mazon **W**eb **S**ervices, **G**oogle **C**loud **P**latform.
Azure Active Directory	See Microsoft Entra ID.