EHS Software – What to Look for in MOC Software

The following is a set of common requirements relating to the procurement of Management of Change (MOC) software, compiled from multiple requests for proposal (RFP) by current and prospective clients of Frontline Data Solutions. These clients operate in a variety of industries, including Chemicals, Oil & Gas, Manufacturing, Engineering, and Transportation.

System Functionality

Initiating MOCs

1. Low-level users can request MOCs via custom shortcuts.
2. MOC requests from low-level user are automatically routed to specific higher-level users for review based on the type of request.
3. Higher-level users can request MOCs through an alternative workflow that does not entail the same pre-approval review required of low-level users.
4. Corrective action items relating to an incident or near-miss can require the initiation or completion of an MOC.

MOC Workflow

5. Custom set of tasks and forms can be assigned before approval is considered.
6. Discussion and feedback regarding the MOC can be required of participants and is automatically saved as part of the MOC record.
7. One or multiple users can be assigned to approve the MOC, in any combination of sequential and parallel tasks.
8. After approval, a custom set of tasks and forms can be assigned to any number of users as part of implementation.
9. Tasks can be assigned to specific users or to generic job titles containing multiple users.
10. Tasks assigned to job titles can be completed by anyone with that job title. The system tracks which specific user completed the task.
11. Users can be assigned multiple job titles.
12. Additional users can be assigned to verify that each task was completed correctly.
13. Users are notified by email of any new or overdue tasks.

14. System tracks temporary, permanent, and emergency MOCs, with unique notification and task requirements for each.

15. Attachments can be associated with the MOC in general and with specific tasks within the MOC.

16. Equipment and other assets can be associated with MOCs.

System Configuration

17. MOCs can be categorized using custom codes and tags defined by the user.

18. Designated users can create and modify custom workflow templates without the vendor's involvement.

19. An unlimited number of custom workflow templates can be created and saved by designated users.

20. Custom workflow templates can specify the users involved, the order of tasks, due date, and any forms that must be completed.

21. Individual tasks in the custom workflow can be designated as Mandatory, and must be completed, and other tasks can be modified by the MOC lead on a case-by-case basis.

22. Pre-defined workflows can be selected manually by the MOC lead or automatically based on responses to custom forms.

23. Workflows can contain any combination of simultaneous and sequential tasks in each stage (approval, implementation, etc.).

24. Action items can be added to MOCs and assigned to specific users or to generic job titles.

25. Action items can be triggered automatically based on responses to custom forms.

26. Users can create an unlimited number of custom forms without the vendor's involvement using a drag-and-drop editing tool built into the application.

27. Custom forms allow for the following field types:

    a. Dates

    b. Text boxes

    c. Check boxes

    d. Radio buttons

    e. Drop-down menus

f. Decision trees

28. Implementation tasks can be set to Critical or Non-Critical. The workflow will automatically progress to the next Critical item as long as all preceding Critical tasks are complete, even if some Non-Critical tasks are not yet complete.

29. Startup can be initiated after all Critical items are complete, even if some Non-Critical tasks are not yet complete.

User Management

30. Clients can add new users to the application without the vendor's involvement.

31. Existing users can be deactivated by the client without the vendor's involvement. Records relating to deactivated users are stored indefinitely.

32. Tasks associated with any users can be reassigned on a temporary or permanent basis to other users.

33. Clients can control user permission settings for individual users to control what MOCs they can see or edit (only ones they are responsible for, any MOCs in the division, any MOCs in the company, etc.), what reports they can run, and what settings they can alter.

Archiving & Reports

Archives

34. Unlimited storage is available for all completed, cancelled and in progress MOC information.

35. Completed and cancelled MOC information is archived and locked for editing.

36. Completed and cancelled MOCs can be copied and used as the template for new MOCs.

37. All data is owned by the client and can be returned by the vendor within 30 days of cancellation.

Reports

38. Users can create and modify an unlimited number of reports, customized to show any information captured by the MOC system.

39. Reports can contain information entered into custom, user-created form fields.

40. Report types are available for the following MOC-related topics:

    a. MOC overview

b. Approvals

c. Implementation requirements

d. Discussion details

e. Action items

f. Email notifications

g. User desktop information

41. Report types are available for the following system administration-related topics:

    a. Reassignment of user tasks

    b. Equipment

    c. User permission settings

    d. User supervisor settings

42. All reports can be exported to a spreadsheet.

43. Reports can be set to filter for specific data along multiple criteria.

44. Date filters can be set based on specific date ranges or using relative dates (e.g., “Last Month”, “Yesterday”, etc.) to allow reports to run repeatedly without changing settings.

45. Reports can be saved and emailed automatically on a recurring schedule.

46. Users can create private reports visible only to them or view/publish public reports available to other users.

47. Shared reports display different information to different users, based on their individual permission settings.

Implementation

Training & Support

48. Vendor in-person or remote training (via video conference) for client administrators and other heavy users.

49. Practice site is created and available to attendees during the training session and for at least four weeks after the initial training.

50. Vendor provides post-training assistance to client administrators and other heavy users for configuration of the system.

51. Technical support over phone and email is provided by employees of the vendor physically located at the vendor's head office, and not outsourced to a third-party or personnel based in secondary locations.

Data Migration & Integration

52. Existing MOC records in an electronic format (Access database, Excel spreadsheets, etc.) can be imported by the vendor upon request into the application.

53. Custom integration with other software applications can be established by the vendor with the following systems:

    a. Single sign-on (SSO)

    b. Human resource information systems (HRIS)

    c. Document management systems

    d. Asset management systems

    e. Process Hazard Analysis (PHA) applications

    f. Enterprise resource management systems

54. Application is part of a broader platform that includes other EHS functions including:

    a. Incidents and near-misses

    b. Behavioral observations

    c. Audits

    d. Action items

    e. Computer-based training

f. Classroom training.

Information Technology

Hosting

55. Application is hosted remotely. Vendor is responsible for all maintenance, updates, and hardware and software infrastructure.

56. Alternatively, the application can be hosted on a local intranet maintained by the client, with updates provided by the vendor via periodic scheduled remote access.

57. Application is compatible with any internet-connected device running Internet Explorer (10+), Chrome, Firefox, Safari, or Edge.

Data Backup & Continuity

58. Client applications are hosted redundantly in at least two different locations.

59. Client data is backed up continuously and on a periodic (daily) basis.

60. Application has a historical average uptime of at least 99.9%.

Security

61. Client data is encrypted while at rest and during transmission.

62. Client data is stored in data centers with 24x7x365 onsite security, CCTV surveillance, biometric access control, mantraps, and redundant power and cooling.

63. Attachments can be uploaded to the vendor's servers or saved in the application as links to files stored on the client's local network.

64. Access to the application can be restricted to specific IP addresses associated with authorized facilities.

65. Two-factor authentication can be required when users log in.