imc
part of Scheer

Technical Setup

Service Description

imc Learning Suite

October 10, 2023

im-c.com

Preface / Objectives

This document describes the services provided by the imc project team as part of the Technical Setup of an implementation project for the Learning Management System (LMS) imc Learning Suite. The Technical Setup includes various technical and organisational services that are necessary for the installation and technical operation of the software - both in the cloud and for on-premises installation.

The technical setup includes (a) a technically functional **installation of the standard product**, (b) the **codeline management and licence management** including the general setup of the language packages, (c) the **technical integration for URL and mail sending**, and (d) the **implementation of the design package**, i.e., the adaptation of the user interface to the CI/CD (corporate design).

For this reason, the service description includes the various work packages considering the following aspects:

- **Description of services to be provided** as part of the technical setup by the imc project team. The document also describes additional options that may be provided as additional services within the scope of the implementation project.
- **Description of competences and responsibilities**, which are partly on the part of imc and partly on the part of the customer.
- **Description of procedure, process, and time dependencies** for the technical setup, so that a transparent view of the individual steps is possible for all those involved.

Installation of Standard Product

This section describes the installation of the standard product of the imc Learning Suite as part of the technical setup. In general, a distinction must be made between the cloud and on-premises operating model when installing the systems.

- In the case of a **cloud operating model**, imc takes care of the installation of the systems (both the productive system and other environments if ordered) and the customer is not involved in this.
- In the **on-premises operating model**, imc conducts the installation of the systems together with the customer. However, this only includes one environment, usually the productive environment. The customer must install further environments unless there is a separate agreement that imc also supports the installation of further environments. In the on-premises operating model, imc provides the customer with the corresponding installation packages. The actual installation is then conducted by imc, whereby the customer should be present during this installation, as the responsibility for the environment is then transferred to the customer. If configuration files (which are required for technical operation) are adapted during the installation, these must be sent to imc so that they are included in future deliveries. The same applies if the customer operates other environments in addition to a productive environment (e.g., test, stage, dev). In this case, imc must also be informed so that future deliveries can take this into account. If further deliveries are made available to the customer during the project, the customer will conduct these updates himself.

In connection with the installation of the LMS in the on-premises operating model, reference is made at this point to the official documents of the software regarding system requirements and installation instructions. The customer is obliged to ensure that the necessary requirements for an on-premises installation are met before an imc technician can conduct the installation.

The installation performed by an imc technician covers the following areas: (i) Java SDK, (ii) Tomcat application server, (iii) imc application files, and (iv) system specific configuration (this includes the connection to the provided SMTP server). If desired, we can also connect the application via ISAPI to an IIS web server to enable Windows SSO. Further connections and configurations, such as the connection to ReverseProxy, WAF or others are not part of our service portfolio.

Note: Each environment (e.g., production, test, or stage) has information stored in the technical operating parameters about which environment it is (**system context**). This allows to distinguish between productive and non-productive environments (e.g., only productive environments send mails, while non-productive environments always send mails in test mode) or to allow environment-specific configurations (e.g., URLs, SSO). While completing the implementation project, we recommend - if more than the productive environment is used - to evaluate the data mirroring from production to the other environments to ensure that the corresponding settings are completely adopted (e.g., the SSO on the test environment).

Independent of the operating model, there is an **imc internal reference system** for each customer, which is used for the preparation of deliveries as well as the adjustment of problems or the implementation of customer-specific adjustments (if possible, in the operating model). Customers do not have access to reference environments.

After receipt of the order and initialisation of the project by the imc project manager, the installation of the systems is planned and conducted on the imc side (in the cloud model) or coordinated with the customer (if on-premises model). The imc project manager involves the imc technical department and coordinates the provision of the packages required for the initial installation.

The availability of the system or the installation packages usually requires a lead time of about two weeks.

Note: In cloud operation, the project team has access to the environments. For on-premises installations, access to the web application for the imc project team (and later for imc support) must be clarified at an early stage.

Codeline Management & License-Management

imc manages the current delivery status of the software for each customer. For this purpose, the customer systems are stored and managed in the imc **codeline management system**. In general, there are three distinct types of codelines:

- Dedicated codeline (cloud operating model)
- Dedicated codeline (on-premises operating model)
- Cloud codeline (non-dedicated codeline)

A dedicated codeline (cloud or on-premises) allows to implement customisations for customers, if it includes a code area that allows customisations to the source code. In the cloud codeline, there is no possibility to implement customer-specific adaptations to the existing source code.
The type of codeline is already determined when the order is placed, so that the imc project team forwards the necessary information to the relevant department as part of the technical setup.

Note: If a dedicated codeline is used, the imc project team will regularly update the codeline with patches and innovation packages as part of the project. The timely and regular updating of the environment with current software versions of the LMS is also necessary and is the responsibility of either the project team (cloud operation) or the customer / customer IT (on-premises operation). In the case of the cloud codeline, the software updates take place automatically so that the environments are always up to date with the latest software.

Within the scope of **licence management**, the imc project team licenses all ordered modules and language packages. The imc project team takes care of applying for the necessary licences and configuring the language packages.

The licence and language packages are usually already clear from the order, so that the imc project team configures them after successful installation of the system. The most important aspects here are the number of users, the platform languages used and the additional modules that need to be explicitly licensed.

If several environments are available to the customer, only one licence is used. The activated licence is part of the database and is automatically transferred from production to lower systems during data mirroring. However, the licence can also be installed manually on each environment.

Technical Integrations

As part of the technical setup, the URL (including secure access) and the mail sending are also set up.

Coordination URL and SSL Certificate

The aim of the technical coordination is to ensure that the LMS is accessible under the desired URL and secured by an SSL certificate. Until the changeover to the customer's URL, the LMS is accessible in cloud operation under a temporary URL of imc.

The imc Learning Suite is a web-based application that is opened via a browser (e.g., Google Chrome, Firefox, Edge). For the LMS to be accessible under the URL requested by the customer, imc requires certain information. For productive use of the Learning Suite, the application should run on a domain (Internet address) registered by the customer and an SSL certificate suitable for this domain. The addressing of the website is then completed accordingly via a URL defined by the customer.

Note: It is also possible to map the operation of the LMS in the cloud completely via an imc URL. For this purpose, imc offers sub-domains (depending on the cloud operating model).

Important note: In the case of several systems (productive environment, test environment), all URLs and the respective SSL certificates are required (at best, this information is already available at the start of the project). **The responsibility here lies with the customer to initiate the necessary steps and to provide the information and files to imc**. The imc project team can provide support in an advisory capacity or actively by creating a certificate request (CSR) to simplify the application for an SSL certificate by the customer.

In cloud operation, the imc project manager forwards the URL and the SSL certificate to imc Hosting after receiving them. After all preparations have been completed by imc Hosting, the final change of the URL can be conducted.

The aim of the URL change is that the Internet address (domain) registered by the customer refers to the LMS server so that a user can access the LMS when calling up the URL. For this purpose, the customer must set up a forwarding (DNS entry). The recommendation of imc is to set a CNAME entry here, although an A record is also possible as an alternative. Depending on the customer's decision, the imc project team will provide the customer with the required information for the DNS entry (URL imc traffic manager or IP address). As soon as the customer has set the DNS entry, imc Hosting can conduct the final change to the imc side and the imc project team informs the customer as soon as the system is accessible under the desired URL.

Additional more detailed information on this topic is explained below:

An SSL certificate serves as a binding proof of identity - furthermore, the certificate contains information with which the browser and server can establish encryption. This means that

communication from the computer, smartphone, or tablet to the website (the LMS) is secured and encrypted.

For productive use of the LMS, the application must run on a domain registered by the customer and a suitable SSL certificate for this domain. This applies to all operating models (cloud and on-premises). In principle, an own domain or a sub-domain (e.g. https://lms.customer.com or https://academy.customer.com) of an existing domain can be used. The use of a context path (e.g. https://customer.com/academy or https://customer.com/lms) of an existing domain is not possible.

The use of a subdomain is recommended by imc. A major advantage of using a subdomain is that it is often easier for the customer's IT department to obtain a certificate for the subdomain, as registration for the main domain has already taken place. If no subdomain is to be used for the LMS, it is also possible to register a new domain. In this case, the customer must do this himself - imc will not acquire any domains.

If the LMS is operated in the cloud by imc, the SSL certificate for a domain or sub-domain is provided to imc in the following way:

- Either as one file in .pfx format (certificates including private key) + password.
- Or as individual files:
    - Certificate in .crt, .cer, .cert, .pem format
    - Private key in .key format + password
    - Intermediate certificates

It is important that the **intermediate certificates (intermediates)** are supplied. Although the secure connection to the website can be established, the certificate is not classified as trustworthy in all web browsers.

Note: For security reasons it is important that the SSL certificate and the corresponding private key are provided separately to the imc. It is recommended to use separate communication channels.

If support is required for the creation of a so-called certificate request (CSR), the imc project team can help. A CSR is a file that contains all necessary data and de-tails (contact data & public key). For imc to create a CSR, the following information is required:

- **Common name**: e.g., lms.customer.com
- **Organisation**: e.g., Customer Name
- **Organisational Unit**: e.g., IT
- **City/ Locality**: e.g., Munich
- **State/ Province**: e.g., Bavaria
- **Country**: e.g., Germany

Using the data provided by the customer, the imc creates a CSR and then makes it available. This CSR can then be registered with a certification authority (CA) to request an SSL certificate.

Note: SSL certificates have a limited validity period and must be updated regularly. Should the SSL certificate expire, the use of the LMS may be severely restricted for users. In the operation of the LMS, imc Support will usually inform about the imminent expiry of a certificate. However,

the responsibility for providing an updated certificate lies on the customer side. Therefore, the customer should keep an eye on the renewal of certificates.

Important note: In the on-premises operating model, the customer's IT is responsible for providing and updating a valid SSL certificate. Here, imc cannot provide support for the creation of the certificate. The SSL certificate must be provided at the time of the initial installation, otherwise technical problems and additional work may occur during the project.

As soon as imc has received the relevant files of the SSL certificate, the domain can be changed. The aim of the change is that the Internet address (domain) refers to the LMS server so that a user can access the LMS when calling up the URL. For this purpose, a forwarding (DNS entry) must be set up by the customer.

In the case of the on-premises operating model, the complete setup is the responsibility of the customer's IT, which is responsible for the operation of the LMS. In the case of cloud operation, there are two options:

- **Option 1: CNAME (recommended by imc)**: A CNAME is a hostname-to-hostname reference. In contrast to the second variant, this type of forwarding is more flexible. In addition, it is guaranteed that dynamic IP addresses can also be addressed as a destination. For this, the following must be set up:

  Set up a DNS entry (CNAME) on the traffic manager of the LMS.

- **Option 2: A RECORD (not recommended by imc)**: Here a fixed forwarding to the IP address of your LMS server is set up. It may happen that this changes. In such cases, the customer's IT would have to adjust the DNS entry to the new IP address and there may be restrictions on access that are outside the responsibility of imc. The following must be set up for this purpose:

  Set up a DNS entry (A Record) on the IP address of the LMS server.

Note: The customer will be informed of the details of the traffic manager or the IP address of the LMS server in cloud operation during the technical setup.

As soon as the forwarding (DNS entry) has been set up, the last step is taken by imc Hosting and the imc project team informs the customer as soon as the LMS can be reached via the desired Internet address (URL).

Important note: We advise against using the DNS entry with an external WAF or similar, as this can lead to support cases and unforeseeable problems. The analysis effort for such support cases where the DNS entry was not set as recommended in variant 1 will be charged separately by imc.

Supplementary note: In the standard case (unless otherwise ordered), the Technical Setup assumes that the LMS should be available under a single URL. In principle, it is possible to make the LMS available under several URLs (clients with their own URL). The use of several URLs can make sense, for example, in a scenario with different target groups. If this is the subject of the order and the desired scenario, this can be coordinated accordingly by the imc project team.

Coordination Mail Sending

As part of setting up the mailing functionality of the LMS, it is ensured that the LMS correctly sends any emails (system emails, booking emails, notifications) with the sender address defined by the client (e.g. lms@customer.com).

Important note: In the on-premises operating model, the customer's IT is responsible for providing its own mail server for which the LMS has permission to send mails. The mail server is already connected as part of the initial installation of the standard software. Technical problems are to be analysed by the customer's IT.

In cloud operation, there are three options for configuring the mail dispatch of the LMS.

- **Variant 1(sending via imc mail server; recommended):** The mail sending of the LMS takes place via a sender address of the customer (e.g. lms@customer.com or academy@customer.com). For this, an SPF record for the customer.com mail server must be set by the customer's IT department, otherwise there is a risk that mails will be identified as spam. An exceptional case for which no SPF record is required is when the customer.com mail server only sends mails to its own users and mail sending is explicitly permitted for the LMS server.

Note: In addition to an SPF record, mail can be sent with a signature. DKIM signing is supported by imc and can be implemented as part of an additional order. In this case, imc creates the corresponding key pairs and makes them available to the customer's IT department for storage in the customer.com DNS entry.

- **Variant B (direct sending via customer mail server):** If it is not possible to set a SPF record or if there is an explicit wish not to send via the imc mail server, the customer's mail server can also be connected directly to the LMS. The mails are still sent via a sender address of the customer (e.g., lms@customer.com or academy@customer.com). The direct connection of the LMS to the customer's mail server does not require a separate order within the scope of the technical setup, but it does mean that imc has significantly fewer options for analysing mail problems.
  The following three current restrictions must be observed: (i) the mail server must be directly accessible (a VPN connection is not possible), (ii) authentication is via SMTP-Auth, i.e., imc requires a user's login data for setup, and currently only TLS 1.2 is currently supported, and (iii) the further security settings (security policies) of the customer's mail server are the responsibility of the customer (the IP address of the LMS server may have to be released or there are restrictions on forwarding to the actual recipients).

Note: In this variant, from the point of view of the LMS, the mail sending is completed whenever the LMS has transferred the mail to the customer's mail server, i.e., the mail sending is marked as successful or logged in the LMS. All further analyses and examinations in case the mail does not reach the recipient are the responsibility of the person in charge of the customer's mail server and therefore outside the responsibility of imc.

- **Variant C (sending via imc sender address):** In exceptional cases, imc also offers to send mails via an imc sender address (e.g. customer@lms-saas.com or cus-tomer@imc-learning.com). The relevant security settings are made on the imc side to ensure successful

sending. However, it should be noted that the customer does not have access to the corresponding mailbox should users reply to the sent mails. And a recipient address is still required on the part of the customer for the receipt of system-side mails.

The imc project manager clarifies the relevant issues directly at the beginning of the implementation project. Especially for the first variant, the setting of an SPF record is important and the imc project manager will provide all relevant information on this, e.g.:

- *The Sender Policy Framework (SPF) is an open standard that specifies a technical procedure to prevent the forgery of sender addresses. More specifically, the current version of SPF - called SPFv1 or SPF Classic - protects the sender address of the envelope used to deliver messages.*
- *SPFv1 allows the owner of a domain to set their policies for sending mail, such as which mail servers they use to send mail from their domain. This technology requires two sides to work together: (1) the owner of the domain publishes this information in an SPF record in the domain's DNS zone, and when another mail server receives a message claiming to come from that domain, then (2) the receiving server can verify that the message matches the domain's stated policy. For example, if the message comes from an unknown server, it may be considered a forgery.*

This SPF record may look like the following (more detailed information is always provided by the imc project manager):

domain.com IN TXT "v=spf1 a mx include:spf.imc-hosting.com -all"

Important note: Setting this SPF record is the responsibility of the customer. As soon as the entry has been set on the customer side, the customer informs the imc project manager. The entry is then checked by the imc hosting site and the setup is completed. A later removal of the SPF record can result in mails no longer reaching the users.

Supplementary note: In the standard case, the technical setup assumes that the LMS sends mails under a single sender address. The LMS also allows the use of several sender addresses (e.g., different sender addresses per organiser/client). This can make sense in a scenario with internal and external users, for example, where the LMS is also available under several URLs and different names are used for both target groups. In this case, effects must be carefully considered, and all the above facilities must be ensured per sender address.

Design Implementation

As part of the technical setup, the **LMS design is also adapted to the client's corporate design** to ensure that the LMS is visually aligned with the client's CI / CD (e.g., logos, colours, font). It is important to mention that at this point a distinction must be made between design and configuration. Among other things, displayed contents (e.g., navigation entries in the main navigation or in the footer), the showing / hiding of buttons and settings (e.g., catalogue filters or texts / arrangements on description pages) or the system wordings are not part of the design and can be adapted within the framework of the implementation project.

Unless otherwise ordered, the creation of one customer-specific design is conducted by imc, which can be assigned to the clients of the system. Additional designs can be ordered separately. The design is always implemented for browser access to the LMS and for the two standard mobile apps (iOS, Android).

Supplementary note: The LMS allows the use of a separate design per client and additional designs can be implemented as part of a separate order.

For an optimal process of customisation by the imc design team, the customer provides the imc project manager with a description of the desired design. This usually includes CI / CD guidelines or a link to the company website. If a non-licence-free font is required, the corresponding web font files must also be provided to imc - imc does not assume the acquisition of such files. If there are different basic colours in the CI / CD of the customer, a note with the preferred basic colour is necessary.

Once all the information has been collected, the imc project manager will hand over the order to the imc design team. **As a rule, the design is then created within two weeks and imported into the project system. After the design has been imported, the customer has the task/responsibility of checking the design and providing imc with collected, comprehensible feedback.** After clarification of the feedback and the possibilities between the customer and the project manager, a revision round can be scheduled if necessary.

If there is a particular need on the part of the customer to examine the options and possibilities more closely, imc offers a so-called **user experience design workshop** with a front-end designer. This workshop usually lasts half a day and requires - unless otherwise agreed - a separate order.