ASSET - Vaultastic on AWS for Insurance - Compliance with IRDAI cyber security guidelines v1.2

	Domain	Sub Domain	Risk Statement	Controls Requirement	Availability	Comments on how the AWS platform layer addresses these requirements	Comments on how the VAULTASTIC platform addresses these requirements	Section (as per cyber security guidelines)
1.1	Physical and Logical Security	Data centre surveillance & monitoring	Absence of data centre physical security procedures may lead to unauthorized physical access	1) Physical security process / procedure document. 2) Approval authorities & levels.	Service Organization Controls 1 (SOC 1), Type II report **Section:** Physical Security and Environmental Protection	AWS' data centres are state of the art, utilizing innovative architectural and engineering approaches. AWS has many years of experience in designing, constructing, and operating large-scale data centres. This experience has been applied to the AWS platform and infrastructure. AWS data centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.	NA since we are hosted on AWS and naturally benefit from their physical security practices for the data centre	
1.2	Physical and Logical Security	Data centre surveillance & monitoring	Absence of data centre surveillance may lead to unauthorized physical access.	1) Physical separation using fences, walls and barriers. 2) Physical monitoring : Guards, reception desks, gates. 3) Electronic security : CCTV surveillance, biometric card reader, metal detector/bag scanner.	Yes. These are specifically outlined in the SOC 1 Type II report. In addition, other certifications AWS supports such as ISO 27001 and FedRAMP require best practice physical and environmental controls.	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data centre floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Centre Physical Security Policy. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.	NA since we are hosted on AWS and naturally benefit from their physical security practices for the data centre	

1.3	Physical and Logical Security	Data centre environment controls	Absence of data centre environmental controls may impact data centre systems	1) Fire Fighting Equipment: Smoke detectors, Fire extinguisher. 2) Temperature: Air conditioner type(), Provide temperature level maintained. 3) Power supply: UPS, backup generators capacity & load supported. 4) Preventive & Maintenance plan of above equipment.	Yes. Covered in Security Whitepaper	1) Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data centre environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems. 2) Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centres are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. 3) The data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centres use generators to provide back-up power for the entire facility. 4) AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.	NA since we are hosted on AWS and naturally benefit from their physical security practices for the data centre	
1.4	Physical and Logical Security	Data Centre Access	Absence of data centre access controls may lead to unauthorized access.	1) Data centre access process/procedure. 2) Logs of users/vendors/contractors accessing DC.	Yes. These are specifically outlined in the SOC 1 Type II report.	AWS only provides data centre access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centres by AWS employees is logged and audited routinely.	NA since we are hosted on AWS and naturally benefit from their physical security practices for the data centre	
1.5	Physical and Logical Security	Data centre location	Location of data centre overseas may lead to implication of various norms & regulation over data accessibility, audit, sharing etc.	1) Data Centre location	AWS has a Region in India, Mumbai	AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. Rights of determining region is with the customer	NA since we are hosted on AWS and naturally benefit from their physical security practices for the data centre	21 (1)
2.1	Data Security	Data leakage	Absence of DLP solution may lead to non identifying, monitoring & protection of sensitive data.	1) DLP solutions implemented. 2) Monitoring & escalations process.	Vaultastic has controls to prevent Data leakage	Through Vaultastic:	Mithi hosts Vaultastic as a SaaS on AWS and we control and own the data we place there. Each customer on our platform, has TOTAL ownership of their email data and they have controls via the administration panel to specify which of their users can only read their email, can export, download, print the email data, can forward, reply the email, and so on. All these actions are logged in audit trails and maintained for a period of 10 years on our site for retrieval on demand.	21 (4) 21.1 (a) III 21.1 (b) 21.3 (d)

2.2	Data Security	Data Backup & Restoration	Absence of backup & restoration controls may lead to loss of critical information.	1) Backup & restoration process/procedure document. 2) Offsite backup moment. 3) Restoration testing.	Using the highly durable S3 store for email data and using the AWS native backup mechanism to secure the server stores and configuration	AWS offers native capability for backup of the hot storage devices, server stores and databases. These backups are stored on the highly durable S3 store for easy retrieval on demand. Files can be encrypted automatically using AES-256 encryption.	Vaultastic stores all email data in the highly durable S3 store of AWS, offering a data durability of 11 9's. This store, by design, uses multiple availability zones (different Amazon data centres) to store redundant copies of the email data ensuring an offsite copy too. Vaultastic also does has no delete option making it very safe for a user at any level to access the data via the portal. In addition, Vaultastic servers and server stores are backed up using AWS technology for easy recovery if required.	21 (4) 21.1 (a) III 21.1 (b) 21.1 (c) 9
2.3	Data Security	Data Access	Absence of adequate access controls may lead to unauthorized access & data leakage.	1) Data access process/procedure. 2) Tools/solutions implemented to monitor access. 3) Logging & monitoring access.	Through S3 bucket policies, IAM and ACL at the Infrastructure layer and access control policies at the Vaultastic application layer	Data stored in Amazon S3 is restricted by default; only bucket and object owners have access to the Amazon S3 resources they create (note that a bucket/object owner is the AWS Account owner, not the user who created the bucket/object). There are multiple ways to control access to buckets and objects: 1) Identity and Access Management (IAM) Policies 2) Access Control Lists (ACLs) 3) Bucket Policies You can further restrict access to specific resources based on certain conditions. For example, you can restrict access based on request time (Date Condition), whether the request was sent using SSL (Boolean Conditions), a requester's IP address (IP Address Condition), or based on the requester's client application (String Conditions). To identify these conditions, you use policy keys. For more information about action-specific policy keys available within Amazon S3, refer to the Amazon Simple Storage Service Developer Guide. Amazon S3 also gives developers the option to use query string authentication, which allows them to share Amazon S3 objects through URLs that are valid for a predefined period of time. Query string authentication is useful for giving HTTP or browser access to resources that would normally require authentication. The signature in the query string secures the request.	Vaultastic uses all the AWS controls described here to secure our S3 buckets, which store the email data of all our customers. This means that the S3 buckets of Vaultastic are secured and locked to be accessible only to Vaultastic resources. Further, Vaultastic provides an individual user level self service portal access to the email data, which is secured by authentication (coming soon 2 factor mfa) and authorisation controls such as trusted IPs from which the user can access, which users can access the portal, what all can the user once they sign into the portal, and so on All of these activities are maintained in logs on our site, and stored for 10 years.	21 (4) 21.1 (a) III 21.1 (b)

2.4	Data Security	Data Encryption	Absence of data encryption controls may lead to unauthorized access to data in transit & data at rest.	1) Encryption techniques & type for data in transit & data at rest	AWS cryptographic processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP. Vaultastic deploys encryption at rest and in transit	Data at Rest: AWS offers encryption capability for EBS volumes (block storage) and S3 (object store), customer has choice of using their own encryption keys or AWS managed keys using KMS. Customers can also use alternate approach of file system encryption using third-party tools like bitlocker or dm-crypt. Customers can also use client side encryption where data will be encrypted by customer's application and their own key and encrypted data (cyphertext) will be stored in S3. Data in transit: AWS support HTTPS/TLS for securing data in transit with S3 and elastic load balancer. Customer can use IPSec VPN for connecting their on premise infrastructure to AWS.	Vaultastic encrypts all email data stored on the S3 to lock it for access only by Vaultastic resources. In addition, all transport and access of data to and from Vaultastic happens over TLS. Additionally, you have the option to deploy IPSec VPNs from their environments to AWS for securing securing their access.	21.1 (a) III 21.1 (b) 21.3 (b) 21.3 (c)
2.6	Data Security	Data Classification	Absence of data classification controls may lead to unorganized data difficult to retrieve and segregate	1) Data classification process / procedure.	Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits. Vaultastic indexes all data for instant access using complex search queries	AWS Customers retain control and ownership of their data. Data classification of any data in AWS can be done by the customer using existing organization policies AWS has controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default.	Within Vaultastic, all email data is indexed and classified an mail attributes such as from id, to id, content etc., to allow instant access using ediscovery/search.	21.1 (a) III 21.1 (b) 21.2 (b)
2.7	Data Security	Data Segregation and Isolation	Absence of controls on data segregation and data isolation may lead to data of different organizations getting comingled or leaked in multi-tenancy environment.	1) Role based access controls 2) Multitenant controls implemented.	Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. Vaultastic multi-layered security framework	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers.	Vaultastic's resources are logically isolated from data of other customers on AWS and we use AWS prescribed best practices to encrypt the data and sessions within our control. In addition, our setup is also multi-tenant and a customer's data stored in Vaultastic is logically isolated from the data of other customers using a unique tag, ensuring no mix-up is possible. All this data is visible only via the self service controls, all of which are controlled by role based access.	21.1 (a) III 21.1 (b) 21.2 (b)
2.8	Data Security	Data Sovereignty	Absence of recognition of data sovereignty requirements may lead to legal issues	1) Personal information disclosed during an overseas meeting or conference 2) Publish personal information to the internet either intentionally or unintentionally 3) Send personal information via email or hard copy overseas	https://aws.amazon.com/aispl/agreement/ https://www.vaultastic.com/terms-of-service	AWS Customers retain control and ownership of their data. AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities.	Our Vaultastic customers control all their information, including profile and contact information. Mithi will not share this with any other entity or publish this information in any form unless required to comply with the law or requests of governmental entities.. There are no provisions in any flow to do this. Mithi will not also receive modifications requests via email or call for this information. Our customers are requested to perform the changes themselves using a secure self service portal. https://www.vaultastic.com/terms-of-	21.1 (a) III 21.1 (b)

2.9	Data Security	Secure Disposal	Absence of secure disposal of data controls may lead to unauthorised data recovery.	1) Policies and procedures defined for data disposal 2) Technical measures implemented, for the secure disposal and complete removal of data from all storage media.	As per guidelines described in: DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) https://www.vaultastic.com/terms-of-service	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.	In accordance with our policy of cancellation of accounts, when a customer exits our system, there are automatic systems which will clean out the customers data after the necessary grace period, totally and completely and will not retain any copy or trace whatsoever. We firmly believe that our customer owns the data and that they decide what they want to do with the data. This is also documented in our SLA https://www.vaultastic.com/terms-of-service .	21.1 (a) III 21.1 (b) 21.1 (c) 10 21.3 (e) 21.3 (f)
2.1	Data Security	Availability	Absence of DDOS controls may lead to unavailability of the service.	1) Solutions implemented for monitoring trend in network traffic. 2) Mitigation methods post attack.	AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance. Vaultastic deploys digital eyes, ears, always on DDOS detection and mitigation, and a 24/7 NOC team to ensure availability	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection	In addition to the protection provided by AWS to our resources, Vaultastic has its own in built DDOS protection mechanisms based on IP reputation and IP throttle control to provide a silent, hands free, in line mitigation, thus eliminating human involvement and ensuring an efficient, always on protection All this is monitored using digital eyes and ears, super monitored by a 24/7 NOC centre.	21.1 (a) III 21.1 (b) 21.1 (c) 10 21.3 (e)

3.1	Application Security	Application Security	Absence of security measured while application development may lead the application vulnerable to threats.	1) OWASP guidelines followed for application development. 2) Following risk covered. a. Injection b. Broken Authentication and Session Management c. Cross-Site Scripting (XSS) d. Broken Access Control e. Security Misconfiguration f. Sensitive Data Exposure g. Insufficient Attack Protection h. Cross-Site Request Forgery (CSRF) i. Using Components with Known Vulnerabilities j. Under protected APIs	Using WAF and AWS Config Using a multi layered security approach covering tools such as a. Account lockout b. Strong password policies c. Session cleanout on timeout and logout d. Data Encrypted at rest & in transit e. Granular access and policy controls f. Intelligent DDOS attack prevention g. Up-to-date component library h. Using AWS API gateway to secure interfaces i. Hardened servers, and web components	AWS provides multiple services to help the team implement various aspects. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of web security rules. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.	The Vaultastic App is built on the OWASP guidelines to make it a modern secure web and mobile application The Vaultastic application is secured at multiple layers right from the core data layer to the periphery using cyber security best practices to create an impregnable web application, which is based on principle of lock down all and allow only as required. All resources on Vaultastic are hardened and hosted on AWS and leverage the strong security capability of the IaaS layer of the cloud platform to set a secure foundation. The core data is encrypted at rest and in transit and is accessible only via special keys embedded in the application and only through the interface. The self service portals are secured by tight authentication and authorisation layers based on the roles of the user. The access to these portals is over SSL can be locked to trusted IPs or blocked altogether to reduce chances of attacks. These web sessions are cleaned up with no data trace in the browser post timeout or logout. The apps are protected by strong password policies covering history, age, complexity, etc. and also an account lockout mechanism to block out password harvest attacks. Vaultastic leverages more than 25 AWS services which are secure by design to add to the security of the solution. Vaultastic is regularly scanned for vulnerabilities by our team and by our customers, and vulnerabilities are fixed immediately to ensure continued up-to-date security	21.1 (a) III 21.1 (b) 21.1 (c) 10 21.3 (e)
3.2	Application Security	VA/PT	Absence of VA/PT may lead to exploitation of vulnerabilities resulting in critical data loss.	1) VA/PT reports. 2) Identified vulnerabilities fixed report/evidence.	http://aws.amazon.com/security/vulnerability-reporting/	Regular vulnerability scans are performed on the host operating system, web application, and databases in the AWS environment using a variety of tools. Also, AWS Security teams subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at: http://aws.amazon.com/security/vulnerability-reporting/ You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy.	Regular vulnerability scans are performed on the Vaultastic resources, their operating system, and applications across all the open ports using a variety of tools. Our team also proactively receive feeds from our component vendors on latest security updates to allow us to proactively apply these on the resources We encourage our customers to report vulnerabilities discovered using their own scans and tools as required to meet your specific compliance requirements.	21.1 (a) III 21.1 (b) 21.1 (c) 10 21.3 (e)

4.1	Compliance & Audit	Right to Audit	Absence of Audit may lead to unidentification of critical issues.	1) Right to audit clause in SLA. 2) Regulator to independently audit.	AWS SOC 1 Type 2 report provides further details. AWS has been validated Vaultastic records every micro activity and stores these logs for the long term.	The customers are free to audit their infrastructure through the access to the AWS Console. Due to the fact that our data centres host multiple customers, AWS does not allow data centre tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our SOC 1 Type II report. This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. Independent reviews of data centre physical security is also a part of the ISO 27001 audit, the PCI assessment, ITAR audit, and the FedRAMP testing programs. (Note - this is available through Artefacts section via your AWS console)	Vaultastic stores audit logs of all user and admin activity for a period of 10 years and we are open to sharing the customer's audit logs with the customer as required for their audits. The customer can then independently audit this information for their compliance or investigative purposes.	21.1 (a) III 21.1 (b) 21.1 (c) 10 21.3 (e)
4.2	Compliance & Audit	Internal Audit	Absence of Audit may lead to unidentification of critical issues.	1) Internal audit conducted. 2) Audit reports. 3) Action taken on audit observations.	Internal and External audits done regularly with an effective response team ensures proactive monitoring and prevention of critical issues	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC reports provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	Our resources and configurations are proactively audited by our internal security teams to ensure compliance to SLAs and data safety/security guidelines. Any deviation or recommendation is corrected immediately to prevent any flare up of critical issues.	

4.3	Compliance & Audit	Certifications	Absence of certification may lead to lower competency, less commitment to clients, less awareness about the domain.	1) Certification and scope coverage.	https://aws.amazon.com/compliance/	ISO 9001 ISO 27001 ISO 27017 ISO 27018 MLPS Level 3 MTCS PCI DSS Level 1 SEC Rule 17-a-4(f) SOC 1 SOC 2 SOC 3	Mithi's solutions are compliant with General Data Protection Regulation (GDPR), the new EU legislation (coming into effect on 25th May 2018) and also support HIPAA compliance for the healthcare industry. While our platforms are not officially certified for security, Mithi has taken these measures to ensure security on all the layers Vaultastic. https://www.vaultastic.com/blog/2016/11/10/why-vaultastic-the-most-secure-e A testimony to our fine attention to security at the App layer is the fact that Fortune companies like Alembic Pharma, IPCA, Aditya Birla, Mahindra and Mahindra, DRDO (govt defence), BFSI customers like SBI Life Insurance, Cosmos Bank, Capital Small Finance Bank and from the ITES/BPO segment, EXL, iProcess and many more such high risk high target companies use our cloud or deploy our software in Internet-facing zones, with full confidence and securely. In addition, most of these companies, as a practice, run VAPT (Vulnerability Assessments and Penetration tests) periodically to confirm that the servers and service is fully secure at all layers. We are proud to highlight that so far in over a decade of deploying our solutions on hundreds of servers, not a single instance of intrusion has been reported. P.S. At the point of writing this article, Mithi is in the process of acquiring an ISO 27001 certificate.	
4.4	Compliance & Audit	Software compliance	Absence of software compliance controls may lead to unidentification of unauthorized software.	1.Identification of Software Assets. 2.Verifying the Software Assets including licenses, usage, and rights. 3.Identifying gaps that may exist between what exists on the installations, and the licenses possessed, and the rights of usage. 4.Taking action to close any gaps. 5. Software compliance procedure.		Responsibility of Solution provider (ISV) for software hosted on AWS	NA since Vaultastic is offered as a SaaS and we take care of the software installed on our servers.	

4.5	Compliance & Audit	Compliance Reporting	Absence of compliance reporting may lead to unnoticed non-compliance points	1) Reporting of non-compliance. 2) Remediation actions done.	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC reports provides details on the specific control activities executed by AWS.	Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of the AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution	Based on the shared security model of AWS, Vaultastic builds on the AWS compliance enablers to add compliance for the application layer. The compliance in Vaultastic is documented and implemented at multiple layers and the whole stack is auditable via access to the audit logs. Our internal audit teams regularly ensure compliance of the service to SLA, and prescribed security standards There is a 24/7 team at Mithi to tackle incidents at various severity layers, and close them to ensure business continuity and data safety.	
5.1	BCP DR	BCP DR documentation	The continuity of process & access to systems will be affected if business continuity plan is not defined & tested	1) BCP& DR process/procedure/planning documents.	https://aws.amazon.com/disaster-recovery/. Vaultastic Data Safety & Disaster Recovery– Architecture V3.pdf	AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. It is the customer's responsibility to leverage these capabilities to build highly available application architectures.	Vaultastic, leverages the multiple AZs (data centre) in the AWS region to achieve full DR capability, driving towards an RPO of zero and RTO of on hour. The elastic cloud storage is designed for extreme data durability, upward of 11 9s (99.999999999%) and it instantly replicates each piece of data written from the first Availability zone (AZ1) to the second availability zone (AZ2). This means that the data is automatically backed up in two regions, instantly. In case of an outage on AZ1, all of the data can be FULLY recovered from AZ2. Besides the technology which ensures extreme email data durability as explained above, Vaultastic uses the EBS snapshot replication system to replicate the complete compute infrastructure stack to the other AZ, and maintain an on-going sync. This simply means that all the resource elements in AZ1 are replicated to AZ2 on a continuous basis creating a mirror image of the entire Vaultastic setup on AZ1 to AZ2. In case of a disaster on AZ1, the full services, with all the archived email data can be spun up from AZ2 in the matter of 1 hour. These are done by rebuilding all the machines and disks using the snap shot backups taken in the AZ1 daily and replicated to AZ2 instantly. Post recovery, the end users continue to use the service transparently. Full details of Vaultastic BCP DR attached: Vaultastic Data Safety & Disaster Recovery– Architecture V3.pdf	

5.2	BCP DR	DR Testing	The continuity of process & access to systems will be affected if business continuity plan is not defined & tested	1) DR sites location. 2) BCP DR performed results.	AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11 provides additional details. AWS has been validated	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity. Details of every aspect of BCP covered in the Risk and Compliance document section BCR-01.1 to BCR-11.5	The BCP DR plan of Vaultastic is put through a DR Drill periodically as defined by our procedures, which ensures that the process is behaving as expected.	
6.1	SLA/Vendor Management/ Legal	SLA/Vendor Management	In absence of clear and adequate vendor level agreement on adherence to regulations may lead to dispute	SLA covering following points: a. Sustainability, support for fail safe operations b. Data Retrieval time, protection of IPR, etc. c. Security control measures to prevent, detect and react to breaches including data leakage and demonstration of the same. d. Ensure confidentiality, integrity, availability and privacy of the data collected, processed, stored and disposed. e. Reporting of network performance, application uptime, application response time. f. Escalation & penalty matrix.	https://www.vaultastic.com/terms-of-service	Points covered under Customer Agreement	All these points and more are part of the SLA we get into with all our customers. https://www.vaultastic.com/terms-of-service	21.1 (a) I 21.1 (a) ii 21.1 (c) i
6.2	SLA/Vendor Management/ Legal	Adherence to agreement	In absence of clear and adequate vendor level agreement on adherence to clauses may lead to dispute	Vendor adherence to following clauses: a. Service Level Agreement b. Data Security c. Location of Data d. Ownership of Data e. Confidentiality f. Access to Data for Purposes of Discovery, g. Emergency Security Issues h. Disclaimer of Warranty i. Guarantees and metric j. Service Activation k. Governing Law and Jurisdiction - Mumbai l. Right to Audit.	https://www.vaultastic.com/terms-of-service	Points covered under AISPL Customer Agreement	All these points and more are part of the SLA we get into with all our customers. https://www.vaultastic.com/terms-of-service	21.1 (c) i

7.1	User access management	User access documentation	Absence of controls on user access may lead to unauthorized access & data leakage	1) User Access Management process/procedure document.	Through AWS IAM Service and Vaultastic's role based administration framework	AWS Identity and Access Management (AWS IAM) AWS IAM allows you to create multiple users and manage the permissions for each of these users within your AWS Account. A user is an identity (within an AWS Account) with unique security credentials that can be used to access AWS Services. AWS IAM eliminates the need to share passwords or keys, and makes it easy to enable or disable a user's access as appropriate. AWS IAM enables you to implement security best practices, such as least privilege, by granting unique credentials to every user within your AWS Account and only granting permission to access the AWS services and resources required for the users to perform their jobs. AWS IAM is secure by default; new users have no access to AWS until permissions are explicitly granted. AWS IAM enables you to minimize the use of your AWS Account credentials. Once you create AWS IAM user accounts, all interactions with AWS Services and resources should occur with AWS IAM user security credentials. More information aboutAWS IAM is available on the AWS website. An IAM role uses temporary security credentials to allow you to delegate access to users or services that normally don't have access to your AWS resources. A role is a set of permissions to access specific AWS resources, but these permissions are not tied to a specific IAM user or group. An authorized entity (e.g., mobile user, EC2 instance) assumes a role and receives temporary security credentials for authenticating to the resources defined in the role. Temporary security credentials provide enhanced security due to their short life-span (the default expiration is 12 hours) and the fact that they cannot be reused after they expire.	Vaultastic supports different types of users 1. Our own DevOps and NOC engineers, who have limited access to the resources to allow them to only maintain the resources, upgrade them, patch them and respond to alerts. This access is managed using the IAM framework of the AWS cloud. This layer of people have no access to the data or customer/user configurations. 2. Our support helpdesk, who have access only to the master admin portal, allowing them to view and manage the global policies, controls applicable to select or all customers. Again this layer of people have no access to the customer data 3. Customer admins and users who are limited to access only the data which belongs to their organisation, only via secure tamper proof consoles 4. Further within the customer's users, role based controls to provide only limited and relevant access to the data.	21.1 (c) 3 21.2 (c)
7.2	User access management	User Creation/deletion	Absence of controls on user access may lead to unauthorized access & data leakage	1) Tools/process implemented for user access management. 2) Audit trails/monitoring/review user access.	Through AWS IAM Service and Vaultastic's role based administration framework	https://aws.amazon.com/iam/details/manage-permissions/ Permissions let you specify access to AWS resources. Permissions are granted to IAM entities (users, groups, and roles) and by default these entities start with no permissions. In other words, IAM entities can do nothing in AWS until you grant them your desired permissions. To give entities permissions, you can attach a policy that specifies the type of access, the actions that can be performed, and the resources on which the actions can be performed. In addition, you can specify any conditions that must be set for access to be allowed or denied.	Vaultastic provides an administration console to your super admin, who can define roles with rights and assign them to specific users. This encodes your security and access policy right into the system At another level, every activity done on the system by any user is recorded in an audit log and is stored for the long term (10 years), which can be used to review user activity on the platform	21.1 (c) 3 21.2 (b)

7.3	User access management	UserID management	Absence of controls on user access may lead to unauthorized access & data leakage	1) Privilege user ID management. 2) Password Compliance: a. Complexity b. Length c. History, etc. 3) Segregation of duties.	Infra protected using IAM of AWS App and data protected by authorisation roles, password policies for authentication, account lockout, MFA (coming soon)	AWS provides the mechanisms to configure password policies as per company security policies. In addition, AWS provides following tools for user controls and access management **Passwords** AWS root account or IAM user account login to the AWS Management Console A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters. **Multi-Factor Authentication (MFA)** AWS root account or IAM user account login to the AWS Management Console A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account. **Access Keys** Digitally signed requests to AWS APIs (using the AWS SDK, CLI, or REST/Query APIs) Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS. **Key Pairs** SSH login to EC2 instances CloudFront signed URLs Windows instances To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP. **X.509 Certificates** Digitally signed SOAP requests to AWS APIs SSL server certificates for HTTPS X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3) You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Credential Report	Vaultastic provides an administration console to your super admin, who can define roles with rights and assign them to specific users. This encodes your security and access policy right into the system These rights include ediscovery rights too, which define which users can access whose email information. At another level, every activity done on the system by any user is recorded in an audit log and is stored for the long term (10 years), which can be used to review user activity on the platform The admin of Vaultastic can define password policies to strengthen authentication, which include min password length, password history period, password complexity rules & password age. This whole system is backed by an account lockout mechanism to block password harvest attempts. Vaultastic will soon sport a multi factor authentication for all sign ins to further secure the application access to only authorised people.	21.1 (c) 3 21.2 (b)
8.1	Change Management	Change management documentation	Absence of controls on change to application may lead to application downtime & deviation from business requirements.	1) Change Management process/procedure document. 2) Release manager for change.	Change Management and controls for AWS infra documented in Risk & Compliance Document Section CCC-01.1 to CCC-05.01 Vaultastic change management is controlled using a 3 step release and is internally documented	On the AWS Side, the change management policies and procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements.	All Updates and upgrades to the Vaultastic platform follow a well documented 3 step DevOps process. This process has been refined over a decade and allows us to manage patching, updating and upgrading live setups, which are mission critical and managing data volumes in 100's of tera bytes, with near zero downtime or blips in the service via a very controlled process.	

8.2	Change Management	Change implementation	Absence of controls on change to application may lead to application downtime & deviation from business requirements.	1) Tools/process implemented for change implementation. 2) Authorization/approval matrix. 3) Testing/UAT of changes.	Change Management and controls documented in Risk & Compliance Document Section CCC-01.1 to CCC-05.01	On the AWS Side, the change management policies and procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements.	Before an update/upgrade is ready for release, it undergoes a rigorous automated and manual testing to confirm working and impact. This happens on an on-going basis every night as the development progresses. Change management follows a rigorous review and approval process with detailed analysis of change impact and "what if" scenarios. The CMR goes through 3 levels of review and documented approvals and must include a roll back step. After all the automated tests, validations and approvals, each update, upgrade, however minor or major, goes through the following stages: **Step 1:** Release for internal consumption on staging servers for a controlled UAT. This is used by our internal teams and partners in a live working environment. **Step 2:** Release to a small subset of select beta stage customers under a controlled environment for a live UAT **Step 3:** Release to all customers There are detailed process documents covering the entire roll out cycle, including intimation to customers, garnering feedback, etc.	
9.1	Incident Management	Incident management documentation	Absence of controls on incident may lead to issue/event unnoticed	1) Incident Management process/procedure document.	Digital Eyes, Ears to monitor resources and critical app parameters, coupled with a 24x7x365 NOC and a 24x7x365 helpdesk	**Incident Response:** The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and response	Vaultastic deploys multiple layers of digital eyes and ears to monitor app and service performance. These are fed via a live stream to a 24/7 NOC team to drive proactive resolution at all times. A 24/7 helpdesk interfaces with the customers to receive incident reports, and manage the response and impact.	

9.2	Incident Management	Incident resolution	Absence of controls on incident may lead to issue/event unnoticed	1) Tools/process implemented for handling incidents. 2) Incident reporting.	Digital Eyes, Ears to monitor resources and critical app parameters, coupled with a 24x7x365 NOC and a 24x7x365 helpdesk	**Incident Response:** The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and response	Vaultastic deploys multiple layers of digital eyes and ears to monitor app and service performance. These are fed via a live stream to a 24/7 NOC team to drive proactive resolution at all times. A 24/7 helpdesk interfaces with the customers to receive incident reports, and manage the response and impact. Our helpdesk console allows our customers to generate a consolidated report of all incidents they have reported. An RCA team periodically reviews all incidents and identifies kaizen, and upgrades to drive permanent resolutions and move the platform to the next level.	
10.1	Network Security	Network Segmentation	Absence of controls on network segmentation may lead to compromise of performance and network security	1) Network segment implemented.	Through AWS VPC & VPN on demand	Amazon VPC can enable an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses in the range of your choice (e.g., 10.0.0.0/16). You can define subnets within your VPC, grouping similar kinds of instances based on IP address range, and then set up routing and security to control the flow of traffic in and out of the instances and subnets. AWS offers a variety of VPC architecture templates with configurations that provide varying levels of public access: 1. VPC with a single public subnet only 2. VPC with public and private subnets 3. VPC with public and private subnets and hardware VPN access 4. VPC with private subnet only and hardware VPN access Security features within Amazon VPC include security groups (instance level firewalls), network ACLs, routing tables, and external gateways. Each of these items is complementary to providing a secure, isolated network that can be extended through selective enabling of direct Internet access or private connectivity to another network. Amazon EC2 instances running within an Amazon VPC inherit all of the benefits described below related to the guest OS and protection against packet sniffing.	The Vaultastic application deployment on AWS fully leverages the VPC technology of AWS to isolate and secure the resources from prying eyes. In addition, customers can choose to have a VPN tunnel setup from their environment to the AWS VPC of Vaultastic, secured to their coordinates.	21.2 (a)

10.2	Network Security	Patching network devices	Absence of controls on network devices patching may lead risk to network security	1) Patch management process. 2) Patch testing/Implementation.	In accordance with ISO 27001, NIST and PCI requirements	AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems. AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers.	Patching the Vaultastic application and underlying components involves a rigorous validation and multilevel review to begin the process. The patches are deployed in 3 steps to cover all customers on the shared multi tenant setup. **Step 1:** Release the patch for internal consumption on staging servers for a controlled UAT. This is used by our internal teams and partners in a live working environment. **Step 2:** Release to a small subset of select beta stage customers under a controlled environment for a live UAT **Step 3:** Release to all customers There are detailed process documents covering the entire roll out cycle of patches, including intimation to customers, garnering feedback, etc.	21.1 (c) 6

10.3	Network Security	Network Security	Absence of network security controls would lead to network breaches which may not be detected	Network security controls: a. Access and authentication, b. Intrusion detection/prevention, c. Firewall, d. Traffic monitoring, e. Audit logging, f. Protection from vulnerabilities/malware g. Antivirus h. System Hardening	Details of network security at Infra layer available in the AWS Security Whitepaper From Vaultastic perspective, system is secured at multiple layers https://www.vaultastic.com/blog/2016/11/10/why-vaultastic-the-most-secure-enterprise-email-vault	The AWS network has been architected to permit you to select the level of security and resiliency appropriate for your workload. To enable you to build geographically dispersed, fault-tolerant web architectures with cloud resources, AWS has implemented a world-class network infrastructure that is carefully monitored and managed **Secure Network Architecture** Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. **Secure Access Points** AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows you to establish a secure communication session with your storage or compute instances within AWS. To support customers with FIPS cryptographic requirements, the SSL-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant. **Transmission Protection** You can connect to an AWS access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. AWS CloudTrail provides a log of requests for AWS resources within your account for supported services. For each event, you can see what service was accessed, what action was performed, and who made the request. CloudTrail captures information about every API call to every supported AWS resource, including sign-in events. AWS Marketplace provides multiple choices of AntiVirus and IPS/IDS software. Customer may choose the appropriate solution for their objectives.	Vaultastic has the following controls at each control layer **a. Access and authentication:** Two factor authentication and access rights decide who can get in and with what privileges **b. Intrusion detection/prevention:** Besides the Infra protection provided by AWS, Vaultastic has security at multiple layers to block such attempts - account lockout to block harvest attacks, IP throttling to frustrate brute force attempts, password policies to reduce human errors with password leakages, strict access control policies to allow access to trusted networks only, etc. **c. Firewall:** built into the application, besides the one provided by AWS for the infra. So firewalls are in multiple layers. **d. Traffic monitoring:** Vaultastic deploys digital eyes and ears backed by a 24x7x365 NOC to monitor the entire system proactively and keep a tab on usage, traffic, impending problems and more. **e. Audit logging:** Vaultastic logs every possible event on the platform including but not limited to user access, property changes, mail exports etc. All logs are maintained for 10 years to facilitate audit inspections/investigations. **f. Protection from vulnerabilities/malware:** None of the mails are activated on the platform backend preventing any carried malware from being activated. All indexing action on email is sandboxed to prevent activating any code. **g. Antivirus:** The mails are ingested from the primary mail platform after they are cleaned for viruses & malware so only clean mail are archived. **h. System Hardening:** By using best practices for securing the OS in the enterprise vault services, the servers are hardened during deployment, to reduce risks that arise from having a larger surface of vulnerability i.e. a server doing more than it is supposed to do.	

10.4	Network Security	Monitoring	Absence of adequate network monitoring controls on the traffic between trusted and untrusted connections may be exploited	1) Security information and event management (SIEM) solution implemented. 2) Network/IPS/firewall/antivirus logs.	Details of network security available in the AWS Security Whitepaper From Vaultastic perspective, system is secured at multiple layers https: //www.vaultastic. com/blog/2016/11/10/why-vaultastic-the-most-secure-enterprise-email-vault	AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity. AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.	Vaultastic builds on the network security and in addition deploys firewalls, wafs, other tools, and multiple digital eyes and ears to automatically monitor the application and service performance, traffic, unusual patterns and attacks to provide a high level of performance & availability. The tools deployed on Vaultastic monitor traffic patterns, detect and throttle ddos attacks, lockout brute force attacks, application break-in attempts, and also control use of the application/services outside the limits. The tools are configurable for threholds and these are fine tuned regularly by our NOC team. When any anomaly is detected in the patterns, Mithi NOC team is alerted to initiate a response. The logs of all these tools are maintained for an extended period to allow post mortem analysis.	
10.5	Network Security	VA/PT	Absence of VA/PT may lead to exploitation of vulnerabilities in network resulting in critical data loss.	1) VA/PT reports. 2) Identified vulnerabilities fixed report/evidence.	http://aws.amazon. com/security/vulnerability-reporting/ . Proactive VAPT scans internally and by our customers with verification by external agencies keeps our application secure.	Regular vulnerability scans are performed on the host operating system, web application, and databases in the AWS environment using a variety of tools. Also, AWS Security teams subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at: http://aws.amazon. com/security/vulnerability-reporting/ You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy.	We are committed to ensuring security of your data stored on our platform. To ensure that we have the following systems in place. As part of our maintenance and new release/patch/update processes, our teams scan the application and services for vulnerabilities regularly using a variety of tools. In addition we proactively watch for security fixes and patches in the underlying components used in the platform. Several of our customers proactively scan our solution using third party tools for their internal compliance reporting. All these VAPT test feeds are fed to our security response team, which releases updates in priority relating to the severity and impact of the reported vulnerabilities. VAPT fix reports are shared with customers who have reported vulnerabilities and security fixes are announced to customers via suitable notification channels.	21.1 (c) 8

10.6	Network Security	Audit Logging & protection of logs	Absence of audit logging & logs protection may lead to undetection of unauthorized activities & transactions.	1) Audit logging enabled. 2) Audit log retention & prevention.	https://aws.amazon.com/cloudtrail/ Mithi policy to log every micro activity and retain all logs for 10 years	For after-the-fact investigations and near-real-time intrusion detection, AWS CloudTrail provides a log of requests for AWS resources within your account for supported services. For each event, you can see what service was accessed, what action was performed, and who made the request. CloudTrail captures information about every API call to every supported AWS resource, including sign-in events. Once you have enabled CloudTrail, event logs are delivered every 5 minutes. You can configure CloudTrail so that it aggregates log files from multiple regions into a single Amazon S3 bucket. From there, you can then upload them to your favourite log management and analysis solutions to perform security analysis and detect user behaviour patterns. By default, log files are stored securely in Amazon S3, but you can also archive them to Amazon Glacier to help meet audit and compliance requirements.	Vaultastic uses AWS CloudTrail to track activities and requests to the underlying infrastructure layer by our teams and to detect unauthorised access or attempts. In addition, at the application and service layer all activity by users and mail flow is recorded in logs, rotated daily and stored for a period of 10 years in a safe S3 bucket on the cloud. The activities recorded include but are not limited to sign in attempts, profile changes by users, mail download activities, mail search activities and more. To support your after the fact investigations, Mithi can share relevant portions of these logs with you on request.	21.1 (c) 4
11.1	Asset management	Asset management	Absence of asset management controls may lead to over or under maintenance of asset.	1) Complete inventory of business-critical assets. 2) Assigned ownership supported by defined roles and responsibilities, including those assets used, owned, or managed by customers (tenants).	As per ISO 27001 standard, Annex A, domain 7 Vaultastic uses a proprietary tool to track assets across tenants	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standard, Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	Vaultastic is a multi-tenant environment with logical partitioning of information for each customer. A customer unique identifier is used to tag each asset piece/partition belonging to a customer. This system manages the ownership of assets/data and also the access rights based on roles.	
	Selection of Hosting	Criticality	The selection of cloud hosting model shall depend on the criticality of the information being hosted			Criticality to be defined by customer	Criticality to be defined by customer	21 (2)