UCF Impact Zone List

The UCF breaks down Common Controls into sections based on the scope of an audit. These sections are referred to as Impact Zones.

Here is the listing that is most current.

- **Leadership and High Level Objectives** - Common Controls that cover the establishing of high level objectives coordinating of strategy with an organization's top leadership and the organization's IS staff's tactics.
- **Audits and Risk Management** - Common Controls that cover the identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks.
- **Monitoring and measurement** - Common Controls that cover the processes of surveillance in order to observe, record, or detect and then giving an account or statement describing in detail an event, situation, or the like, usually as the result of the monitoring activities.
- **Technical Security** - Common Controls that cover the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Access management, identity verification, data protection within and across networks, within databases and records archives, and down to individual computers and their software are all covered within this impact zone.
- **Physical and environmental protection** - Common Controls that cover the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
- **Operational and Systems Continuity** - Common Controls that cover the practice of protecting an Information Technology system against three classifications of threats; Natural threats such as hurricane, tornado, flood, and fire; Human threats such as operator error, sabotage, implant of malicious code, and terrorist attacks; and Environmental threats such as equipment failure, software error, telecommunications network outage, and electric power failure.
- **Human Resources Management -** Common Controls that focus on the areas of identity management, background checks, separation of duties (and when it doesn't make sense), considerations for outsourcing and consulting services, supervision strategies, team development and communication, budgeting, recruiting, job definitions, performance discipline, and more.
- **Operational Management** - Common Controls that cover the management of the design, execution, and control of operations that convert resources into desired goods and services and implement an organization's business strategy.
- **System hardening through configuration management -** Common Controls the activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
- **Records Management** - Common Controls that cover the set of activities required for systematically controlling the

creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.

- **Systems design, build, and implementation** - Common Controls that cover the development of the organization products, including records created to initiate new product design and specification information, produce ability studies, design and specification of spares, research and development records that may or may not result in actual product development, and contract research records regarding new products.
- **Acquisition or sale of facilities, technology, and services -** Common Controls that cover the purchasing of products and services or acquiring organizations (or their assets), or the giving or handing over to a buyer assets or services for money. The complex equation of scoping, assessing, sourcing, and implementing acquired technologies.
- **Privacy protection for information and data** - Common Controls that cover the right of individuals to control or influence information that is related to them in terms of who may collect or store it and to whom that information may be disclosed, as well as how personal information is collected, used, retained and disclosed in conformity with the commitments an organization makes in its privacy notice.
- **Harmonization Methods and Manual of Style -** Common Controls that cover the organization and language structure of an organization's compliance documents.
- **Third Party and supply chain oversight** - Common Controls that cover the intersection of managing the supply chain and third parties. Supply chain management is the oversight of materials, information, and finances as they move in a process from supplier to manufacturer to wholesaler to retailer to consumer. Supply chain management involves coordinating and integrating these flows both within and among companies, i.e., Third Parties. Third party management is the process whereby companies monitor and manage interactions with all external parties with which it has a relationship.

Visit our website so see the documents we’ve mapped.

www.CommonControlsHub.com

Contact sales@unifiedcompliance.com for more information about signing up for a CommonControlsHub Basic Subscription.