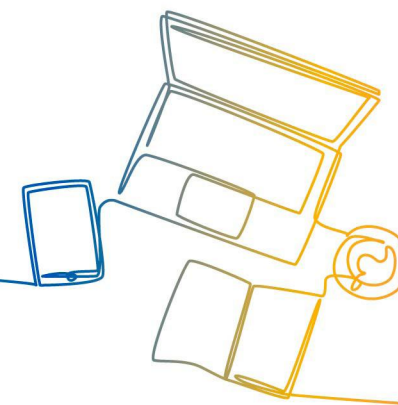


INTELLECTUAL CAPITAL



INTELLECTUAL CAPITAL

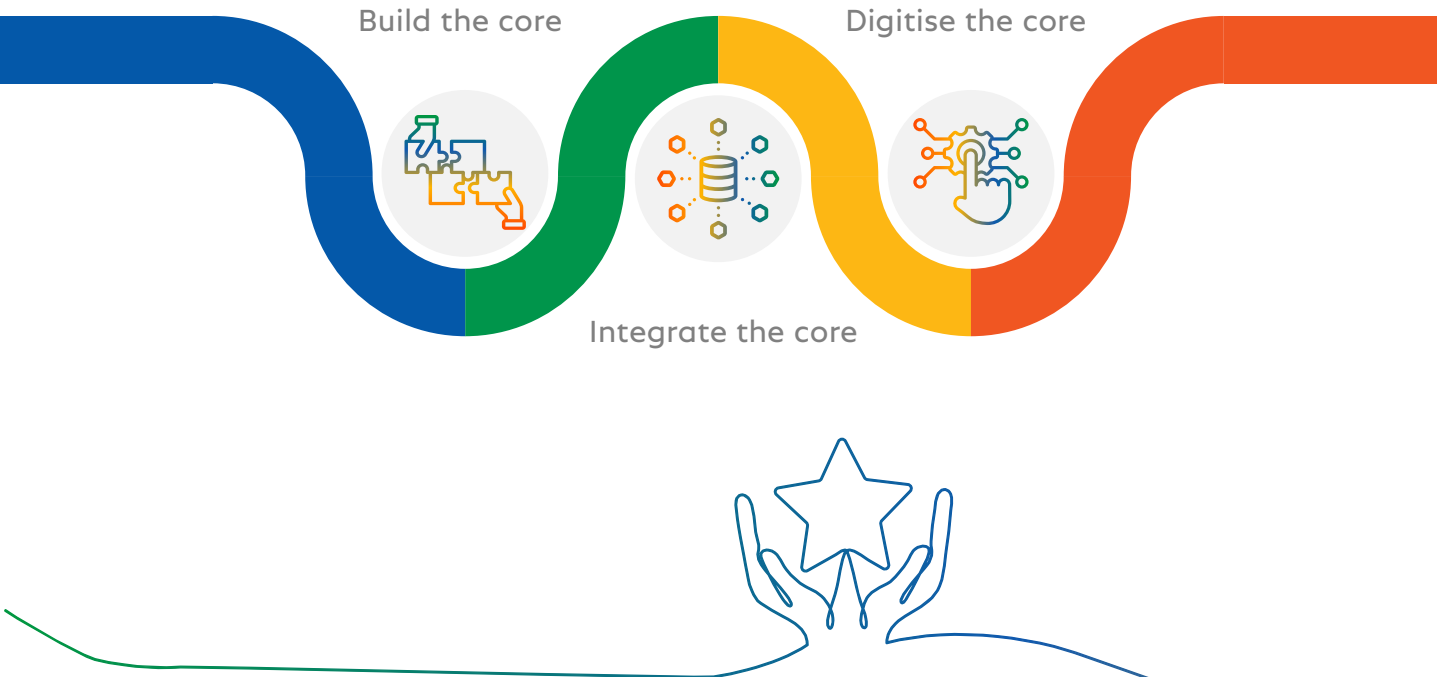
MATERIAL TOPICS

- » Digital Transformation
- » Data Security
- » Risk Management

Keeping pace with advancements in technology is important to be able to leverage them to the organisation’s advantage. At Apraava Energy, we value intellectual infrastructure and expertise that the Company has built over the years. We have always encouraged our people to be explorers so as to remain relevant in today’s rapidly evolving digital world. We firmly believe that a digitally advanced organisation is resilient in the long run. With this belief, Apraava has implemented number of digital initiatives to keep pace with the latest technologies and DigiVartan is one such key initiative.



Apraava’s Roadmap to Digitalisation



DIGIVARTAN

Our biggest digital project to date, DigiVartan, aimed at an organisation-wide transformation, was launched in August 2022. Through this project, we seek to build ‘ONE integrated business platform’ in a phased manner over a period of three years. The objectives involve harmonising and simplifying business processes on ONE Operating Platform, speeding up decision making and streamlining activities across businesses and functions.

As part of the project, we successfully implemented our greenfield cloud-hosted Enterprise Resource Planning (ERP) solution which enables us to make enterprise-wide decisions more efficiently. This project has also led to 75% reduction in paper usage and enhanced automated business processes including billing at our Renewable Energy (RE) sites and sale of fly ash and gypsum at JPL. Apart from this, we have also established a central monitoring hub at all RE sites; implemented an IT service management tool for tracking services, incidents, and safety reporting at JPL and, adopted end-user protection services and software suites -- BLISS and Diligent -- for paperless board meetings. Across JPL and RE business operations, we utilise Artificial Intelligence tools (AI) for analysis and optimisation of plant performance for enhanced results.

OBJECTIVES

- Working on ONE unified business platform
- Streamlining business operations through the usage of ONE comprehensive system
- Achieving transparency and eliminating confusion with ONE master dataset
- Establishing communication through ONE language with ONE set of definitions
- Expedite and enhance decision-making with ONE reliable data source
- Facilitating synchronisation of actions across different business units and functions

OUTCOMES

- Enhanced clarity and openness
- Augmented adaptability
- Elevated employee involvement
- Expanded opportunities
- Greater flexibility and responsiveness
- Superior operational framework

Transitioning to Paperless Invoices

Jhajjar Power Limited (JPL) is a coal-fired power station, produces ash and gypsum as regular by-products during power generation. We have tied up with several cement manufacturers, gypsum board manufacturers, brick manufacturers, traders and ready-mix concrete plants for the offtake of these by-products. This involves inward and outward movement of trucks to and outside JPL. For several years, this process involved use of printed invoices that amounted to over 35,000 copies in a month. Management of these invoices consumed 3-4 person days as well as fuel usage.

It was decided that this process could be digitalised through the logistics management system. The various teams involved collaborated to create and implement an integrated system for generating digitally signed invoices and cloud-based sharing with customers. Customers can now view and download their invoices through a web portal and also receive digitally signed invoices in real time through auto-generated e-mails.

The initiative has resulted in a 75% reduction in the quantity of paper printed for this purpose while also sensitising internal and external stakeholders about the importance of conserving resources and going digital without hampering the process.



ISO/IEC 27001:2022 - Information Security Management System Certification

OPERATIONAL TECHNOLOGY (OT)

Apraava Energy has successfully undergone ISO 27001 certification for its Jhajjar Power Limited's (JPL) Operational Technology (OT) Environment. This certification, apart from being critical for various compliance requirements of various government bodies, is testimony to Apraava Energy's commitment to best practice security framework to safeguard their information assets.

It helped stabilise JPL OT Security by providing a structured framework for mitigating security threats, strengthening people, process and technology pillars of cybersecurity.

INFORMATION TECHNOLOGY (IT)

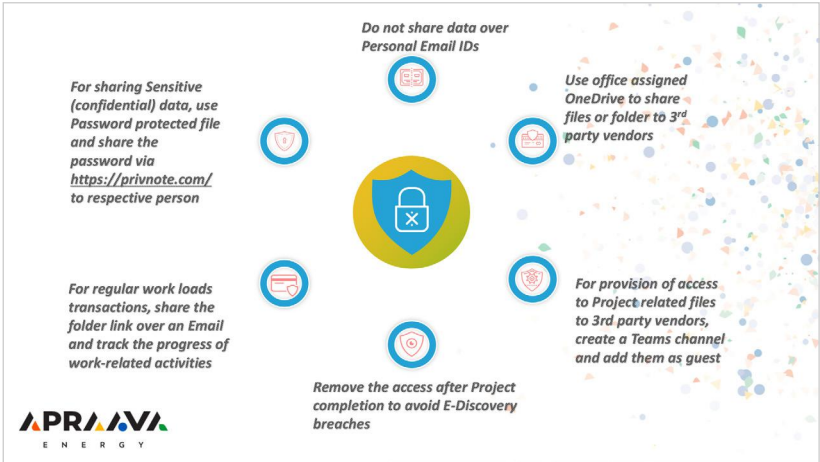
Further, Apraava Energy's Information and Security Management System (ISMS) underwent ISO 27001:2022 certification, to ensure best cybersecurity practices & procedures are deployed across the organization's IT systems uniformly.



Fortifying Cybersecurity Measures

At Apraava Energy, we are aware of the challenges that come with technology. In an increasingly digitalised world, data security risks are rising in tandem. Conscious of this, as we transition to more efficient digital tools, we also prioritise protecting our organisation, assets, and personnel from potential cyberthreats. To this end, we have implemented various measures to minimise these risks.

Our cybersecurity strategy is multifaceted, involving the implementation of robust policies and procedures; adoption of robust IT security practices and, regular cybersecurity awareness trainings for all employees. We also conduct thorough vulnerability assessments to identify potential vulnerabilities, threats and risks to our assets. Furthermore, our data protection infrastructure is designed to rigorously monitor and manage our systems, ensuring maximum security regardless of location or device used to access and process data. We prioritise confidentiality, integrity, and availability of critical information assets so as to maintain the trust and confidence of our stakeholders.



Supplier Invoice Fraud

From: Accounts <accounts@knownsupplier.com>
To: Accounts Payable <ap@recipientorg.com>
Subject: Change of bank details
Attachments: @ invoice.16.21.pdf

Hi Devon,

Due to a change in our accounts system, we have changed our bank details as follows:

Account number: 1241249123

Please direct payment for the invoice attached and all future invoices to the new account.

Regards,

Sam
Accounts Receivable
Known Supplier

Be vigilant & cautious of such emails that ask for bank details and transfer of funds to new accounts.

Please reach your Managers and IT Team during such Scenarios

[External] Tagged Emails

Did you noticed! we enforced an additional 'External' tagging to subject line of all Emails coming from outside of Apraava Domain, in addition to earlier 'Caution' note in email body.

The 'External' tag does not mean the message is a scam, but it signals you to be *extra cautious* on such email.

For Example, if you see an typical email from internal Apraava user / VIP user / generic account like from Admin/HR/IT, with 'External' tagging to subject line, and 'Caution' note in email body, then *beware*, it could be a case of email *spoofing*!

Risks of Storing Passwords in Browser

Malware If your device gets infected with malware, it could potentially access all your stored passwords in the browser.

Shared Devices In scenario of a shared device, your passwords could be breached by others.

Syncing As browsers offer data sync to your email ID, your passwords may get stored across multiple devices, on which emails is logged into, increasing the risk if any of those devices are compromised.

Phishing Attacks When users fall victim for Phishing passwords will be revealed. Auto filling of passwords in websites inadvertently provide your password to a fake website.

Lack of Encryption Passwords might not be encrypted or may only be encrypted with weak encryption methods, making them easier to steal.

Remembering passwords is best way, however if at all password need to be stored, it should be stored in single secured and encrypted format offline.

Secure Collaboration with OneDrive

As we navigate the digital landscape, it's "crucial" to *understand the significance of secure file sharing* and the "role OneDrive" plays in *enhancing our productivity while safeguarding our data*.

It is advised to use OneDrive, in the "Best Interest" of Compliance & Security Practices

Steps for Recommendation for Secure Files exchange

1. Create a folder and shift the files to be shared with Vendors
2. Click on Share option – add the Vendor Email IDs in Add name, group or Email
3. After adding the Vendor Email IDs, click on Copy Link
4. Paste the link in the Email
5. Address the vendor to share or receive the files by opening the link in the Mail

Security Features of OneDrive

1. Control access (view or edit) for each recipient
2. Will get reminders if the files are accessed or not
3. Confidential Files could be set with password to be opened by people you share with Set links to expire after a specific period of time. (access is limited to the intended timeframe)

Achievements

- Only Specific/ Targeted people will have access to the files
- Have control on who, when and from where they are accessing the files

1. Risk Assessment and Prioritisation

We conduct comprehensive risk assessments to identify and prioritise cybersecurity risks based on impact, likelihood, and severity. We utilise the **Defence in Depth** risk management process to evaluate and prioritise risks for targeted mitigation.

2. Security Controls Implementation

Cybersecurity controls are aligned with tactical risk mitigation strategies. We have implemented technical controls, security measures and best practices to address specific cybersecurity risks and vulnerabilities proactively. For example, we do not conduct similar phishing simulations to gauge **User and Entity Behaviour Analytics** (UEBA). Instead, we tweak the phishing simulation content to challenge existing user behaviour and, based on the results, align security controls.

3. Continuous Monitoring and Improvement

We implement continuous monitoring mechanisms to track cybersecurity risks, vulnerabilities and threats in real time. The organisation leverages **Defence in Depth** principles and **CERT-IN** guidelines to refine cybersecurity practices, enhance resilience and adapt to evolving cyberthreats.

4. Actionable Intelligence

Predictive analytics is a powerful tool for identifying potential security threats before they occur. We have upgraded to latest Artificial Intelligence (AI)- and Machine Learning (ML)-based threat analysis for harvesting predictive risk-based data.

Integrating tactical risk management practices within the Apraava Energy Cybersecurity Framework has helped us strengthen cybersecurity defences and mitigate cyberthreats effectively. We are in a position to navigate the complex cybersecurity landscape with agility, resilience and confidence.

To effectively pursue growth in action for Apraava Energy, transforming into a technologically enhanced organisation is imperative. We are firmly on the path to leverage this digital advantage to transition towards becoming a low-carbon business and contribute to a sustainable, happy planet.

