Definitions

Updated: 18 March 2025

If you and your organization use different terms or scope, that is ok; just think about your wording with my scope or whether your scope of that term is broad enough.

Term	My Perspective Definition
ALL	*All* in every language is All – All business units, all employees, all contractors, all suppliers, all countries, all customers, etc.
Analytics	The evaluation of information or data to ask and answer questions that drive changes in an organization.
Assessment	Checklist (egad), tools, the pen test, tabletop, etc.) – finding and hopefully exploiting vulnerabilities with actionable solutions.
Asset	Hard/physical asset (e.g., building), electronic asset (e.g., stuff on a computer), intellectual property, processes, people.
Assets	Physical, Electronic, and Intellectual Assets that have a material impact/risk to the organization, suppliers, companies, and societies.
Audit	The (independent) verification and validation of a control to verify it meets the legal, regulatory, or business need to protect the business, government, or consumer.
Authorized Fraud	The commitment of fraud by a person that is technically approved/authorized to perform a specific function. They just abuse that authority to commit the fraud.
Background Investigations	Investigations that are generally PROACTIVE on the review of the background of a person (background checks/investigations) or company (due diligence) to determine the viability and integrity of the individual or company before a relationship is established or renewed.
Buildings	Locations where an organization's assets are located, this can be as simple as a cinder-blocked building, a supplier's warehouse, all the way to interesting "buildings" like "street furniture" (an old Telco term).

Term	My Perspective Definition
Classified information vs. information classification	Classically speaking, *classified information* has been tied to sensitive and critical information assets that need protection for national security interests. Whereas *information classification* is, the establishment of information owner-defined labels and controls for an organization's non-public information. These terms have been used interchangeably, but, classically, *classified information* is, actually, the implementation of *information classification* in a government/national security environment.
Compliant	A term that indicates an assessed element (organization, process, technology, function) meets the requirements of a documented standard, generally accepted set of requirements, law, regulation, or legally binding document like a contract. *Compliant* does not mean the element is secure.
Cyber Security	The functional role, hopefully in a converged security program, to "Secure stuff with wires" from breaches in confidentiality, integrity, and availability.
Distributor/ Distribution	A middle entity or person in the supply chain of a product somewhere between manufacturer and end user.
Enterprise-wide	A way of describing the scope of an element of a security program/function/project where it represents all organization elements under the Chief Executive Officer.
Ethical Stop	A term I coined many years ago in my fraud and insider threat presentations and classes; the goal of a security and ethics department to encourage people to not go beyond a certain point of unethical behavior. For instance, stop at stealing pens …
First Responder	An individual trained in one or more emergency response disciplines that is generally (part of) the first individuals on the scene to care for others or prevent further crisis.
Fraud	Any activity that relies on deception in order to achieve a gain. Fraud becomes a crime (thus a security concern) when it is a *knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment* based on the Fraud Triangle.
Fraud Investigations	Sometimes called a *Fraud Examination*; investigations that specifically focus on fraud and usually involve specialized skill sets around financial crimes, occupational fraud, and fraud analytics. (I hope to do a *Top 25* just in this area in the next edition.)

Term	My Perspective Definition
Fraud Management	The end-to-end coverage of activities involved in preventing, discovering, investigating, and mitigating fraud, including but not limited to fraud awareness, pro-active fraud analytics, pre-deploy fraud assessments, mitigation, or corrective active project management … oh, and investigations.
HR Investigations	Personnel investigations that involved employees and usually, but not always, are run by HR team members and not the security department. These investigations tend to involve, what some people might call social policy violations, like hostile work environments, and sexual harassment.
Incident Response	This is the immediate reaction to some type of safety or security incident and involves steps to reestablish a safe environment for ongoing business operations. There may be one or more investigations after the priority of response is completed to figure out the cause and ongoing mitigation that triggered the incident.
Information	Classic definition: facts provided or learned about something or someone. Contextual definition: facts supplied or learned about an organization's assets or assets it is entrusted to manage (and secure) regardless of form or where it is located.
Information Security	The prevention, detection, and corrective/response actions to protect the confidentiality, integrity, and availability of an organization's information or information entrusted to the organization.
Information Security vs. (Cyber, Application, Network, Privacy, etc. Security)	It has been said that *cyber security* was once defined as *secure things with wires*. The securing of electronic stuff tends to incorporate not ***just*** security of information, but also the security of services operating within the technology of *cyber*, *applications*, and *networks*. Security of both information and these other areas are important, but without information, organizations do not exist; without technology-based services, organizations cannot run.
Infrastructure	I like to think of infrastructure as all that technology you do not see, but unplug it, do not maintain it, and your security department and security controls go downhill fast.

Term	My Perspective Definition
Insider Threat	The pre-action awareness and indicators of an insider in an organization is planning to commit a security offense in the near future. Insider Threat has also been used as the label for the prevention, detection, and response to an insider's malicious actions.
Insider Threat (Non-Malicious)	A term sometimes used to show that an insider is seen/used to carry out a malicious act, but the insider is simply following standard protocols or weak controls. Another malicious party (insider or outsider), generally has social-engineered this insider to help malicious party.
Investigations	The collection, analysis, and reporting of the facts to prove or disprove an allegation of wrongdoing or incident. Facts can include, but are not limited to, any evidence detectable or performed by the five senses. Investigations can include areas such as a safety investigation (e.g., derailment of a train) that is not necessarily a security investigation. Investigations, in this *Top 25*'s context are not limited to any specific group of human victims or perpetrators.
Law Enforcement Agency	An entity commissioned by the laws of the land to prevent, detect, respond to crime committed against individuals, companies, governments, or property.
Link Analysis	An analytical investigative technology that is usually presented visually on a board or with software, to connect elements, entities, evidence of an incident, background check, or due diligence to better visualize interconnections and possible related incidents.
Loss Prevention	Usually tied to the retail, transportation, logistics industry, with focus on preventing and investigating the thief of products throughout the supply chain.
Pen Test	A structured (hopefully) vulnerability exploitation process to test prevention, detection, and response controls of a target. This target is usually a technology-based target or physical building/area-based target. Using and exploiting people, process, technology, tools, and buildings to accomplish this scope of the test.
Personnel	Employees and non-employees (e.g., suppliers or contractors) with physical access or logical/electronic access to your (confidential) assets. Generally, this does not include the public or customers.

Term	My Perspective Definition
Personnel Investigations	Specific investigation area that is focused on allegations involving employees. Some people will also include contractors in this area.
Risk	The (hopefully measured) probability of *something bad is going to happen*.
Risk Management	The management of controls to reduce the probability that *something bad is going to happen* to the lowest level practical for an organization, taking into considering brand, legal, cost, operations, productivity, etc.
Security	The prevention and detection of, and response to a crime or violation of company policy.
Security Assessment	The assessment of the defined scope to determine if the assets of that scope are susceptible to (or even a victim of) being part of a crime or violation of an organization's policies.
Security Audit	The assessment of the defined scope to determine if the assets of that scope are susceptible to (or even a victim of) being part of a crime or violation of an organization's policies. Security Audits are also tied to compliance scope and usually reported to a board, audit committee, or other oversight organization.
Security Department Technology	The tools used or managed by the Security Department such as websites, databases, analytics tools, desktops, servers, IoT, applications, network, mobile devices, or software (open source, commercial, proprietary).
Security Investigations	An investigation that involves a crime or violation of an organization's policies/Code of Conduct.
Security Response	The tools, techniques, and procedures used to prevent, detect, and respond to an incident (observe–orient–decide–act (OODA) Loop anyone).
Software	Firmware, disk-based software, cloud-based software, operating system level, database level, application level, etc.
Subcontractors	Any external entity, which is used by your direct suppliers, from which you get products or services, that affect the risk to the company, regardless of whether you pay them directly or indirectly, and regardless of whether you have them under contract.

Term	My Perspective Definition
Supply Chain (aka vendor, supplier, third-party)	Any external entity that you get products or services from, that affect the risk to the company, regardless of whether you pay them directly or indirectly, and regardless of whether you have them under contract. (More detailed discussion on "What is a supplier?" is posted in my documents on LinkedIn.)
Supply Chain Investigations	Investigations that involve a supplier or vendor and the organization. Like other specialized investigations, this one also takes special skill sets to cover the unique attributes related to the supply chain.
Threat	The direct or implied communication of intent to inflict harm or loss on another person, entity.
Threat Assessment	The one-time or recurring evaluation of actions, indicators, or communications by a person, entity, or technology that is believed to be planning a breach, attack or other malicious action against another person, technology, or entity.
Threat Management	The ongoing actions to prevent, detect, and respond to threats by an individual, entity, or technology.
Training	The education of an individual through any organization's acceptable means, which is trackable, culturally adapted, that communicates, shows implementation, and tests students on the security, rules, standards, guidelines, good practices, procedures recommended and required for an organization's safe and secure success. This does not mean an organization's employee is the trainer/teacher, but I do recommend a dedicated employee manage the training program.
Training Sustainment Timing	Some training should be yearly, and some monthly; some training should be recurring via, say, a screen saver splash screen. Some should be repeating the same training, others should get naturally more challenging than the last class.
Vulnerability	Weakness in a physical or electronic asset, procedure, or implementation, which could be exploited or triggered by a threat source or operational security assessor. I understand that some people, cultures, environments, or organizations do not like the word *vulnerability*, so they will soften it with the phrase *security gap*. I am not going to go there, I respect the organization's culture, political, and optics challenges, but I'm going to stick with *vulnerability*.

Term	My Perspective Definition
Vulnerability Assessment	The discovery or detection of weaknesses in people, processes, technology, or other company assets (e.g., buildings) that would make them susceptible to being used to commit a crime or violation of organizational policies. This assessment could also involve probability, mitigation, and impact.
Vulnerability Discovery	The malicious or operational security method for finding a vulnerability in a person, physical asset, electronic asset, procedure, or implementation. *Discovery* does not necessarily mean the vulnerability was exploited. For example, I see a door with poor outside hinges or I find a computer running EOL/EOS software, but in either case, I do not take advantage of these findings and compromise the asset.
Vulnerability Exploit(ed)	The active application of methods that uses the discovered weakness to take advantage of the weakness to compromise an asset by the threat source or operational security assessor.
Vulnerability Management	The ongoing actions to prevent, detect, and respond to threats by an individual, entity, or technology. Some may consider this patch management, but patch management is just a subset of overall vulnerability management.
Wholesale	A middle entity or person in the supply chain of a product somewhere between manufacturer and end user. Usually, the first entity after the manufacturer that sells to various parties, but not usually a retail consumer.