Mercer | mettl

uncompromisable information

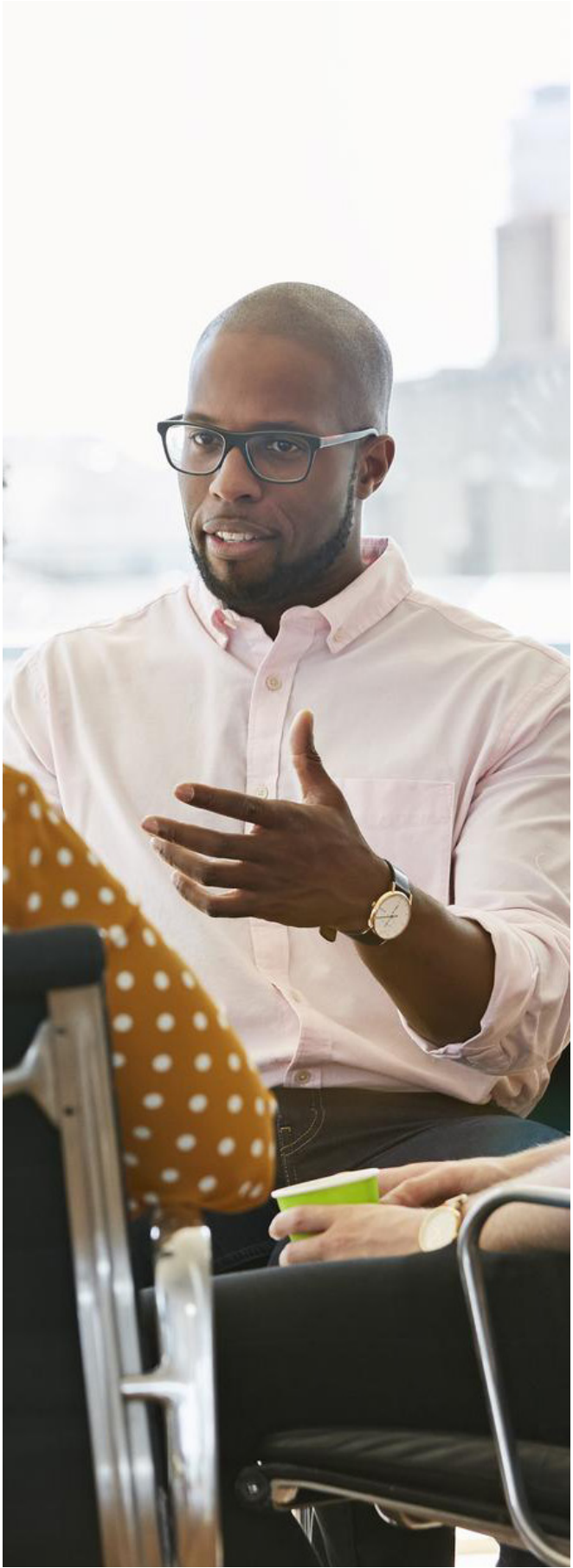
security

welcome to brighter

About the company

The client is a leading player in the global insurance industry with a widespread presence in 50 countries and has a dynamic workforce of 72,000 employees, collectively serving over 65.9 million customers worldwide.

It is one of the world's foremost providers of insurance and asset management services. The company maintains a leading position in Europe and a rapidly growing presence in Asia and Latin America. Eyeing accelerated business growth, the organization offers innovative and personalized solutions through its unmatched distribution network.



Understanding business requirements

The 190-year-old company fosters a learning culture to encourage employee growth and development across geographically dispersed teams. It regards knowledge and skills upgrade as major cornerstones of change and development. It realized that training interventions are the fulcrum on which organizational transformation strategies pivot. This realization gravitated the company toward meticulously defined reskilling programs to gain granular insight into areas where it needed to shore up its employees' skills and competencies.

The company comprehended the need to invest in the employees' near-term and future skills needs, considering the need to build long-term organizational resilience in a continually evolving marketplace. Therefore, it sought a comprehensive reskilling program to provide at least 50% of its employees worldwide with new business, digital and behavioral skills.

The company wanted to assess employee proficiency levels on its specific skills catalog's parameters. Thus, it desired a reliable technology provider to automate and scale the skills assessment process.

However, the company was sensitive to cybersecurity concerns, as it relied on third-party service providers. The reason is that third-party service providers usually perform or support essential operations and are privy to organizational data, be it customer data or access to internal networks.

Due to the nature of the insurance company's business, it needed its partner to maintain the highest levels of information security standards. Thus, it expected its partner to demonstrate an unwavering commitment to information security.

The company needed solutions to meet the following requirements:

1. Enterprise privacy concerns

Data is the most crucial asset for any organization. So, information security was the company's foremost concern, considering the magnitude of the drive, given that large tracts of data was being generated. The company wanted to ensure uncompromising data protection and fail-safe provisions to keep enterprise data safe from theft and leakages before onboarding the right partner.

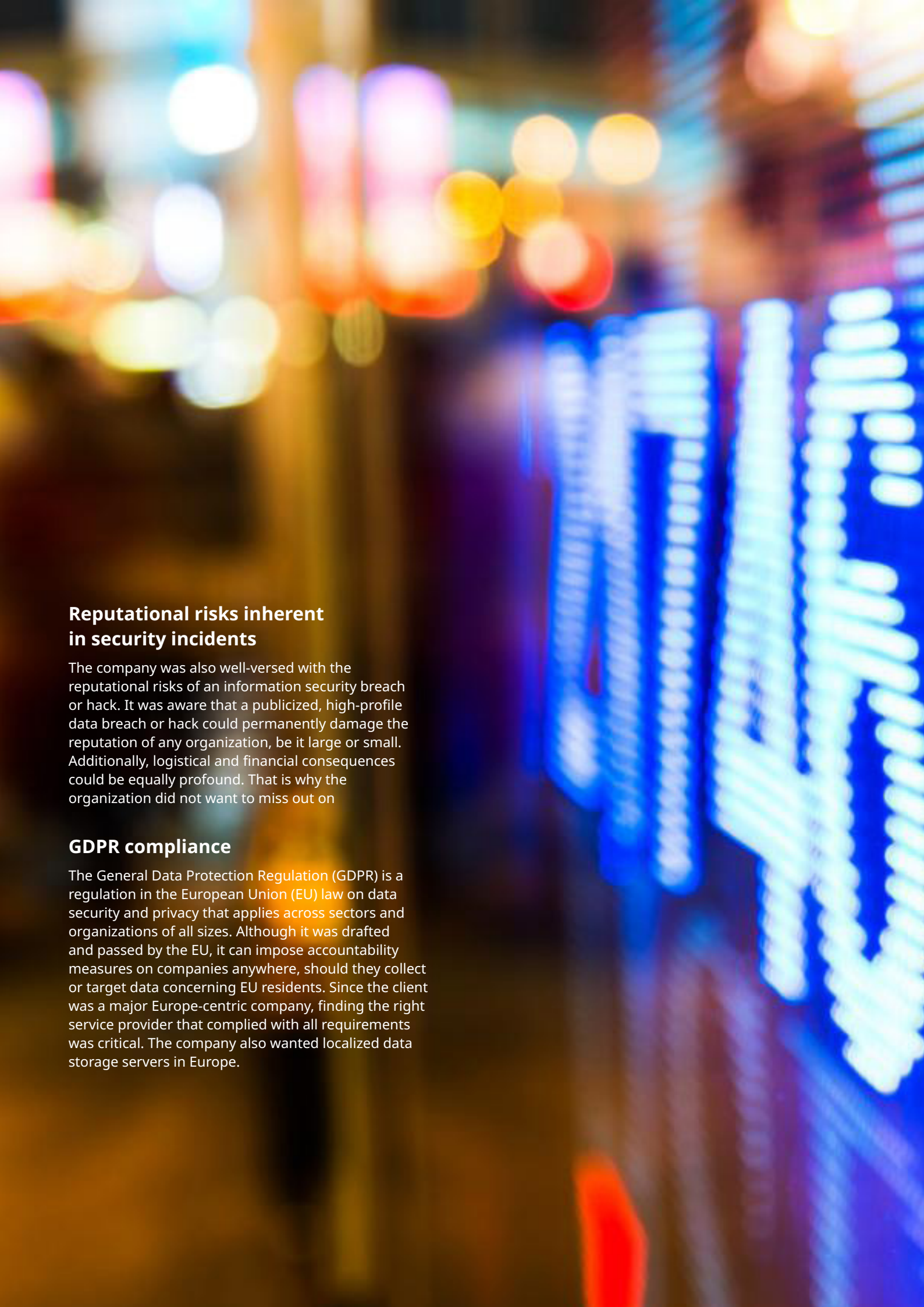
2. Selecting a trusted provider

Due diligence to ascertain that the provider offers adequate security protocols to prevent data breaches is critical before onboarding a technology partner. Effective data security involves safeguarding various datasets and fulfilling regulatory compliance requirements. Thus, the client was also skeptical hat any data breach could seriously dent the corporation’s reputation.

3. Assessing information security preparedness and resilience

The company had defined some critical parameters within which it wanted to assess a service partner's cybersecurity preparedness and resilience. These parameters were:

- The partner needed to ensure that its established security protocols were highly effective, such as System and Organization Controls (SOC) report, the last independent penetration and vulnerability assessment report. Besides, the partner needed to strictly adhere to a regulatory body (I.e., GDPR, ISO/ ICE 27001, etc.)
- The partner needed to provide contracted services even in unforeseen circumstances, such as disaster recovery and business continuity plans.
- The partner needed to demonstrate it possessed a robust incident management program and would rightfully report incidents as mandated by law, regulations and industry practices.



Reputational risks inherent in security incidents

The company was also well-versed with the reputational risks of an information security breach or hack. It was aware that a publicized, high-profile data breach or hack could permanently damage the reputation of any organization, be it large or small. Additionally, logistical and financial consequences could be equally profound. That is why the organization did not want to miss out on

GDPR compliance

The General Data Protection Regulation (GDPR) is a regulation in the European Union (EU) law on data security and privacy that applies across sectors and organizations of all sizes. Although it was drafted and passed by the EU, it can impose accountability measures on companies anywhere, should they collect or target data concerning EU residents. Since the client was a major Europe-centric company, finding the right service provider that complied with all requirements was critical. The company also wanted localized data storage servers in Europe.

Since many software companies claim to be GDPR Compliant, focusing on the three characteristics mentioned below was crucial for selecting the right vendor:

Privacy by design

Article 28 of the GDPR says that companies should undertake due diligence in selecting service providers, employing only those that meet the parameters laid down by the GDPR and safeguard the data subject's rights. A data subject is any person (or entity) whose personal data is collected, controlled or processed by an organization. Personal data is any critical data that can identify an individual, such as name, residential address, card details, etc. A service provider should offer privacy by design comply with the GDPR.

Data control

The GDPR emphasizes the right to be forgotten, which means that individuals should have more control over their data, necessitating organizations to delete the personal data of individuals upon request- or when it is no longer needed. Therefore, a technology partner needed to adhere to these requirements and present a befitting and sustainable plan to control user data.

Stance on data privacy

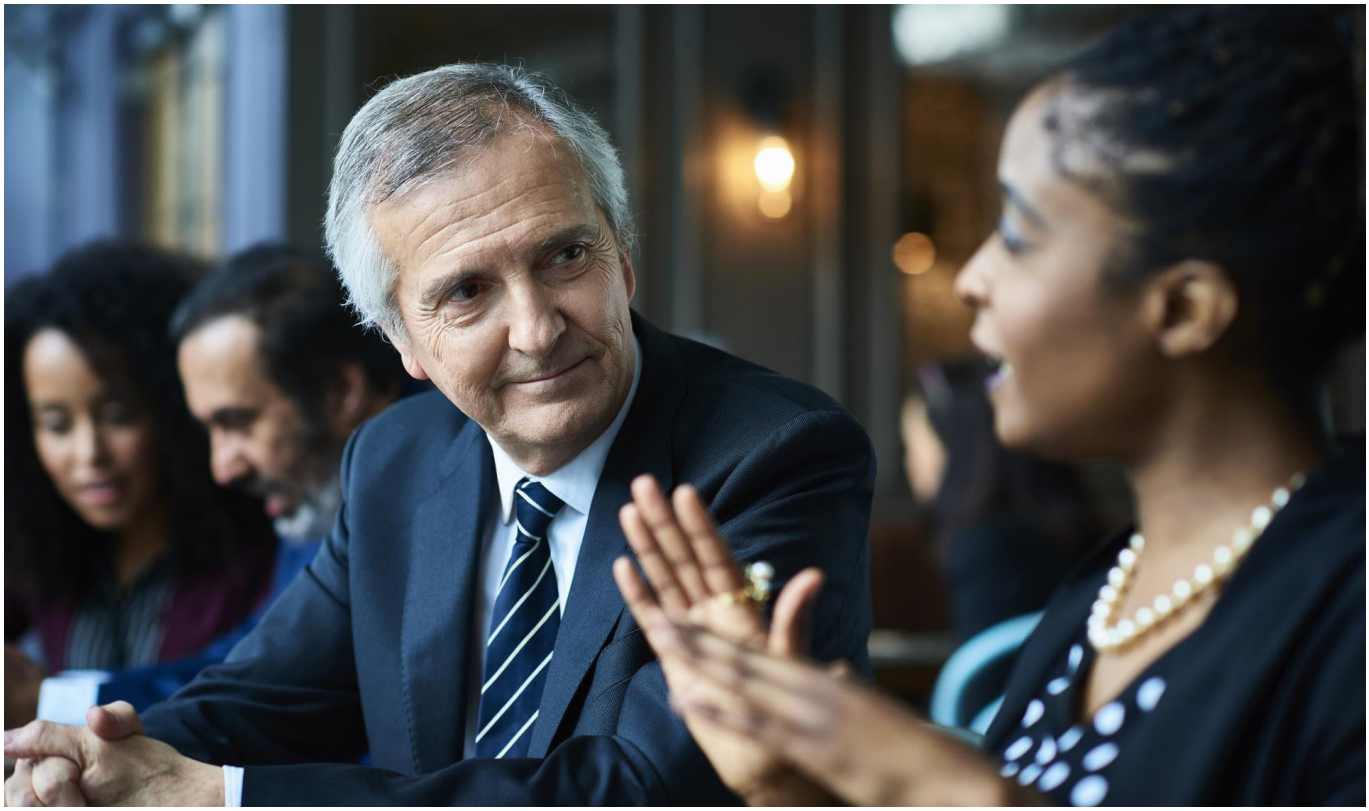
The GDPR is all about protecting individuals' personal data, giving them control over it. Similarly, while selecting a GDPR-compliant service provider, its organizational culture and outlook on data privacy with its stakeholders need to be considered. It is not worth running the risk of onboarding a partner that is not fully committed to ensuring data privacy.

Winning the client’s trust

The company's unparalleled domain expertise and strategically focused innovation approach make it a leader in the insurance industry. Its L&D’s primary focus was on reskilling employees and making them ready for the future of work. Conducting such a task also required that the partnering service provider adopted the latest technology, stringent policies and extensive protocols to ensure information privacy and data security at every stage of the process.

Mercer | Mettl gained detailed insights into the client's reskilling strategy and bottlenecks, and deep-dived into charting out a possible course of action.

Additionally, Mercer| Mettl's leading-edge talent assessment software system and industry-leading data privacy and security provisions instilled a sense of confidence in the client. Moreover, Mercer| Mettl’s customized service offerings resonated with the company.



The solutions

Pleased with the promising potential of Mercer| Mettl's products and info security arrangements, the company decided to leverage them for streamlining its skills assessment process for reskilling drives across various geographies. As a result, the client's collaboration with Mercer | Mettl initiated profound deliberations on understanding the project requirements.

Mercer | Mettl consultants worked closely with the client to integrate the skill mapping framework tailored to the client's needs. It created an advanced analytical dashboard to gain an insight into skills penetration in each geography. The customizable data analytics and reporting dashboard provided readily configurable reports at an individual and group level.

The process of workforce clustering to identify candidates for skill assessment and development followed. Mercer | Mettl's highly advanced platform and scientifically validated assessments were also configured. The team also finalized carefully designed assessments by subject matter experts to gain the best insights into employees' functional knowledge and personality traits.

The HR managers identified crucial parameters to assess employees based on their respective domains. Conducting assessments to evaluate them on the given parameters enabled HR professionals to gain detailed insights on each candidate's top three skills (strengths) and bottom three skills (areas that need improvement). This way, HR leaders localized the training program accordingly in different geographies. Instead of having standardized training programs, they created customized training programs by understanding the core skills that needed training interventions across the business units in diverse locations.

Mercer | Mettl's stringent policies and extensive protocols to ensure information privacy and data security enabled the client to conduct and scale training needs assessments and create a targeted plan for employees without worrying about digital security. Mercer | Mettl, with its deep-rooted commitment towards making training assessments secure, credible and scalable, built a safe ecosystem for the client, ensuring the the candidates' personal data security.

Data security, assessments' credibility and robust processes were the three pillars of Mercer | Mettl's security ecosystem, backed by numerous compliance standards.

Listed below are some of the critical information security features embedded within the Mercer | Mettl ecosystem:

Hosting on AWS

Mercer | Mettl's data is hosted on Amazon Web Services (AWS) - which is one of the most flexible and secure cloud computing environments available on the market. It uses a wide variety of AWS services for data storage and computation.

Data encryption in transit

Data exchanged between a test-taker and Mercer | Mettl over the network is secured and encrypted to safeguard against any breach. All data exchanged over the network between a test-taker and an invigilator is secured and encrypted via HTTPS (256-bit SSL encryption). Besides, a security protocol of TLS1.2 is enabled to support the secure transmission of HTTP calls.

Data encryption at rest

Databases, where personal information, assessment records and other sensitive details of candidates and clients are gathered, are stored in an uncompromisable maximum security environment. Mercer | Mettl is strictly against bartering and selling any information to outside partners, and storing data for personal marketing interests. Moreover, for endpoint access, it offers various authentication combinations to address any vulnerability.

Access right management

Mercer | Mettl platform had set clear guidelines on who can view and access the various system resources, allowing it to track who, when and where accessed the data. It supports creating various roles with defined access rights, log reports and audit trails. In addition, access is allocated with the least privilege rule to avoid any unauthorized data disclosure.

Multi-factor authentication

It ensures only an authorized person is logging into the account, acting as an additional layer of security to the login mechanism. The username and password are prompted for logging in as the primary layer.

Connect with an expert

General Data Protection Regulation (GDPR) Compliance

Mercer | Mettl is GDPR compliant. Its policies and processes adhere to GDPR principles of data minimization, data subject rights and data management (storage and security, retention, breach management). Such policies and procedures are reviewed, at least annually or when a change is required as per the regulation.

Data collection

Mercer | Mettl's clients may require additional information to be collected from assessment takers, and they define what this information could be. There is a provision of configuring and enabling 'explicit consent,' which can be obtained from candidates before administering an assessment. It is to ensure that assessment takers are aware of why such information is being collected.

Moreover, Mercer | Mettl's privacy policy clearly states 'what,' 'why,' and 'how' candidate personal data is processed.

Data subject rights

Mercer | Mettl has implemented processes to acknowledge and respect data subject rights. A data subject can email at '#mettl_privacy_mettl@mercer.com' and request to exercise data subject rights.

Since Mercer | Mettl is a data processor, processing data at the behest of data controllers, the controllers (its clients) determine if the candidate's data subject right request is valid and actionable.

Data management

Mercer | Mettl is a cloud-based SaaS platform hosted on AWS. All the data in transit and at rest is secured using industry-standard mechanisms. Provisions to store data are defined in the contract between the client (the data controller) and Mercer | Mettl (the data processor).

The client can choose to have the data deleted from Mercer | Mettl's cloud-based servers as desired by placing a request to remove all data after the termination or expiry of the contract.

ISO 27001:2013 Compliance

Mettl is compliant with ISO 27001:2013. It possesses all the controls related to secure development, access management, encryption and key management. It also deploys AWS CloudWatch to monitor all the controls and changes across an organization.

In addition, it also has device-and-network-level threat assessment programs, along with web application penetration testing that is compliant with the vulnerability assessment. Mercer | Mettl is assessed by Certifying Body TUV every year as part of the surveillance program.

ISO 9001:2015 Compliance

ISO9001: ISO 9001 is the world's most recognized Quality Management System (QMS) standard. Its primary objective is to meet the needs of its customers and other stakeholders more effectively. Mercer | Mettl has built a framework to ensure consistent quality of goods and services.

It has focused on several quality management principles, including a strong customer focus, standard process approach and continual improvement. Using ISO 9001, Mercer | Mettl ensures that customers get good quality products and services consistently.

Virus safety protocols

Mercer| Mettl has adopted top-notch data security and virus protection standards practiced by Mercer and Marsh McLennan (MMC Group). It runs best-in-class Vulnerability Assessment and Penetration Testing (VAPT) programs. The VAPT program deals with ransomware, botnet and other related threats. In addition, Mercer| Mettl runs the most secure authentication processes on all organizational devices, fortified with stringent data safety and antivirus software.

Penetration testing

Mercer | Mettl conducts penetration testing annually. It also runs device-and-network-level threat assessment programs, along with web application penetration testing.

Vulnerability testing

It conducts vulnerability assessment, assisted by internal experts and external vendors. Third-party network and application vulnerability tests are undertaken annually. Additionally, it runs tools like WhiteHat daily to discover any application vulnerability.

External and internal auditing

Mercer | Mettl takes external and internal auditing seriously. External audits are performed by certifying bodies yearly, in line with ISO 27001:2013. Internal reviews are conducted once every six months.

Localized servers

Most importantly, Mercer | Mettl has localized data storage provision in the following countries:

- Europe
- India
- China

Connect with an expert

Impact

Mercer | Mettl's sophisticated suite of assessment tools and purpose-built end-to-end information security arrangements enabled the leading insurance company to identify skills gaps in its workforce and create individual and organizational development plans without concerns about the security and safety of Mercer| Mettl's data security architecture.

Here are a few highlights:

- Approximately 2500 assessments were conducted across 25 different skills in 14 languages across 40 different business units.

- Being a global conglomerate, the client works across geographies. It signaled its firm stance on data privacy and security standards before partnering with a trusted ally.

  Mercer | Mettl has ticked all the boxes and helped the company conduct over 2500 training assessments thus far.

- Mercer | Mettl's comprehensive and data-driven assessment reports offered actionable insights on areas of development for every employee, complete with a comprehensive list of strong and weak areas.

About us

At Mercer|Mettl, our mission is to enable organizations to make better people decisions across two key areas: acquisition and development. Since our inception in 2010, we have partnered with more than 4,000 corporates, 31 sector skills councils/government departments and 15+ educational institutions across more than 90 countries.

mettlcontact@mercer.com

www.mettl.com

Robust Information Security System

Be sure to carefully read and understand all of the disclaimers, limitations and restrictions before using the assessment services, reports, products, psychometric tools or the company systems or website.

Read the complete disclaimer here:
https://pages.mettl.com/disclaimer

A business of Marsh McLennan