ASSET CODES

ID_Asset Category_Asset Type	Details	Examples
B1_BUSINESS PROCESSES_CRITICAL	Processes - those whose loss or degradation make it impossible to do business	Web hosting, links to on-line terminals
B2_BUSINESS PROCESSES_SECRET	Processes - those processes that are secret or involve proprietary technology	Development of source code, patents pending, IP register
B3_BUSINESS PROCESSES_KEY	Processes - those processes that, if modified, can greatly affect the accomplishment of the organisation's mission	Client billing, monitoring of core systems
B4_BUSINESS PROCESSES_REGULATORY	Processes - those that are necessary to comply with contractual, legal or regulatory requirements	Maintaining privacy of personal information, regulatory reporting
I1_INFORMATION_CONFIDENTIAL	Information for the exercise of the business	Financial data, tendering data, payroll, policies and procedures
I2_INFORMATION_RESTRICTED	"Restricted" information	Client personal data, HR data
I3_INFORMATION_INTERNAL	"Internal Use"	Business plans, budget information, marketing strategies
I4_INFORMATION_PUBLIC	"Public"	Everyone can see this information
I5_INFORMATION_HARDCOPY	Hardcopy Record	Documentation, contracts, paper, slide, transparency
H1_HARDWARE_SERVER	Server	domain controllers, database servers, virtual hosts
H2_HARDWARE_WORKSTATION	Workstation	computers, laptops
H3_HARDWARE_STORAGE	Storage	SAN, NAS
H4_HARDWARE_MOBILE	Mobile Device	cell, tablet
H5_HARDWARE_PERIPHERAL	Processing Peripheral	Printer
S1_SOFTWARE_OS	Operating system	Windows, Linux
S4_SOFTWARE_SUPPORTING	Service, maintenance or administration software	Anti-virus, backup, security system
S2_SOFTWARE_APPLICATION	Standard business application	Financial, CRM, ERP (almost limitless list)
S3_SOFTWARE_CUSTOM	Specific business application	Customized software such as real time monitoring application, data linkage software (also limitless)
N1_NETWORK_CONNECTIVITY	Connectivity	LAN, WAN, WiFi
N2_NETWORK_DEVICES	Devices	switches, routers, firewalls
N3_NETWORK_TELEPHONY	Telephony	PBX, VOIP, Unified Communications
N4_NETWORK_CLOUD	Cloud	SaaS, IaaS, PaaS
P1_PERSONNEL_MANAGEMENT	Management	decision makers, project leaders
P2_PERSONNEL_OPERATIONS	Operations	System administrator, data administrator, network, Help Desk
P3_PERSONNEL_DEVELOPERS	Developers	Application developers

ASSET CODES

ID_Asset Category_Asset Type	Details	Examples
F1_FACILITIES_EXTERNAL	External environment	Premises outside of org's control (homes of personnel, another org's premises, hazard area)
F2_FACILITIES_PREMISES	Premises	Organization's perimeter (buildings, establishment)
F3_FACILITIES_BRANCH	Branch zone	Offices, reserved access zone, secure zone
F4_FACILITIES_ESSENTIAL	Essential services	Services required for org's equipment to operate
F5_FACILITIES_COMMUNICATION	Communication	Telephone line, PABX, internal phone networks
F6_FACILITIES_UTILITIES	Utilities	Power supply, water supply, waste disposal, air conditioning, chilled water pipes

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
V1_ SENSITIVE DATA_IDENTIFICATION	Sensitive data needs to identified and classified. Locate sensitive data throughout the enterprise. A significant amount of sensitive data in a single location poses a high risk due to damage possible from a single breach.
V2_SENSITIVE DATA_CLASSIFICATION	Data needs to be classified and clearly defined. A classification scheme needs to be established throughout the organization based on criticality and sensitivity. Ineffective classification processes can cost the organization through breaches and lost productivity.
V3_SENSITIVE DATA_PROTECTION	Vital data needs to be identified, and a strategy for protection and recovery developed and maintained in order to mitigate the risk of data loss.
V4_SENSITIVE DATA_DATA LOSS PREVENTION	Data loss prevention tools are critical to identify, monitor and protect data in storage as well as in motion over the network. These tools secure your system against data leaks and protection against unauthorized entry or use.
V5_SENSITIVE MEDIA_SANITIZATION	Physical storage resources: sensitive data may leak because data destruction policies applicable at the end of a lifecycle may either be impossible to implement because, for example, media cannot be physically destroyed because a disk is still being used by another business unit or it cannot be located, or no procedure is in place. A retention and disposition policy must be created that defines the timeframes during which documents for operational, legal, fiscal or historical value must be maintained.

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
V6_ CYBERSECURITY_PROGRAM	An organization must identify reasonably foreseeable internal and external risks pertaining to security, confidentiality, and integrity of the information and systems as part of an information security program. The need to shield information from malicious actors is a concern at the highest levels of business and government.
V7_ CYBERSECURITY_TRAINING	Negligent employees, contractors and third-party vendors represent the cause of over half of all enterprise data breaches.
V8_CYBERSECURITY_MATURITY	Independent third-party security assessments are crucial in order to address the adequacy of policies and procedures defined in your organizations cybersecurity program (V6).
V9_SECURITY LIFECYCLE_SYSTEM ACCESS	Sound system access policies and procedures must be in place in order to mitigate the risk of unauthorized access to corporate data.
V10_SECURITY LIFECYCLE_THIRD-PARTY ACCESS	Third-party vendors should have restricted access to systems as defined.
V11_SECURITY LIFECYCLE_PATCH MANAGEMENT	Failure to follow adequate patch management procedures greatly increases the risk of falling victim to a cyber attack or other security breaches. Global ransomware hacks occur daily as a result of poor patch management. These unattended vulnerabilities in IT infrastructure open companies up to numerous security challenges.
V12_SECURITY LIFECYCLE_RESOURCE ALLOCATION	Sufficient resources (both human and financial) are essential to successfully implement security requirements and initiatives. Third-party SME’s should be leveraged as required.
V13_SERVICE MANAGEMENT_CHANGE MANAGEMENT	When an organization employs a weak change management process, more than just money is going to be lost. In fact, there are both short term and long term, direct and indirect costs to the organization.
V14_SERVICE MANAGEMENT_INCIDENT MANAGEMENT	Formal incident management is required in handling any interruptions that occur so as to restore operation /services back to normal [as planned] as soon as possible. The importance is to minimize its impact on business operation/service.

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
V15_SERVICE MANAGEMENT_PROBLEM MANAGEMENT	The ITIL problem management process investigates recurring incidents, the root cause of incidents, and provides a formal focus on incident prevention. Without a formal problem management capability, these activities tend to fall into a black hole.
V16_SERVICE MANAGEMENT_KNOWLEDGE MANAGEMENT	Knowledge management is a required discipline that promotes an integrated approach to identifying, capturing, evaluating, retrieving, and sharing all of an enterprise's information assets. These assets may include databases, documents, policies, procedures, and previously un-captured expertise and experience in individual workers.
V17_SERVICE MANAGEMENT_ASSET MANAGEMENT	Asset management allows the organization to keep track of all their IT assets. It can tell where the assets are located, how they are used, and when changes were made to them. It is important for a company to implement an asset management system to assist in the monitoring of assets, as well as in the asset recovery process.
V18_SYSTEM AND DATA INTEGRITY_HIGH AVAILABILITY	It is important to ensure critical data is readily available in situations like server crash, breach, or other data disaster.
V19_SYSTEM AND DATA INTEGRITY_ANTI-VIRUS	Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete. It is time to think beyond traditional antivirus.
V20_SYSTEM AND DATA INTEGRITY_INTRUSION DETECTION	The main reason behind the advent of IDS is that firewalls and access control on their own do not provide an adequate defence against attack. Therefore IDS must be used to monitor network assets to detect anomalous behaviour and misuse in network.
V21_SYSTEM AND DATA INTEGRITY_SECURITY MANAGEMENT	Security checks need to be performed periodically on essential, life/safety and private data systems e.g. patch levels, access controls, configuration settings, etc. in order to mitigate the risk of a system outage.
V22_NETWORK RESILIENCY_SINGLE POINT OF FAILURE	Taking the time to assess potential "what if" scenarios and plan for the worst-case scenario can prevent or at least minimized the effects of system outages. Critical systems should be protected with some form of redundancy.
V23_NETWORK RESILIENCY_CONTRACT MANAGEMENT	Maintenance contracts must be managed and maintained in order to avoid unsupported hardware and software.

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
V24_NETWORK MONITORING_MONITORING	When problems take place intermittently or only at peak times, they may be difficult to identify at the time. However, when ongoing network monitoring is in place, you can follow logs like a roadmap to recognize key trends in performance and network health.
V25_NETWORK LOGGING & AUDITING_LOGGING AND REPORTING	All critical systems should have automated logging and other reporting mechanisms in place in order to provide proactive analysis's to support system investigations and audits.
V26_NETWORK LOGGING & AUDITING_SCHEDULED REVIEWS	Logs need to be reviewed on a regular basis as part of an overarching security program.
V27_IDENTIFICATION AND AUTHENTICATION_ACCESS CONTROL	Access control and permissions need to be reviewed on a scheduled basis.
V28_IDENTIFICATION AND AUTHENTICATION_ACCOUNT REVIEWS	Systems need to be reviewed on a regular basis in order to identify unauthorized accounts.
V29_BUSINESS CONTINUITY AND DISASTER RECOVERY_BACKUP	Systems are not backed up in a manner or frequency appropriate to the system criticality and type of data.
V30_BUSINESS CONTINUITY AND DISASTER RECOVERY_PLANNING	There are no formal BCP or DRP plans in place to ensure the organization has sound recovery and continuity processes.
V31_BUSINESS CONTINUITY AND DISASTER RECOVERY_ASSETS	IT asset inventories are required for all computers and network devices considered to be "in-scope" for the BCP or DRP
V32_BUSINESS CONTINUITY AND DISASTER RECOVERY_TESTING	BCP/DRP plans need to be tested at least annually.
V33_DATA CENTRE FACILITY_FIRE SUPRESSION	Inadequate fire suppression is in place within a data centre hosting IT assets.
V34_DATA CENTRE FACILITY_POWER AND COOLING	Inadequate power and/or cooling is in place within a data centre hosting IT assets.
V35_DATA CENTRE FACILITY_WATER DAMAGE	A data centre hosting corporate IT assets has deficiencies that may cause flooding or other types of general water leakage that could damage IT assets.

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
V36_RESOURCE_LOSS OF STAFF	The IT team may have the risk of losing key staff that would result in a fundamental gap in system/infrastructure knowledge.
V37_RESOURCE_CROSS-TRAINING	There are no or limited cross-training processes in place that have exposed gaps in the support of critical IT systems. For example: if a single individual were to leave the organization or be absent to a period of time, a system outage could have serious adverse effects on the delivery of IT services.
V38_CLOUD_USER PROVISIONING	a) Customer cannot control provisioning process, b) Identity of customer is not adequately verified at registration, c) Delays in synchronization between cloud system components(time wise and of profile content) happen, d) Multiple, un-synchronized copies of identity data are made, e) Credentials are vulnerable to interception and replay.
V39_CLOUD_HYPERVISOR	Hypervisor-layer attacks are very attractive: the hypervisor in fact fully controls the physical resources and the VMs running on top of it, so any vulnerability in this layer is extremely critical. Exploiting the hypervisor potentially means exploiting every VM. A typical scenario enabled by exploiting a hypervisor's vulnerability is the so called 'guest to host escape', an example of which is 'VM hopping': in which an attacker hacks a VM using some standard method and then – exploiting some hypervisor vulnerability – takes control of other VMs running on the same hypervisor.
V40_CLOUD_POOR KEY MANAGEMENT PROCEDURES	Cloud computing infrastructures require the management and storage of many different kinds of keys; examples include session keys to protect data in transit (e.g., SSL keys), file encryption keys, key pairs identifying cloud providers, key pairs identifying customers, authorization tokens and revocation certificates. Because virtual machines do not have a fixed hardware infrastructure and cloud-based content tends to be geographically distributed, it is more difficult to apply standard controls, such as hardware security module (HSM) storage, to keys on cloud infrastructures.
V41_CLOUD_LACK OF SECURITY AWARENESS	Cloud customers are not aware of the risks they could face when migrating into the cloud, particularly those risks that are generated from cloud specific threats, ie, loss of control, vendor lock-in, exhausted CP resources, etc. This lack of awareness could also affect the cloud provider who may not be aware of the actions that should be taken to mitigate these risks.

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
V42_CLOUD_INADEQUATE PHYSICAL SECURITY PROCEDURES	These can include: a) lack of physical perimeter controls (smart card authentication at entry), b) lack of electromagnetic shielding for critical assets vulnerable to eavesdropping.
V43_CLOUD_LACK OF RESOURCE ISOLATION	Resource use by one customer can affect resource use by another customer. IaaS cloud computing infrastructures mostly rely on architectural designs where physical resources are shared by multiple virtual machines and therefore multiple customers. Vulnerabilities in the hypervisor security model may lead to unauthorized access to these shared resources. For example, virtual machines of Customer 1 and Customer 2 have their virtual hard drives saved in the same shared LUN (Logical Unit Number) inside a SAN. Customer 2 may be able to map the virtual hard drive of Customer 1 to its virtual machine and see and use the data inside it.
V44_CLOUD_USER DEPROVISIONING	Deprovisioned credentials are still valid due to time delays in roll-out of revocation.
V45_CLOUD_ ENCRYPTION OF ARCHIVES AND DATA IN TRANSIT	Failure to encrypt data in transit, data held in archives and databases, un-mounted virtual machine images, forensic images and data, sensitive logs and other data at rest puts the data at risk. Of course the costs of implementing key management [V11] and processing costs must be taking account and set against the business risk introduce
V46_CLOUD_DATA PORTABILITY	The organization needs to have the ability to “move” corporate applications/data between on-premise and cloud services from different providers.
V47_CLOUD_INTEROPERABILITY	Public and private cloud services need to understand each other’s APIs, configuration, data formats and forms of authentication and authorization. Interfaces are standardized, so that the organization can switch from one cloud service to another with minimal impact to enterprise systems.
V48_CLOUD_VENDOR LOCK-IN	Vendor lock-in becomes an issue when an organization considers moving its assets/operations from one cloud provider to another. The organization discovers the cost/effort/schedule time necessary for the move is much higher than initially considered due to factors such as non-standard data formats, non-standard APIs, and reliance on one CSP's proprietary tools and unique APIs.
V49_CLOUD_PROVIDER DUE DILIGENCE	Organizations migrating to the cloud often perform insufficient due diligence. They move data to the cloud without understanding the full scope of doing so, the

VULNERABILITY CODES

ID_Vulnerability Category_Vulnerabiity Type	Details
	security measures used by the CSP, and their own responsibility to provide security measures. They make decisions to use cloud services without fully understanding how those services must be secured.
V50_CLOUD_CORPORATE CLOUD POLICY	A corporate policy on cloud usage may not exist or be inadequate (e.g. out-dated). A policy provides guidelines for secure and effective cloud computing operations to ensure the integrity and privacy of company-owned information.