



SOC 1 TYPE 1 REPORT

Enerpact LLC

13007 Peach Meadow Dr, Cypress TX 77429 US

DEC 31, 2021



This report is intended solely for use by the management of ENERPACT, user entities of ENERPACT's services, and other parties who have sufficient knowledge and understanding of ENERPACT's services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Bala & Co Chartered Accountants as a result of such access. Further, the auditor(s) does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT.....	3
SECTION 2: MANAGEMENT'S ASSERTIONS	7
SECTION 3: ENERPACT'S DESCRIPTION OF CONTROLS.....	11
SECTION 4: INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF CONTROLS.....	29

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To
ENERPACT LLC

Scope

We have examined ENERPACT LLC's (ENERPACT) information technology general control system for their "**Electronic Invoicing and Procure to Pay solution for E&P companies**" as on Dec 31, 2021 (the description), and the suitability of the design of controls to achieve the related control objectives stated in the description.

Enerpact Solutions Pvt. Ltd., a wholly owned subsidiary of Enerpact LLC, is an independent subservice organization providing IT Solutions and Technology Support Services to Enerpact LLC. The description includes those elements of the IT Solutions and Technology Support Services provided to Enerpact LLC and the controls designed by Enerpact LLC and operated by Enerpact Solutions Pvt. Ltd. that are necessary for Enerpact LLC to achieve its service commitments and system requirements based on the applicable trust services criteria.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at ENERPACT, to achieve ENERPACT's service commitments and system requirements based on the applicable trust services criteria. The description presents ENERPACT's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ENERPACT's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

As indicated in the description, Enerpact uses AZURE for data center services. The description in Section 3 includes only the controls of Enerpact and excludes controls of the various subservice organizations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Enerpact, to achieve Enerpact's service commitments and system requirements based on the applicable trust services criteria. The description presented by Enerpact also indicates that certain trust services criteria and the types of complementary subservice organization controls can be met only if the subservice organization's controls, contemplated in the design of Enerpact's controls, are suitably designed and operating effectively along with related controls at the service organization. The description does not disclose the actual controls at the subservice organization. Our examination did not extend to controls of various subservice organizations for data center services and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

ENERPACT has provided the accompanying assertion titled "Management Assertion of Enerpact." as on Dec 31, 2021 about the fairness of the presentation of the description and suitability of the design of controls to achieve the related control objectives stated in the description. ENERPACT is responsible for (1) preparing the description and the Assertion; (2) providing the services covered by the description; (3) specifying the control objectives and stating them in the description; (4) identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and (5) designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Subservice Organization's Responsibilities

Enerpact Solutions Pvt. Ltd. has provided the accompanying assertion titled "Assertion of Enerpact Solutions Pvt. Ltd." (assertion) about the description and the controls stated therein. Enerpact Solutions Pvt. Ltd. is responsible for preparing the portion of the description related to the IT Solutions and Technology Support Services to ENERPACT LLC and Enerpact Solutions Pvt. Ltd.'s assertions, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; and implementing, operating, and documenting controls designed by ENERPACT LLC, which

enable ENERPACT LLC to achieve its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and suitability of the design of controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3000, Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls were suitably designed to achieve the related control objectives stated in the description, as on Dec 31, 2021.

An examination of the description of the service organization's system and the suitability of design of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to achieve the related control objectives stated in the description. An examination of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon.

We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 of this report.

Opinion

In our opinion, in all material respects:

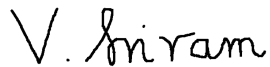
- a. the description presents ENERPACT's "**Electronic Invoicing and Procure to Pay solution for E&P companies**" that was designed and implemented as on Dec 31, 2021, in accordance with the description criteria;
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if user entities applied the complementary user entity controls contemplated in the design of ENERPACT controls as on Dec 31, 2021.

BALA & Co.,
Chartered Accountants

Restricted Use

This report, and the description of tests of controls and results thereof are intended solely for the information and use of Enerpact, User entities of Enerpact, as on Dec 31, 2021 and prospective user entities; independent auditors and practitioners providing services to such user entities, and regulators who have a sufficient knowledge and understanding to consider it, along with other information including information about the controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Sriram Visvanathan,
Partner, M/s Bala & Co CAs
FRN: 000318S
FCA, Certified Public Accountant
CPA M No. 25816
Dated: 20th Jan 2022

SECTION 2: MANAGEMENT'S ASSERTIONS

Assertion of Enerpact LLC



MANGEMENT ASSERTION OF ENERPACT LLC

We have prepared the accompanying Description of ENERPACT's experienced "Electronic Invoicing and Procure to Pay solutions for E&P companies" as on December 31, 2021. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of ENERPACT's controls are suitably designed, along with related controls. The description does not extend to controls implemented in the user entities.

Enerpact LLC uses a subservice organization, namely Enerpact Solutions Pvt Ltd to provide IT Solutions and Technology Support Services. Enerpact LLC's description includes a description of Enerpact Solutions Pvt Ltd's IT Solutions and Technology Support Services used by Enerpact LLC to process transactions for user entities and business partners, including the controls of Enerpact LLC and the controls designed by Enerpact LLC and operated by Enerpact Solutions Pvt Ltd that are necessary for Enerpact LLC to achieve Enerpact LLC's service commitments and system requirements based on the applicable trust services criteria. Enerpact Solutions Pvt Ltd's assertion is also presented in section II.

ENERPACT uses Azure Services ('Azure' or 'subservice organization') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ENERPACT, to achieve ENERPACT's service commitments and system requirements based on the applicable trust services criteria. The description presents ENERPACT's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ENERPACT's controls. The description does not disclose the actual controls at the subservice organization.

We confirm, to the best of our knowledge and belief, that:

- a. The Description fairly presents ENERPACT's experienced "Electronic Invoicing and Procure to Pay solutions for E&P companies" as on December 31, 2021. The Description includes control objectives and related controls. The criteria used in making this assertion were that the description:
 - (i) Presents how the system made available to User entities was designed and implemented, including:
 - The types of services provided, including, as appropriate, the classes of transactions processed.
 - The procedures, within both automated and manual systems, by which services are provided, including as appropriate, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to User entities.
 - The related records, supporting information, that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for User entities.



- How the system captures significant events and conditions, other than transactions.
 - The process used to prepare reports or other information for User entities.
 - The specified control objectives and controls designed to achieve those objectives.
 - Controls, including as applicable, complementary User entities' controls contemplated in the design of service organizations' controls.
 - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of User entities.
- (ii) Does not omit or distort information relevant to the scope of the system, while acknowledging that the Description is presented to meet the common needs of broad range of User entities of the system and their independent auditors and may not, therefore include every aspect of the system that each individual User entity of the system and its auditor may consider important in its own particular environment.
- (iii) The Description includes relevant details of changes to the system as on December 31, 2021.
- (b) Our controls related to the control objectives stated in the Description, were suitably designed as on December 31, 2021, to achieve those control objectives. The criteria we used in making this assertion were that:
- (i) the risks that threaten the achievement of the control objectives stated in the Description have been identified by the Management;
 - (ii) the controls identified in the Description would, if operating as described, and if User entities applied the complementary User entities' controls contemplated in the design of ENERPACT's controls as on December 31, 2021, provide reasonable assurance that those risks would not prevent the control objectives stated in the description being achieved.

A handwritten signature in black ink, appearing to read "Pradeep Deshpande".

Pradeep Deshpande
CEO, ENERPACT

Date: December 31st 2021

Assertion of Enerpact Solutions Private Limited



Assertion of Enerpact Solutions Pvt Ltd

Enerpact Solutions Pvt Ltd provides IT Solutions and Technology Support Services to Enerpact LLC. The services provided by Enerpact Solutions Pvt Ltd are part of Enerpact LLC's IT Solutions and Technology Support Services. We have prepared the portion of the accompanying description of Enerpact LLC's services titled "Description of Enerpact LLC's IT Solutions and Technology Support Services", as on 31st December 2021, (description) disclosing Enerpact Solutions Pvt Ltd's IT Solutions and Technology Support Services provided to Enerpact LLC based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 1[≠] Report (AICPA, Description Criteria)*, (description criteria).

The description is intended to provide report users with information about Enerpact LLC's IT Solutions and Technology Support Services that may be useful when assessing the risks arising from interactions with Enerpact LLC's system, particularly information about system controls that Enerpact LLC has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to **security, availability, and confidentiality (applicable trust services criteria)** set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

We confirm, to the best of our knowledge and belief, that

- a. the description presents Enerpact Solutions Pvt Ltd's IT Solutions and Technology Support Services made available to Enerpact LLC as on 31st December 2021, in accordance with the description criteria.
- b. Enerpact Solutions Pvt Ltd's controls stated in the description, which were designed by Enerpact LLC, operated as described as on 31st December 2021, based on the applicable trust services criteria.

For Enerpact Solutions Pvt Ltd

A handwritten signature in blue ink, appearing to be "Rajesh", is written over a faint, illegible stamp.

Authorized Signatory

Date: 31[≠] December 2021

Enerpact APX Invoice Disposition Overview

SECTION 3: ENERPACT'S DESCRIPTION OF CONTROLS

Purpose of the Report

a. Scope and Purpose of the Report

This report is designed to provide sufficient information for the customers of Enerpact LLC (“ENERPACT”), and its user entities and other related authorities in order for them to obtain an understanding of ENERPACT controls and to enable the customers to use the report as audit evidence that controls at ENERPACT are designed effectively.

b. Company Overview and Background

Enerpact APX is the complete Electronic Invoicing and Procure to Pay solution for E&P companies of all sizes. APX provides superior AP workflow, operator & supplier portals, supplier invoice submission w/AI parsing and data verification, along with full purchase order functionality, and much more. It is the best-valued alternative to OpenInvoice, with no long-term commitments or contracts necessary.

Enerpact provides real-time data access, helping E&P companies free their data trapped in specialty applications for accounting, land, and reservoir management. Data access and operational efficiency are central to success for E&P companies. We support operators with 250+ reports and productivity tools, including LOS statements, Budgeting Reviews, AFE Management, Capital Planning & Scheduling, etc.

c. Overview of Products and Service

Enerpact APX is the only complete Electronic Invoicing and Procure to Pay solution for E&P companies of all sizes.

APX e-Invoicing - APX is a complete Procurement to Pay system designed specifically for Upstream suppliers and operators. APX offers complete e-Invoicing functionality, providing unparalleled software, support, and unrivaled value for its price-point. It’s unique features and user-friendly design, including rock-solid integration with all E&P systems will allow you complete control of your payment schedules.

APX is a fully-functional invoice management system designed explicitly for oil and gas companies. It is rooted in Enerpact’s dual core expertise: Having a complete understanding of E&P data integration combined with highly configurable workflow. Our workflow will adapt to the best practices and needs of your organization and integrates into your accounting system - at no additional cost.

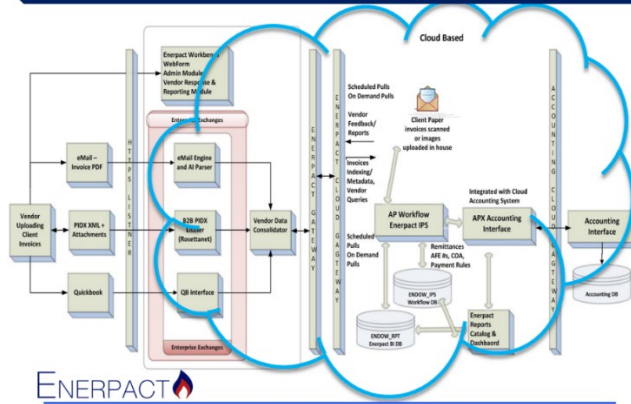
d. Infrastructure and Architectural Diagram

The scope of the examination included ENERPACT’s information technology general control system of their infrastructure built around its APX Application.

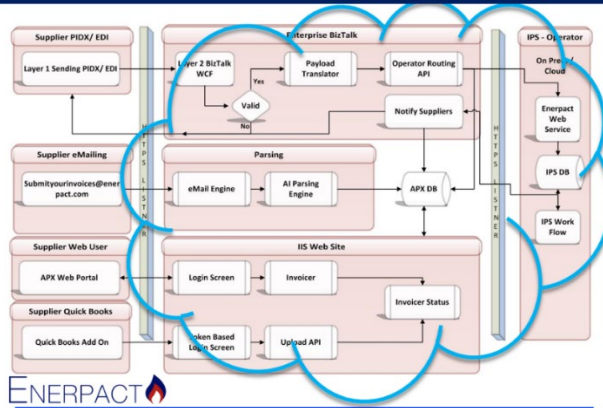
Enerpact APX is a SaaS application hosted in Microsoft Azure Cloud. It is primarily used for processing invoices of Oil & Gas companies. Input entirely comes from the client accounting system. Invoices are routed and approved by workflow defined by operators. Once approved, invoices are made available in upload files consistent with formats that are designed to be imported into operator accounting systems. Operator’s also have the ability to import invoices manually. Automation of invoice routing, approval and upload files are the productivity tools Enerpact offers. All accounting systems have additional checks within the accounting system to ensure only invoices consistent with internal rules are accepted and an additional check of manual effort of releasing posted invoices for payments from within the accounting system. Enerpact tools by themselves are not equipped to issue payments without checks by accountants. Exactly similar if they processed invoices manually within the accounting system.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases. The AZURE architecture is shown in the diagram below:

Enerpact APX Cloud Architecture

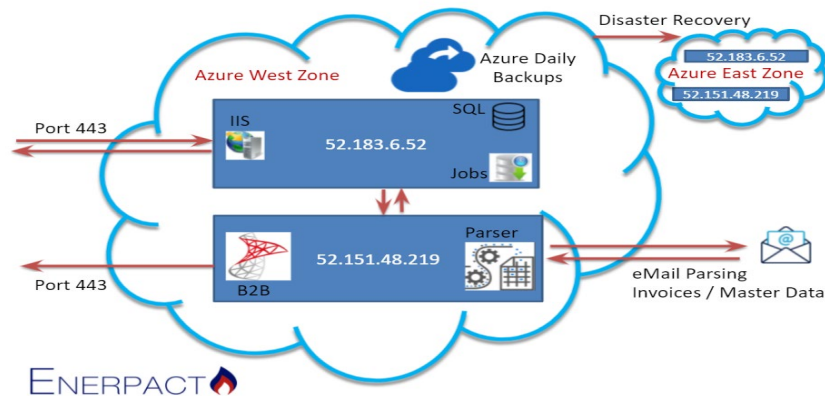


Enerpact APX Components & Architecture



e. Servers

All servers ENERPACT uses are hosted on the Azure (AZURE). Enerpact Servers are restricted with only HTTPS Inbound requests. No other outbound ports are opened.

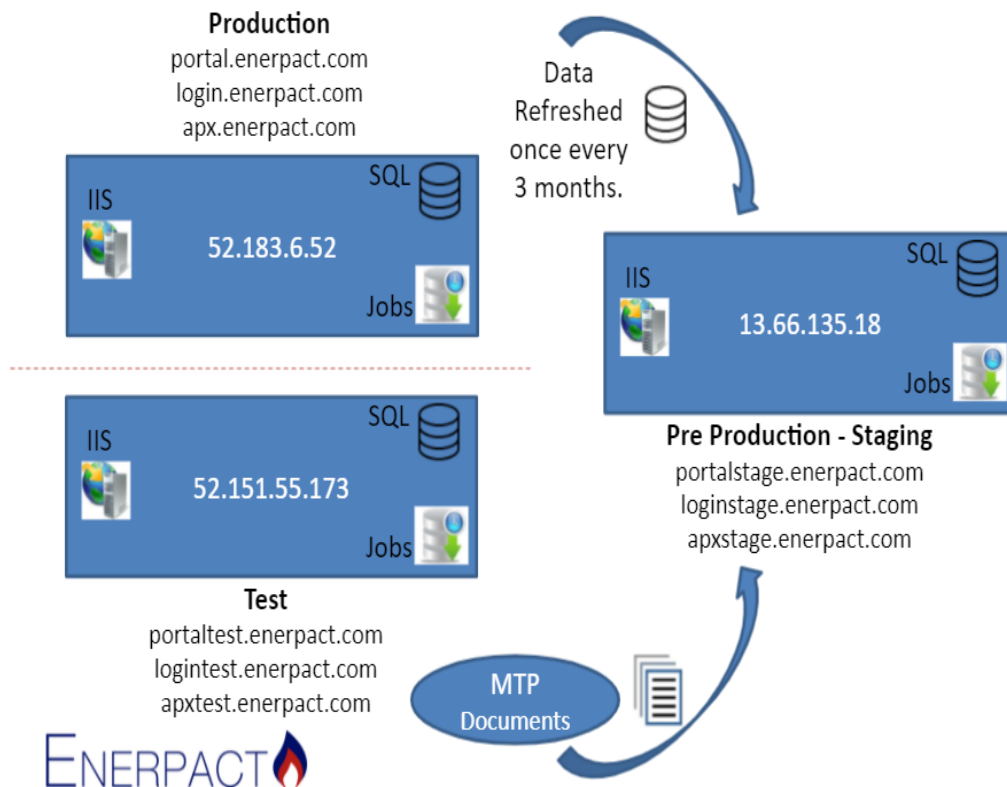


f. Database

All databases used by ENERPACT are hosted on AZURE as a managed service. In these types of provided services AZURE is responsible for the management, operation and security of provided databases. Enerpact Azure Infrastructure has been secured to provide access only to authorized users. Logging in Portal is done through Multi Factor Authentications. Remote Desktop is authorized only using Just In Time Activation for Whitelisting Enerpact Users IP and then allowed.

Enerpact has enabled Azure Defender and various other Azure Notifications in prevention of any Ransomware / Malware attacks in Enerpact Cloud Infrastructure:

- Azure Remote Desktop Login and Logout Notifications. To monitor only authorized users are logging into the system.
- Ransomware Check. Any unexpected files created and any files created that have exceptional sizes are monitored using File Server Resource Manager.
- Azure Notification for any Administrative Activities. The likes of User Creation, VM Management, NSG, IP Whitelisting, Backups Management etc.
- Azure Defender in place.
- Azure Notification on SQL Injection.
- Azure Notification on Brute Force Attack.
- Drive Space Alert: Enerpact Framework monitoring is set in place to notify any drastic changes in Drive Storage changes.
- SQL Server Restart Notifications to understand any unwarranted changes in the system.



g. Software

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Objects	Providers
Cloud Servers	Microsoft Azure
DNS	GoDaddy
Ticketing System	Bug Tracker (Customized)
Web Server	Internet Information Server
Development Stack	MS .NET, MS Identity, SQL Server, Rapid Dev Tools like DevExpress & Telerik, Doconut, Gmail Business, BizTalk.
DMS	Open KM
AI Parsers	Rossum, Adobe DC, Invoice2Data
Version Tracking Build Tools	TFS, Jenkins

h. Data

Enerpact keeps client data for one year unless there is a contract for a longer period with each individual client. Typical SLA with a client is written on the following broad topics to take into consideration the guarantee of recovery and loss of customer data:

- Availability (e.g. 99.99% during work days, 99.9% for nights/weekends)
- Performance (e.g. maximum response times)
- Security / privacy of the data (e.g. encrypting all stored and transmitted data)
- Disaster Recovery expectations (e.g. worst case recovery commitment)
- Location of the data (e.g. consistent with local legislation)
- Access to the data (e.g. data retrievable from provider in readable format)
- Portability of the data (e.g. ability to move data to a different provider)
- Process to identify problems and resolution expectations
- Change Management process (e.g. changes – updates or new services)
- Dispute mediation process (e.g. escalation process, consequences)

i. Organizational Structure and Chart

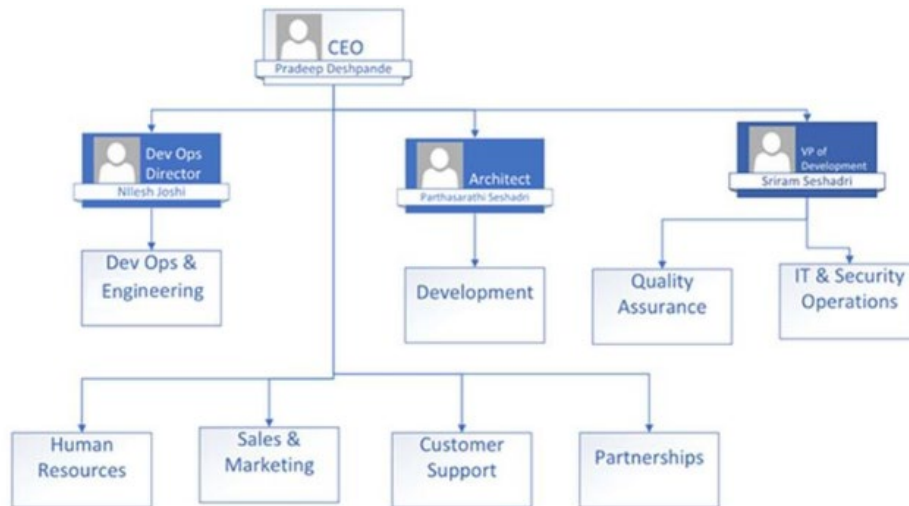
ENERPACT's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. The Company has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

ENERPACT's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This includes policies relating to business practices, knowledge and experience of key personnel, and

resources provided for carrying out duties. In addition, policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable are in place.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority, responsibility and lines of reporting.
- Management has considered the reporting structure and accountability for business functions and segregated responsibilities by functional areas.



Commitment to Competence

ENERPACT management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The Company's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into position requirements.
- An employee training program with a predefined calendar is in place.

Accountability

ENERPACT has defined lines of management authority, which are outlined in the organizational chart. On a bi-weekly basis, the senior management team, consisting of executives and managers across functional areas, meets to discuss any issues with the potential to impact multiple departments. Management maintains an "open door" policy to encourage personnel to bring forth questions or concerns.

ENERPACT uses documented hiring practices to ensure that new employees are qualified for their job responsibilities. The hiring process requires prospective candidates to interview with the department members with whom the candidate will work and with senior management. The chief executive officer (CEO) approves each prospective employee before ENERPACT extends an employment offer. Hiring policies and procedures include confirmation of prior work experience through performance of reference checks.

ENERPACT has established a code of ethics to guide its employees with the handling of internal and customer information. New employees sign the acknowledgement of employment contract containing code of ethics on their first day of employment. Additionally, employees are required to sign a Professional Employee Agreement, which

includes standard employment terms including requirements to conform with ENERPACT's code of ethics as described in the employee handbook.

Employees receive annual performance reviews. Each employee is evaluated based on performance criteria and management provides each employee with feedback. Salary increases and incentives are determined on the basis of the annual review. ENERPACT management conducts informal performance reviews for new employees at the end of a 90-days probationary period. Most of the Company's personnel hold certifications that are relevant to their area of expertise.

The following functional areas are used to support the services offered to clients as described within this report:

- Sales & Marketing – Does marketing of the product. This unit coordinates and produces all materials representing the business.
- Human Resources – This unit handles the HR related functions and Recruiting.
- Partnerships – This unit focuses on customer partnerships.
- Sales & Marketing – Takes the initiatives to connect with the customers to sell the product/services.
- Customer Support – Connect with the customers to communicate the system changes and collect the feedback as well as issues back to the engineering team.
- Development – Manages the development and enhancement of Software solutions.
- QA – Provides a quality testing process that ensures to deliver the best products or services possible to the customers.
- IT and Security Operations - Manages the cloud operations, IT tasks and Security Operations tasks.
- DevOps & Engineering – Focus on deployment process and automations.

j. Policies and Procedures

ENERPACT maintains a Policy Management Program to help ensure policies and procedures:

- Are properly communicated throughout the organization
- Are properly owned, managed and supported
- Clearly outline business objectives
- Show commitment to meet regulatory obligations
- Are focused on continual iteration and improvement
- Provide for an exception process
- Support the Policy Framework and Structure

Policy Requirements

Every policy has a Policy Owner who is responsible for managing the risk outlined in the Policy Objective. All policies are reviewed to help ensure they are relevant and appropriately manage risk in accordance with ENERPACT's risk appetite. All ENERPACT methodology documents and internal policies are reviewed at least annually.

Description of the Control Environment

a. Control Environment

The control environment at ENERPACT is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the senior management and the executive committee.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ENERPACT's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ENERPACT's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Management communicates entity values and behavioral standards to personnel through policy statements and codes of conduct.

Senior Management and Executive Committee Participation

ENERPACT's control consciousness is influenced significantly by the participation of the executive committee. Responsibilities of the executive committee are documented and understood by executive and senior management personnel.

Specific control activities that the service organization has implemented in this area are described below.

- A committee of senior management personnel is in place to oversee management activities and company operations.
- Senior management personnel meet on a daily basis to discuss management activities and operational issues. We work on Agile methodology and continuous integration and delivery methodologies.
- An external audit is performed on an annual basis to monitor financial statement reporting practices.

b. Risk Assessment

ENERPACT performs periodic Information Technology Risk Assessments (IT RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation measures. IT Risk Assessment is a vital component of Company Risk Management.

Enerpact has established an Information Security Risk Assessment, Review and Treatment Procedure. The overall scope of Risk Assessment framework includes the following:

- Identify and highlight that the resources are at risk
- Existing control measures are applied to the resource
- Mitigate improvement plan to minimize the risk (Both long and short term)
- Assignment and Deadline – who will be responsible and when control measures will be applied
- Estimate business risk level and impact estimate - both reputational and financial

Risk Assessment:

The risk assessment process starts from the assets and asset values from Enerpact's information assets inventory. The vulnerabilities and the threat that can make use of these vulnerabilities are identified. The likelihood and the impact of the threats are assessed. Based on the asset value and the threat value, the risk values of the information assets are

calculated. According to the risk level decision rules, the risk levels of the risks are determined based on the risk values. The risk levels will further guide the risk treatment process. The risk assessment results are reported to the Information Security and Data Privacy Workgroup for further assessment and treatment decisions.

#	Topic Name	Who	Name Role Type	Topic Description
1	Collect updated assets & asset values	Information Security Manager	Responsible	To perform the information security risk assessment, Information Security Manager retrieves the updated assets and asset values from the Asset Inventory.
2	Identify/update vulnerabilities of assets	Information Security Manager	Responsible	Information Security Manager identifies the vulnerabilities that exist in information assets or asset groups through assessment software, gap analysis against best practice baselines, asset analysis and professional experience.
3	Identify/update threats	Information Security Manager	Responsible	With environment analysis and/or professional experience, Information Security Manager identifies the threats that can exploit the vulnerabilities to cause damage. The external and internal threats from deliberate (intentional) or accidental (unintentional) sources or events are identified.
4	Identify likelihood and impact of threats	Information Security Manager	Responsible	For each information asset, Information Security Manager performs assessments on the likelihood the threat can occur and the exposure (loss) if the threats occur. Then the threat impact level is calculated based on the likelihood and the exposure value. Refer to <i>ISMS_PR_03_Information Asset Inventory and Risk Assessment Procedure</i> for methodologies and scenarios of threat impact calculation.
5	Calculate risk values	Information Security Manager	Responsible	Information Security Manager calculates the risk value of the information asset based on the asset value weight and the threat impact value. Refer to <i>ISMS_PR_03_Information Asset Inventory and Risk Assessment Procedure</i> for details of risk value calculation.
6	Evaluate risk values	Information Security Manager	Responsible	Based on the risk values of the information asset, Information Security Manager works out the risk levels of the information assets according to the predefined risk level rules. The risk levels together with the risk values will be used for prioritizing the identified risks and will guide the risk treatment process.
7	Report risk assessment results	Information Security Manager	Responsible	The risk assessment results and evaluations are reported to the Chief Executive Officer for further assessment and treatment decisions.

Risk Treatment: The risk treatment process starts with the risk assessment results from the risk assessment process. Information Security Manager identifies the controls for the risks and then presents the risk assessment with these controls to the Chief Executive Officer. The Chief Executive Officer considers the risks and takes the decision on the risk treatment approach. The risk treatment plan is sent to all responsible persons for the implementation of the necessary controls.

Risk Review: The risk review process aims to detect the changes in the risk environment and re-assess the defined risks and the effectiveness of the implemented controls. Periodically, a specific risk domain is selected for review based on various reports and risk factors. The risk review is performed according to a pre-defined checklist for the selected domain. Based on the risk review findings, the risk assessment and the risk treatment plans are updated to reflect the changes of risks and the improved controls.

c. Information and Communication

ENERPACT has implemented an internal knowledge base to disseminate information to employees. The information is primarily in relation to responses to customer inquiries, but also includes general information. Individual departments are charged with maintaining their relevant information in the knowledge base. Once information is finalized, it is published to the knowledge base for company-wide distribution. Publishing to the network is performed by IT and operations management who follow a two-step process ensuring that changes are approved prior to release to the production environment. Restrictive access controls are also applied if the material being published is not intended for general viewing.

ENERPACT has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities, and that significant events are communicated.

d. Information Security

The Information Security Policy addresses all information, systems, facilities, programs, data, networks and all users of technology in the organization.

Information Security Controls

Workstation configuration is determined by business requirements based on user role. All workstation hardware and software are approved by IT. Users request IT with service tickets or via emails for any additional software request with business justifications. Servers and server platforms, which store and/or process Enerpact data, are protected at least with:

- Antivirus.
- Data encryption.
- Host Intrusion prevention system and Host firewall.

To ensure data availability, integrity and service work stability all servers, which are running in Production mode, are mirrored and backed up on a regular basis.

A strict password policy is in place which ensures that users with locked accounts co-ordinate with ITIM Member services to reset the password. User authentication methods do not transmit credentials as plain text. User credentials are not cached or stored as plain text at any time. Passwords comply with the following requirements:

- Must contain characters from at least one uppercase, lowercase, number, special character.
- Password length should be of minimum 8 characters
- Cannot repeat the same password on rest (previous 5).

Password expiration:

- Expires in every 90 days.
- Expiry reminder sent with two weeks left to expire.
- Daily reminder of the last week of password expiry .

e. Change Management

ENERPACT's Change Management Policy provides a high-level overview of the change management process and applies to Enerpact, all employees and contractors using Enerpact assets. The Change Management Policy does not apply directly to Enerpact customers or other third parties (service providers) unless specified in contractual agreements. The foundation of an effective change control within Enerpact is the Change Management Policy. These stakeholders include the end users, the developers, the engineers, and the system and network administrators. Senior management's endorsement and enforcement of this policy are mandatory to successful implementation. The responsibility to manage this document is assigned to Information Security Manager of the Enerpact.

The main objectives of change management policy are to:

- The objective of the change management process is ensuring that changes are recorded, assessed, authorized, prioritized, planned, tested, implemented and documented and reviewed in a controlled manner.
- The goals of change management are to respond to the customer's changing business and responding to Requests for Change (RFCs in Appendix A) from the business and IT.
- Changes must be controlled adequately, so that the exposure to risks is minimized, the severity of the impact and service interruption is minimized and the change is implemented successfully in first attempt.
- For emergency cases, with the decision and the approval of the Information Security Manager, the change control process includes a "fast path" to handle high-risk change requests in a compressed decision cycle.

The policy rules are outlined below:

Request for Change and Change Approval

- The change is raised by a request from the initiator - the individual or organizational group that requires the change. All RFCs must be registered in Support team or development team to identify them via unique identification numbers.
- The scope and impact of the eventual change determine how much information is required for the change.

Change Implementation

- IT cost estimations are re-evaluated during impact assessment.
- After the development activities, development tests and functional tests must be done by different parties.
- User acceptance tests are to be done by business users.

Change Management Records

- Having acquired verbal/written confirmation/verification of the Change Requestor change record may be closed.
- For the completion of the change items, the business will be informed.
- Change Management process is continuously monitored. The Post Implementation Review must be conducted.

f. Logical Access

1. User Access Provisioning

Access to all information systems used within Enerpact infrastructure is granted by creating a discrete user account by designated System Administrators after necessary approvals. User accounts may be privileged or unprivileged. Security-relevant actions performed on behalf of a user are traceable to the user and the user is accountable for the actions. User account request registration is administrated by the Information Security Manager. The Asset Owner is responsible and accountable for appropriately controlling access to their assets. The Asset Owner maintains the list of groups and monitor the security related activities of the user accounts creation and user account activities. Users are issued a single unique user ID and all accounts on various components created on behalf of that user are based on that unique user ID. A non-privileged user has a single account per component. There are two main types of non-privileged accounts:

- Default User Account is created and added to the core Enerpact systems, according to the newcomer's role in the list of groups;
- Requested User Account is initiated via Service Desk request or relevant type of communication for those who are not a member of any Enerpact team, though need to have an access to Enerpact resources, with the following information:-
 - Account purpose, which is short account description;
 - Project name, namely the name of the projects, in which account will be involved;
 - Access permission, namely with what folders/servers/services and with what access type user must be provided;

System Administrators whoever in charge of assigning user ID assign a unique user identifier (user ID) and an initial password. The user ID and the (initial) password are communicated to the user in a secure manner.

2. User Access De-Provisioning

User accounts are disabled prior to being deleted whenever the account is no longer needed
Accounts are deleted based on the following:

- Change of duties or operating location for the owner of the account;

- Change of owner's team;
- Termination of the owner's business need for the account;
- Termination of employment of the owner of the account;

On the request of CEO, the account of a dismissed employee may be saved from deletion. Prior to the deletion of an account, the directories, mailbox and files owned by the account are reviewed and reassigned as appropriate by System Administrator in co-operation with the appropriate Manager.

3. *User Role Changes*

User role change upon change of team or duties or location is covered in above two points.

4. *Risk Assessment (Vulnerability Scanning)*

This is a continuous ongoing process to evaluate the vulnerabilities. The risk assessment process starts from the assets and asset values from Enerpact's information assets inventory. The vulnerabilities and the threat that can make use of these vulnerabilities are identified by security experts. The likelihood and the impact of the threats are assessed. Based on the asset value and the threat value, the risk values of the information assets are calculated. According to the risk level decision rules, the risk levels of the risks are determined based on the risk values. The risk levels will further guide the risk treatment process.

5. Encryption

ENERPACT uses Microsoft Encryption model to store user credentials. For authentication the MS Identity module is used and the passwords are stored in the standard encryption model. The ASP.NET Core Identity password hasher mode uses the PBKDF2 algorithm with HMAC-SHA256, 128-bit salt, 256-bit subkey, and 10,000 iterations.

g. Physical Access

Due to the pandemic, all employees are working from home. The office space has been given up and some remaining devices have been shifted to a storage facility. So, the physical controls and environmental controls are not applicable.

ENERPACT's entire architecture is on AZURE. Azure is responsible for maintaining the physical and environmental security with respect to the services as per the AZURE Shared responsibility model.

Remote Facility Resource Access –

- Remote access is restricted to individual authorized users only.
- All remote access uses a two-factor authentication that meets the requirements in the following section.
- It is the responsibility of Enerpact employees, who have remote access privileges to the internal Enerpact network, to ensure that their remote access connection is given within the same security considerations as the user's on-site connection. The user demanding remote access submits a request by using the internal new access right request process.
- Logging in Portal is done through Multi Factor Authentications
 - Azure Password and Authentication through Microsoft Authenticator App in the registered mobile.
 - All user accesses are monitored and logs reviewed to ensure no unauthorized access was made in the servers.
- Remote Desktop is authorized only using Just In Time Activation for Whitelisting Enerpact Users IP and then allowed.
- There is one Jump Server that has the ability to do JIT activation and the rest are accessible only from the Jump Server.
- The user accounts under Azure Portal are managed as part of Entry and Exit process and with necessary approvals.

Enerpact Application Security

- Enerpact application security is covered with Authentication and Authorization framework modules.
 - Enerpact Authentication framework is built on top of Microsoft Identity Authentication services.
 - Enerpact Authorization (ISAM) is built around the Enerpact Authentication framework.
- Enerpact Authentication Framework requires a Unique ID either eMail or a Unique User ID for the user to login. There are 3 types of Admin users who can manage the users in the system.
 - Enerpact Super Admin: Users with this role can enable Application for clients based on their subscription.
 - Enerpact Admin: Users with this role can create Client Admin users manage their account in case of any support issues. On a need basis these users can also manage client users.
 - Client Admin: Users with this role can only grant/deny access to Client Users.
- **USER NAME**
 - Users of Enerpact Portal are identified with a unique User ID. This can be users' email (preferably their official email) or a unique name assigned by the User Admin.
- **PASSWORD**
 - Below are the password minimum requirements
 - Require at least one digit (0-9)
 - Require at least one lowercase letter (a-z)
 - Require at least one non alphanumeric (other than 0-9 and a-z)
 - Require at least one UPPERCASE letter (A-Z)
 - 8 Characters minimum
 - Cannot repeat the same password on reset (previous 5).
- **PASSWORD EXPIRATION**
 - Enerpact reminds the users on their password expiration
 - Expires every 90 days
 - Expiry reminder sent with two weeks left to expire.
 - Daily reminder of the last week of password expiry.

h. Capacity Management

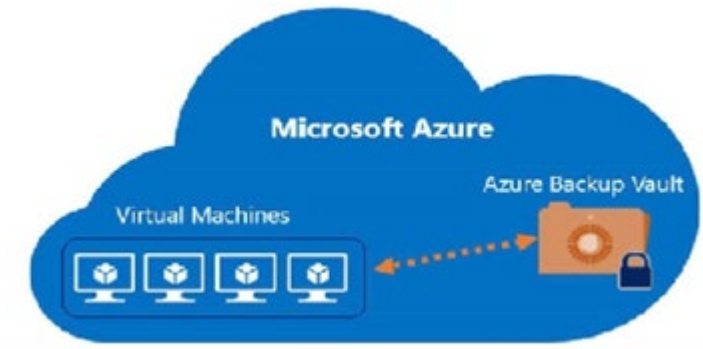
A capacity planning program helps ENERPACT determine what the current and future resource (people and technology) needs are in order to meet customer expectations of the goods and services being delivered. Currently, the ENERPACT stakeholders gather the necessary data to forecast compute (processing) and capacity (storage) trends, where the potential resource thresholds are, when the thresholds will be reached and what are the identified resources needed to help ensure compute and capacity are meeting customer needs and expectations.

A capacity planning process needs to happen on a perpetual basis to help ensure the projections are accurate and complete. With capacity planning in place, customer needs will be better met, compute and capacity resources will be better optimized for use and capital expenditure forecasting will be more accurately reported for guidance to investors.

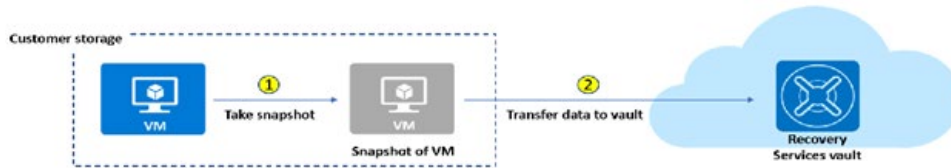
i. Backup and Restore

Data Backup

All three APX instances (Prod, Stage & Test) are backed up using Azure Cloud Vault backup system at various frequencies designed to eliminate any loss of user data, latest code changes and transactions.



Enerpact has determined the best economics is using Azure vault. Azure vault backups store snapshots of entire instances virtual both locally on the instance and remotely in the cloud. The backup mechanism does so almost instantly and with minimal overhead and impact to the system performance. The backups are remotely stored in the cloud and guards against any possibility of losing backup due to intentional or unintentional deletion of backups. This also addresses offsite backup requirements.



APX sites are backed with the following frequency:

System	Extent	Frequency	Locale
Production APX	Complete VM	Every 2 hours from 8AM to 5PM CST	Stored locally & Azure Vault
Test APX	Complete VM	Nightly	Stored locally & Azure Vault
Stage APX	Complete VM	On demand	Stored locally & Azure Vault

Recovery Process

Enerpact APX production data is restored every time a new version of the APX migration is planned. It is critical to have the latest data to test the application before the new version is moved to production. Part of the change management process requires us to restore a production VM into stage. Then make changes to both code and database objects in the test. This process helps us test the recovery process on an ongoing basis.

Enerpact APX disaster recovery process from PRODUCTION to STAGE occurs on a weekly basis. This change is tracked by adding a record to the change tracker.

Enerpact APX Change Management process requires development of new versions to start with production footprint. This restoration process occurs almost on a weekly basis. Enerpact exercises restoring the test instance VM back into test instance at least once every two weeks. This change is tracked by adding a record to the change tracker.

Enerpact APX disaster recovery process is exercised frequently that combined with the usage of Azure infrastructure guarantees restoration process in case of disasters. Gives the assurance needed to sign necessary SLAs. This change is tracked by adding a record to the change tracker.

Enerpact APX database disaster recovery process is tested every month by restoring a production VM into STAGE and then applying the logs from the time the VM snapshot was taken to restore the transactions that occurred after the VM Snapshot is taken. This change is tracked by adding a record to the change tracker.

Data Restore

Must the data be damaged or lost during normal operations, the System Administrator attempts to restore the data using the most recent backup. In case the information cannot be restored from the most recent backup, the appropriate backup is retrieved.

In a situation where old copy of a file is used for the restoration, the following is performed:

- The Asset Owner is informed of the issue and the date of the file used for the restoration.
- Procedures to restore the contents of the lost file by updating the old version of the data is activated.

If a hard disk of a laptop or server fails, a new hard disk is formatted and the contents of the lost drive restored to the new drive. Procedures address reconstitution of hard disks specifically addressing drives containing operating systems and/or relational database management systems. If a mainframe loses a hard disk, procedures are followed for replacement of the drive. Procedures specifically address fail over for drives providing mirroring services.

Reconstitution of systems that are lost due to a catastrophic event is addressed in contingency, business continuity, and disaster recovery planning. Any procedures associated with a plan address the continuous protection of backup storage. If special software or hardware is required to support processing of backup storage, the means of addressing those requirements are identified before the plan is published.

j. Monitoring

Management at ENERPACT undergoes periodic external audits and assessments to evaluate control effectiveness, and, in some cases, receive recommendations for improvement. Additionally, internal examinations of controls are performed as business needs or regulatory environments dictate.

The stakeholders in the audit processes report any finding to a member of the senior management team. The senior management team meets on a periodic basis to review company issues and plan direction. Reviews of current and upcoming audits are performed during these meetings and input is solicited from the team.

Monitoring systems at ENERPACT are set with automatic alerting thresholds that generate system alerts to the Azure Notifications for any failures noted within ENERPACT's systems. System alerts are categorized by severity and dispatched accordingly to the teams for investigation. CloudWatch alarms and actions are configured with all enabled AZURE services logs. A log metric filter and alarm exist for unauthorized API calls, for management console sign-in without MFA, for usage of root account, for IAM policy changes, for CloudTrail configuration changes, for AZURE management console authentication failure attempts, for S3 bucket policy changes, for AZURE configuration changes, for Security Group and NACL changes and for VPC level changes. EC2 monitoring is enabled.

In addition, some of the notifications release tickets into ENERPACT Services Desk, when they are tracked by ENERPACT Operations Team. Every security and performance related event is recognized, stored, analyzed and evaluated from the several perspectives. Relevant findings are analyzed in depth and if necessary new remediation actions are performed.

Evaluating and Communicating Deficiencies

Customer complaints are tracked in an automated ticketing system (Enerpact Tracker) and reviewed on a quarterly basis for consideration on how to improve control activities. Regulator comments and feedback are incorporated and reviewed by senior management at the conclusion of any audit or auditable actions.

All ENERPACT methodology documents and internal policies are reviewed at least annually. Lessons learnt from projects and daily operations are harvested and all findings are incorporated into the new version of documents. Dedicated employees of ENERPACT update methodical document and internal policies to reflect the current needs and real-life operation in project and in daily work.

k. Incident Management

- Documented incident response and support procedures are in place to guide operations personnel in the monitoring, documenting, escalating, and resolving of problems affecting managed hosting and network services.
- The Chief Executive Officer is accountable for the management of Enerpact Incident Management Program. For providing resources needed to manage incident management and for external communications regarding incidents.
- Information Security and Data Protection Manager is responsible for reporting of incident management efforts and operational loss data due to incidents to the CEO, analyzing incident statistics and trends, determining business process improvement possibilities according to incident and prevention/registration/investigation and documentation of personal data incidents.
- Personnel/staff are responsible for timely and proper reporting of incidents and disseminating the lessons learned from incidents to appropriate peer.

Incident Registration and Prioritization

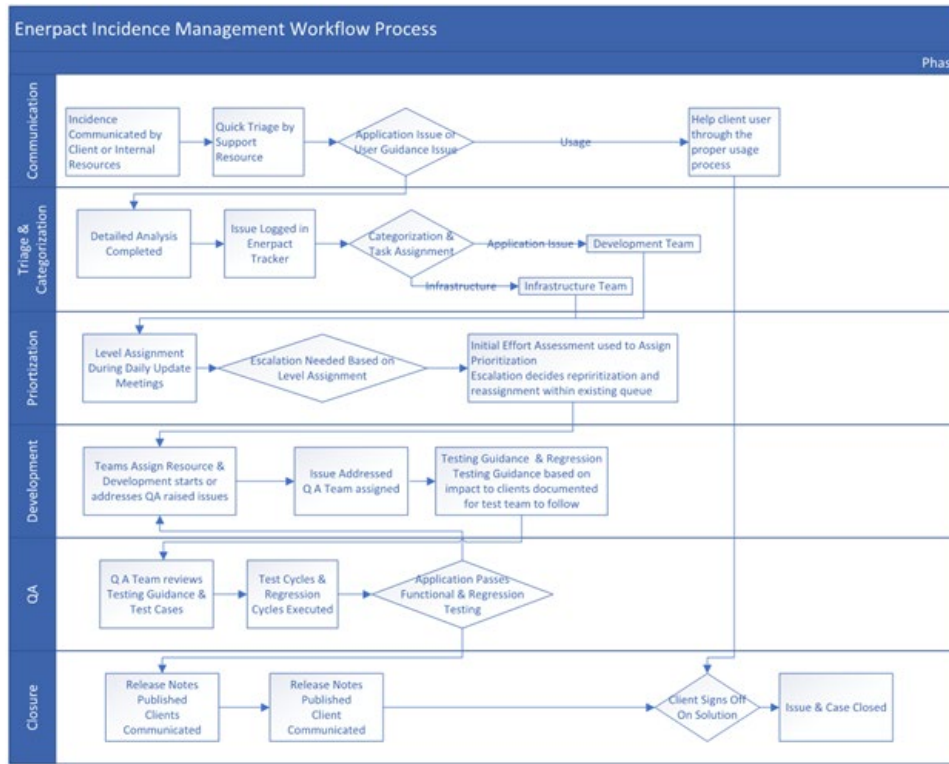
- All incidents are registered and an appropriate response is assured for all incidents reported by clients or internal resources. Categorization is based on the type of issue and the type of effort that will be needed to address the incidence. Prioritization can normally be determined by taking into account both the urgency of the incident (how quickly the business needs a resolution) and the level of impact it is causing.

Incident Response

- Response to an incident is guided by the principle of proactively minimizing damage to Enerpact's reputation, assets, and partners and rights and freedoms of individuals. On receipt of an incident, Ticket is initiated and reported issue is investigated based on the category of the incident.
- Investigation and diagnosis:
- All incidents are diagnosed based on the type of reported incidents and investigated by the designated responsible owner.
- Escalation methods and principles:
- Criteria for escalating the incident investigation are defined. These criteria include when and how the incidents are escalated.
- Resolution and recovery actions:
- Resolution and recovery actions are identified and documented.
- Protection and retention of evidence:
- The gathered evidence is retained based on applicable Azure and regulations.
- All incidents are officially closed after recovery is completed. Incident closure must define the incident properties that need to be updated to contain relevant information about the incident.

- VP of Development issues general inter-and intra-company communications regarding an incident if needed and decided. External communications are performed by the Chief Executive Officer.

Incident Flowchart:



Tracking Systems:

Enerpact manages changes to both the servers and applications using a change management system. System changes and application changes are logged, tracked and reported using a tracking system called Enerpact Tracker.

- Issues reported by Customers are logged into the system as tickets.
- Tickets have a predefined life cycle followed rigorously for all material changes.
- A ticket once logged follows the life cycle of change through the following steps:
- Ticket Creation
- Assignment to developers
- Reporting of change made
- Assignment to QA resource
- QA assurance cycle with any reported issues going back to the developers
- QA approves change to the system
- Management approval of all changes
- Change management team creates an MTP document
- Document reviewed by both developers and change management team
- Change planned and made during low system usage time
- Employee Onboarding and Terminations are documented as a ticket.
- Change Requests are tracked.
- Every change is recorded as a Minor change or a Major change based on the effort, fixes, and new functionality being released with the latest change.
- Changes are tracked and documented with Release Notes.

SLA:

Enerpact agrees to SLAs with clients on the following broad topics as per the client needs. SLAs are added as part of the:

- Availability (e.g. 99.99% during work days, 99.9% for nights/weekends)
- Performance (e.g. maximum response times)
- Security / privacy of the data (e.g. encrypting all stored and transmitted data)
- Disaster Recovery expectations (e.g. worse case recovery commitment)
- Location of the data (e.g. consistent with local legislation)
- Access to the data (e.g. data retrievable from provider in readable format)
- Portability of the data (e.g. ability to move data to a different provider)
- Process to identify problems and resolution expectations
- Change Management process (e.g. changes – updates or new services)
- Dispute mediation process (e.g. escalation process, consequences)

I. Complementary Controls at User Entities

ENERPACT's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called Complementary user entity controls. It is not feasible for all of the Controls Objectives related to ENERPACT's services to be solely achieved by ENERPACT control procedures. Accordingly, user entities, in conjunction with the services, are established on their own internal controls or procedures to complement those of ENERPACT.

The following complementary user entity controls are implemented by user entities to provide additional assurance that the Controls Objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors have exercised judgement in selecting and reviewing these complementary user entity controls.

- a. User entities and subservice organizations are responsible for understanding and complying with their contractual obligations to ENERPACT.
- b. User entities are responsible for notifying ENERPACT of changes made to technical or administrative contact information.
- c. User entities are responsible for maintaining their own system(s) of record.
- d. User entities are responsible for ensuring the supervision, management and control of the use of ENERPACT services by their personnel.
- e. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ENERPACT services.
- f. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
- g. User entities are responsible for ensuring the confidentiality of any user IDs and passwords used to access applications hosted by ENERPACT.
- h. User entities are responsible for ensuring that the data submitted to ENERPACT is complete, accurate and timely.
- i. User entities are responsible for immediately notifying ENERPACT of any actual or suspected information security breaches, including compromised user accounts.
- j. User entities are responsible for defining the communications method utilized to connect to ENERPACT's systems.

SECTION 4: Independent Service Auditors' description of Controls

PROJECT PLANNING AND MONITORING	<i>1. Controls provide reasonable assurance that project plan which forms the basis for project execution and monitoring of project activities are prepared and approved.</i>
--	---

CONTROLS
1.1 A project plan is prepared at the start of each project. The plan includes project metrics management, project risk management, defect prevention, knowledge transition and configuration management plan.
1.2 A Statement of Work (SoW) is agreed upon and documented between ENERPACT and its user entities for the application development and maintenance services provided by ENERPACT.
1.2 Effort estimates (wherever applicable) are prepared for incoming project work requests and customizations by the Project Engineering Team.
1.4 The project plan is reviewed and approved by the Delivery Manager.
1.5 Project status review meetings are conducted as per the frequency specified in the plan or as agreed upon with the user entities. Action items identified during the course of the meeting are documented in specifications document and entered in the Tracker.

APPLICATION DEVELOPMENT	<i>2. Controls provide reasonable assurance that key stages of the application development are documented, monitored and defects are addressed before release.</i>
--------------------------------	--

CONTROLS

- | |
|---|
| 2.1 There exists a formal methodology for system development and product implementation. |
| 2.2 The design document is prepared by the Project Engineering Team on the basis of the approved SoW document. The design document is then reviewed by the Team Leader of the Project Engineering Team or the user entity before commencing the system development phase. |
| 2.3 Checklists containing guidelines for identifying requirement specifications, design documentation, coding, test case preparation (unit, integration and system test cases) and product implementation exist |
| 2.4 A record of notes for each release is maintained by the DevOps Team during product releases. This is recorded in a tracker. |
| 2.5 Testing is carried out by testing team as per project plan and bugs identified during testing (unit, integration and system testing) are logged in a defect tracking system and tracked to closure. |
| 2.6 User Acceptance Testing (UAT) signoffs are obtained from the user entity before releasing the source code along with the deployment guide and release notes to the user entity. This is done in the Staging Environment. |
| 2.7 Access to modify code in development source code libraries is restricted to user accounts accessible by developers. |

- | |
|--|
| <p>COMPLEMENTARY USER ENTITY CONTROLS</p> <ul style="list-style-type: none"> • User entity is responsible for providing details such as planned scope, expected functionality and assumptions for requirements related to application development. • User entity is responsible for assessing and taking required action on the known open issues or defects. |
|--|

APPLICATION TESTING	<i>3 Controls provide reasonable assurance that the application testing is performed and defects are documented and communicated to the user entity.</i>
----------------------------	--

CONTROLS	
3.1	Requirements for creating test conditions or test conditions received from user entity, are logged by the testing team in the user entity provided tool or as specified in project plan, and are allotted a unique reference number.
3.2	Peer review of the test cases is performed and review comments if any are documented in the defect tracking system or as specified in the project plan.
3.3	Test results are updated in the test case documents and defects are logged in a user entity provided tool or as specified in the project plan and communicated to user entity.
3.4	Application development and testing efforts are performed in development environments that are logically separated from the test and production environment.
COMPLEMENTARY USER ENTITY CONTROLS	
User entity is responsible for providing accurate details about the test conditions.	

<p>APPLICATION MAINTENANCE</p>	<p><i>4. Controls provide reasonable assurance that user entity requirements for maintenance projects are documented and tracked to closure.</i></p>
---	--

<p>CONTROLS</p>
<p>4.1 There exists a formal methodology for system maintenance projects.</p>
<p>4.2 Work items are created in a work item management tool for maintenance or enhancement requests and a unique work item ID is allocated and tracked to closure. The tool captures effort and schedule estimates, and status of each work item as per the guideline in project plan.</p>
<p>4.3 There exist guidelines for coding and test case preparation.</p>
<p>4.4 An impact analysis is performed as per the classification of work items to analyze the impact on existing systems and estimate the effort to complete the work item.</p>
<p>COMPLEMENTARY USER ENTITY CONTROLS User entity is responsible for providing accurate enhancement or maintenance work specification request.</p>

**INFORMATION SECURITY
FRAMEWORK**

5. Controls provide reasonable assurance that information security policies and procedures are documented and appropriately communicated to employees.

CONTROLS

5.1 ENERPACT has developed an Information Security (IS) Policy, which covers aspects relating to information security. These policies are reviewed at least annually or when significant changes occur, and are approved by the CEO. The IS policies are made available on the intranet to the ENERPACT employees.

5.2 There exists an information security organization headed by the CEO. The roles and responsibilities of the members of the information security organization are defined.

5.3 Employees are required to read and accept the terms and conditions containing do's and don'ts upon their hire. All new employees sign a Non-Disclosure Agreement (NDA).

5.4 New joiners are required to undergo induction training which comprises of information security aspects at ENERPACT. Information security related policies and procedures are communicated to the employees during induction training.

5.5 Information security team is responsible for creating and maintaining the risk assessment framework which is to be used for conducting the risk assessment.

5.6 Periodically, a specific risk domain is selected for review. The risk review is performed according to a pre-defined checklist for the selected domain. Based on findings, the risk assessment and risk treatment plans are updated to reflect the changes of risks and the improved controls.

HUMAN RESOURCES

6. Controls provide reasonable assurance that only selected candidates with appropriate skills and experience are hired and trained to fulfill the business requirements.

CONTROLS

6.1 There exists a policy and procedure document that describes the hiring process applicable to employees within ENERPACT. The document is reviewed by CEO on an annual basis.

6.2 Candidates are evaluated for fitment to the job positions by the Technical and the HR Team members during the interview process.

6.3 All new joinees sign an acceptance and agreement to the Internet, Email and Computer Use Policy which contains the do's and don'ts towards information and information systems.

6.4 All the new joinees sign an offer document as their acceptance and agreement to gross remuneration and other terms of employment.

LOGICAL ACCESS	<i>7. Controls provide reasonable assurance that logical access to information system resources is restricted to authorized individuals.</i>
-----------------------	--

CONTROLS	
7.1	User access control policy and procedures are formally documented as part of ISMS and reviewed on an annual basis by the CEO.
7.2	User accounts for the ENERPACT domain are created upon receipt of email confirmation from the HR as part of the on-boarding process.
7.3	Access to the domain and user account is revoked by the IT Team upon termination of an employee on their last working day.
7.4	Administrative access to workstations is restricted to authorized personnel. User access privileges for users are approved by authorized personnel as defined in the approval matrix.
7.5	A password policy is applied to all user accounts that are created and managed directly in Microsoft Azure AD.
7.6	There is a defined password policy configured on the domain controller specifying minimum password length, maximum password age, password complexity requirement and account lockout.
7.7	If there is a project request to provision servers, ENERPACT uses solely AZURE as a cloud provider.
7.8	Apart from the common intranet for all employees, specialized departments have their own Google Drive as well which contains all relevant materials and information.
7.9	User access to the production database is restricted to limited users that have a unique username and password.

NETWORK SECURITY	<i>8. Controls provide reasonable assurance that access to ENERPACT's network components is restricted to authorized individuals, protected from network intrusions and the systems are protected from malicious software.</i>
-------------------------	--

CONTROLS	
8.1	There exists a formal policy and procedure document that describes the process for controlling access and protecting ENERPACT's network components. The document is reviewed by CEO on an annual basis.
8.2	Data Loss Prevention and Protection systems have been installed to detect and prevent potential data breaches / data ex-filtration transmissions in the organization's network. Incidents identified, if any are tracked to closure. Azure secure portal is used to manage and track all actions.
8.3	Use of removable media to store or transfer ENERPACT's information is prohibited. Employees sign the terms during the absorption period.
8.4	Audit log of computer/server operating systems are configured to be active.
8.5	The Gateway between ENERPACT network and the internet is protected by Firewall, intrusion prevention system, Gateway antivirus and content filtering.
8.6	Firewall rule sets are reviewed on a quarterly basis. This is managed in Azure Secure portal.
8.7	All components are monitored for intrusion attempts. Suspected intrusion attempt patterns potentially leading to denial of service (DoS/DDoS) are deemed a confirmed intrusion attempt.
8.8	Update Management in Azure Automation is used to manage operating system updates for Windows virtual machines.
8.9	Vulnerabilities and penetration testing is in place.
8.10	All e-mail attachments encrypted by the mail system are scanned before the contents are accessible to employees.

CHANGE MANAGEMENT	<i>9. Controls provide reasonable assurance that changes to network design and components are documented and authorized.</i>
--------------------------	--

CONTROLS
9.1 There exists a formal procedure for managing changes to systems and infrastructure which are approved and reviewed by management on an annual basis.
9.2 Changes to ENERPACT infrastructure are documented in a tracker and a change control form is raised by the IT Infrastructure team. Documentation includes the change number, description, classification, and business reason for the change, priority, impact analysis and time to implement.
9.3 Access to migrate the application source code changes to production is restricted to System Administrators.
9.4 Changes to network devices, server and firewall configurations are required to follow the change management process and approval and authorization are required prior to implementation. Post implementation of the changes, network and IT architecture diagrams are updated.
9.5 Changes to source code result in the creation of a new version of the application code. Changes are capable of being rolled back to prior versions of the application code when needed.

<p>SECURITY INCIDENT MANAGEMENT</p>	<p><i>10. Controls provide reasonable assurance that incidents related to information security are logged, resolved and tracked to closure.</i></p>
--	---

<p>CONTROLS</p>
<p>10.1 Process manual for incident handling is defined and documented which covers procedures for identification and escalation of security breaches. The process manual is published and available on the company intranet.</p>
<p>10.2 Documented procedures exist for the identification and escalation of security breaches and other incidents.</p>
<p>10.3 Security incidents are logged in the incident tracker and tracked to closure by authorized personnel.</p>
<p>10.4 Security relevant incidents are logged in the incident register and reviewed on a regular basis for the timely closure of incidents. Issues identified, if any are tracked to closure.</p>
<p>10.5 A formal disciplinary process is defined for employees who have committed an information security breach. The disciplinary action is decided based on the severity of the information security incident.</p>

Annexure: List of Abbreviations

S. No.	Abbreviation	Expanded d Form
1	AD	Active Directory
2	AICPA	American Institute of Certified Public Accountants
3	CCTV	Closed Circuit Television
4	CEO	Chief Executive Officer
5	HR	Human Resources
6	IS	Information Security
7	ISMS	Information Security Management System
8	IT	Information Technology
9	NDA	Non-Disclosure Agreement
10	SOW	Statement of Works
11	UAT	User Acceptance Testing