

Two-Stage Automated Public Tender no. 31/23

For the provision of a system for the management of Internal Audit and Risk Management

Part IV – Definition of the Services (the Specification)

This translation is provided for readers' convenience. Only the Hebrew version is binding.

1. General definitions

- 1.1 **“Sabbaths and Jewish holidays”** – Sabbaths, the Jewish New Year, Yom Kippur, the first day of Succot, Simhat Torah, the first and seventh days of Passover and Shavuot – from two hours before the entrance of the Sabbath/the holiday until two hours after the end of the Sabbath/holiday.
- 1.2 **“Regular working hours”** – Sunday thru Thursday from 8:00 to 17:00, apart from Sabbaths and Jewish holidays, Sabbath eve and the eve of Jewish holidays.
- 1.3 **“Outside of regular working hours”** – Working hours outside of normal working hours, including working hours on Sabbaths and Jewish holidays during which the Bank will pay 150 percent of the price of normal working hours.
- 1.4 **“Installation”** – Installation of the products on the Bank's servers or network, according to the circumstances. The installation will include, among other things: media for installation, media cleansing, updates and a patch for the installations, user accounts and authorizations on the server, documentation, initial instruction and a user guide.
- 1.5 **“Implementation”**:
 - 1.5.1 Preparation of a project file including documentation of the configuration that will be installed at the Bank.
 - 1.5.2 Configuration of all components of the product (hardware and software) according to the Bank's requirements.
 - 1.5.3 Initial instruction for the Bank's technical staff.
 - 1.5.4 Accepted modifications as requested by the Bank.
- 1.6 **“Breakdown”** – An event that adversely affects a central/important part of the proposed system's functionality or that of the Bank's systems, according to the sole discretion of the Bank.

2. Description of the services

The Internal Audit Department and the Risk Management Unit of the Bank of Israel are interested in acquiring a system for the management of Internal Audit and risk management processes at the Bank of Israel (**“the Bank”**), and which will allow for expansion, if the Bank of Israel so desires, to the domains of SOX, compliance and others. The system will make it possible to manage Internal Audit processes and Risk Management processes, from end to end.

The Bank of Israel has about 950 employees. The Internal Audit Department has about 10 employees and the Risk Management Unit has about three employees. The employees in the Internal Audit Department and the Risk Management Unit will be defined as **“key”** users of the

system (“heavy” users) while the rest of the Bank’s employees (about 950 in number) will be defined as “light” users in the system. For the latter, about 500 floating licenses are needed (licenses that are not allocated by name and allow for simultaneous entry into the system).

Currently, the information and data for internal audit and risk management activity are managed by means of Excel spreadsheets and a system for storage of documents (of various types), apart from the implementation of recommendations follow-up which is managed in the MSP system.

The public complaints (ombudsman role) system in Internal Audit is managed in the SharePoint system.

All of the data found in the existing systems will need to be converted to the system proposed in this tender.

3. General requirements of the system

The processes carried out in the system: The Bank is seeking to acquire and implement a system for the management of internal audit and for risk management in order to facilitate and support all of the following processes:

- 3.1 Writing in both Hebrew and English, at least.
- 3.2 The system will also support Hebrew and it will make input and output data available both in Hebrew and in English, including: reports sent from/to the system, report formats, screens, field descriptions, help screens, system documents, emails, etc.
- 3.3 All of the instruction/help for users materials will be available in Hebrew and English in the version of the system proposed in the tender and in any future update of the version to be installed.
- 3.4 The system will support at least the following internal audit processes:
 - 3.4.1 The management of risk-based multiyear workplans and annual workplans;
 - 3.4.2 The opening of tasks within the workplans;
 - 3.4.3 Support of the pre-survey process and the formulation of audit plans, support of audit processes (working papers) and the traffic of messages and documents between the auditors and the auditees;
 - 3.4.4 Support for processes to request and receive material from the auditees;
 - 3.4.5 Support for formulating draft reports, support for processes to receive responses from the auditees and various discussions;
 - 3.4.6 Support for approval processes at each of the stages by staff members to be defined and support for the management of authorizations for this purpose;
 - 3.4.7 Support for the management of draft reports and final reports;
 - 3.4.8 Organizing findings, recommendations and other data in the form of a report for the purpose of follow-up execution, including rating of degree of importance for each item in the report;
 - 3.4.9 Management of a form to monitor the handling and processing of a task, including the determination and monitoring of timetables;
 - 3.4.10 Support for documentation and filing of the relevant documents;

- 3.4.11 Follow-up of the implementation of recommendations in the audit reports and other reports (the State Comptroller, an external accountant, etc.);
- 3.4.12 Support for writing an audit follow-up report, including the automated transfer of data (including findings and recommendations) from the original report to the follow-up audit report for the purposes of following up the execution of recommendations;
- 3.4.13 Support for management, supervision, monitoring and internal control abilities with regard to tasks that are being executed; each manager/employee for the activity under his responsibility;
- 3.4.14 Support for documentation of discussions, including those in the Audit Committee and in the Supervisory Council, according to task, plan or document;
- 3.4.15 Support for processes to produce semiannual and annual final activity reports;
- 3.4.16 Support for reporting processes and ad hoc tasks;
- 3.4.17 The system will support, to whatever extent possible, processes to manage the following public enquiries (ombudsman role):
 - 3.4.17.1 A structured enquiry form in the system for files that are under the responsibility of Internal Audit and the Ombudsman role.
 - 3.4.17.2 A structured enquiry form in the system for monitored files.
 - 3.4.17.3 A structured enquiry form for files opened as a result of public enquiries/complaints and that are not under the responsibility of Internal Audit.
 - 3.4.17.4 Support for documentation and filing of relevant documents.
- 3.5 The system will support at least the following processes for risk management:
 - 3.5.1 The management of multiyear workplans and annual workplans;
 - 3.5.2 Opening of tasks within the workplans;
 - 3.5.3 Support for the pre-survey process and documentation of working papers;
 - 3.5.4 Support for the documentation and management of the process life cycle, risk registry, means of internal control and failure events, creation of a new object, change in status, changes in ranking and comparison to previous periods;
 - 3.5.5 Processes for risk appetite according to accepted methodologies;
 - 3.5.6 KRI management.
- 3.6 The system will support processes to monitor the implementation of recommendations: creation, ranking, change in status and life cycle management.
- 3.7 The system will include dashboard screens for all of the relevant office holders, which will present graphs, heat maps, summary information and information that needs to be supplemented in the system, alongside reports on outliers and the ability for data drill down.
- 3.8 The system will facilitate changing users in the process and will also support the chain of signatures among the relevant office holders, in order to change the status of selected objects in the system.

- 3.9 The system will facilitate identification against the Bank's existing AD and will provide authorizations according to the existing AD group in the Bank. The system will be linked with the Bank's identity management system.
- 3.10 The system will facilitate an ability to define classified tasks / documents / information that are to be exposed only to defined office holders, according to the type of object and the object's life cycle.
- 3.11 The system will enable users to concentrate audit tasks and to document them according to accepted IIA standards on the basis of a work framework, on the basis of COSO, or some equivalent.
- 3.12 The system will support the application of international audit standards that will be determined by the IIA from time to time. The system will provide operational tools for the management and monitoring of task status.
- 3.13 The system will, to whatever extent possible, support compliance management processes.
- 3.14 The system will, to whatever extent possible, support Israeli SOX processes, including the description of processes, process management, control matrices, status execution and documentation, walkthrough, report production, etc.
- 3.15 The system and the activity with the bidder will meet the requirements specified in Regulation 15 of the Privacy Protection Regulations (Information Security), 5777-2017.

4. Technological requirements of the system:

4.1 Mandatory characteristics

A **mandatory characteristic** – A characteristics that exists in the system being proposed to the Bank at the time of the submission of the bid, in the version being proposed to the Bank, as standard functionality:

#	Type of characteristic	Description of characteristic
1	Information security	The system supports Single Sign On (SSO) based on Kerberos.
2	Information security	The system has initial access control and management of authorizations in an application according to LDAP or AD groups.
3	Information security	The system supports SSL browsing from the users to the application.
4	Information security	The system has the ability to harden the application server.
5	Technological	The system supports on-premises installation at the Bank, and the information will be stored on the Bank's servers.

4.2 Requested characteristics

A requested characteristic – A characteristic that is requested for the system being proposed to the Bank at the time of going live but is not necessarily required when submitting the bid and

can be developed up until the date for going live at the expense of the bidder. The bidder must specify in his bid if the characteristic exists in the system or that it can be developed and the expected time for development. The date for actual development will be coordinated with the Bank:

#	Type of characteristic	Description of the characteristic
1	Technological	The system will be required to distribute a complete Hebrew system (within and GUI). The system will support writing in Hebrew (from right to left) and right alignment; the titles will be completely automated in Hebrew and with right alignment, including the user interface, which includes reports.
2	Technological	The system will interface with the Active Directory in order to define and manage authorizations and users and will support the management of authorizations according to functions and populations defined by the Bank.
3	Technological	The system will enable the generation of user-friendly reports for all system users, which will facilitates dynamic definition of reports, forms and queries and their storage for repeat generation, including drill down reports. All of the data will be exportable to Excel and to other familiar formats, including the ability to analyze data by means of analytical tools such as Tableau. If requested by the Bank of Israel, the winning company will provide the data model specified for the Bank of Israel and will assist the Bank in understanding the data model.
4	Technological	The operation of the system by the end users will be by means of a browser and will not require the installation of Client.
5	Technological	The system will facilitate the definition of alerts (reminders and warnings) by end users and the sending of notifications by means of the organization's email server, without the need for intervention by a programmer.
6	Technological	The system will enable the definition of automatic rules that will make it possible to allocate a task or announcement by means of the organization's email, when the precondition for the rule is met.
7	Technological	The system will be based on the Oracle or SQL Server database.
8	Technological	The database to be created as part of the project will be accessible for maintenance to the DBA staff.
9	Technological	Hebrew support in the database: the code required in the Oracle database is the IW8ISO8859P8 Character Set. In SQL Server, it is Collation+Hebrew_CI_AS.
10	Technological	The batch processes at the Bank of Israel are run by way of Control M. The bidder will ensure the running of the batch processes in a form that allows for their definition in Control M without the need to define a password when connecting to the database.
11	Technological	The system will have a mechanism that enables the transfer of data from the production environment to the test environment in order to check for problems in the system during a time that does not exceed two hours.

12	Technological	The system has an audit mechanism that facilitates historical monitoring of the end user's activity in the system
13	Technological	The system has an ability to manage historical data with defined ranges according to the Bank of Israel's request.
14	Technological	The system should include a central log for the monitoring of activity and failures in the system.
15	Technological	The user environment will include full support for Windows 10 and higher and Office 2016.
16	Technological	The solution is compatible with touch screens.
17	Technological	The solution can be defined by users without an IT background (without coding or scripts) and without any involvement of the supplier.
18	Technological	The solution should have an administrator who can approve changes in the configuration of the system without that user having access to the Audit data.
19	Technological	Support for the Chrome or Edge browser (from the five most recent versions or higher).
20	Technological	The supplier will define two environments (test and production) for the Bank, which will be used during the project and after going live during the course of the entire contractual relationship.
21	Technological	It will be possible to maintain the system independently over time without being dependent on the system's supplier, in activities such as defining new WFs, changing existing WFs, defining fields, forms, etc.
22	Technological	The specific modifications developed for the Bank will allow for future upgrades or revisions and installation of new versions of the system by the Company without additional development.
23	Technological	The system includes open interfaces for other software which enable built-in integration, such as an interface to SAP – to BI tools including the BI existing at the Bank – Tableau 21.04.
24	Technological	The system will be based on an off-the-shelf product. The supplier will be required to convert the data from the existing system into the new system.
25	Technological	Instead of installation at the Bank or in addition to it, the Bank can implement the product by installation on the cloud and/or a hybrid solution.

4.3 Optional characteristics

An **optional characteristic** – The existence of the characteristic and the possibility of the bidder developing it, subject to the required time for development, is an advantage. The bidder will specify in his bid whether the characteristics exists in the system or whether it can develop the characteristic, the duration of the development and the price of the development. The Bank can order the develop of the characteristic from the bidder according to the implementer hours specified by the bidder in his bid, in coordination with the supplier an any stage prior to the system going live and even subsequent to that:

#	Type of characteristic	Description of the characteristic
1	Technological	The system will provide a mechanism for defining and monitoring the SLA of various entities connected to the Bank, according to levels and/or functions in the organization. The definitions and the monitoring need to be executable by the authorized users without having to involve a programmer.
2	Technological	The system will support the production of operational reports subject to the Bank of Israel's organizations levels, from the level of manager (responsible) of the project up the aggregative level of the entire organization. The main types of reports can be differentiated as follows: <ul style="list-style-type: none"> a. Various operational and managerial reports for project managers: including deviations from milestones (current and future), deviations from a timetable, deviations of current costs and deviation of expected costs, planned activities for various horizons. b. Various operational and managerial reports for the organization's unit managers: these reports will make it possible to audit the collection of projects and tasks under their responsibility. c. Managerial reports for the Bank of Israel management: <ul style="list-style-type: none"> 1. Reports that will make it possible for the Bank's management to obtain an overall picture of the main activities and projects in the Bank and the state of their progress. 2. Reports that will present the Bank's overall workplan, from the level of long-term targets up to the level of tasks and the resources allocated to each of them.
3	Technological	The system will support the retrieval of past planning and execution information.
4	Technological	The system will facilitate an ability to work from mobile phones and tablets (subject to information security procedures).
5	Technological	The system will have an additional module that provides a response to public enquiries, which will make it possible to receive enquiries from the public that are addressed to the Internal Audit Department, manage them, and deal with them.

5. Other priced options and services

The Bank has the right to acquire additional services from the winner in order to expand the system. The winner will modify the system in order to exercise that option, and when building the system the supplier will also take into account the ability to expand the system and to exercise the various options. In addition, the system will facilitate the integrative and mutual connectedness between the internal audit and risk management processes that are managed within it and each option separately and between each of the options themselves, as described

in Part II – The Financial Bid. The various functions will provide the system with all of the existing functionality to meet the needs of Internal Audit and risk management.

6. Reports and queries

The Bank will be able to produce reports from the system according to its needs and the system will make it possible to produce all of the managerial and operational reports and queries requested by the Bank of Israel from the system's data.

7. Topics to be described in the bidder's response

In his response, the bidder will describe the solution he is proposing and will also describe, among other things, the following points:

- 7.1 How the proposed solution meets the requirements of survivability and redundancy.
- 7.2 The mechanism for investigating the logs and the user interfaces.
- 7.3 The hardware and software requirements at the Bank's site in order to implement the proposed solution.
- 7.4 In a full manner, the hosting format in cloud services (if in the future the Bank seeks to transfer to that platform, whether in part or in full or in hybrid) including:
 - 7.4.1 The supplier of cloud services.
 - 7.4.2 The operating systems.
 - 7.4.3 The communication characteristics.
 - 7.4.4 The security measures that are implemented.
 - 7.4.5 The names of products that are in use, including the versions.
 - 7.4.6 The encryption mechanisms.

Mechanisms that ensure operational continuity in an emergency (DR).

- 7.5 If the solution supports the validation of XML files according to the XSD scheme (according to the requirements to be defined during the stage of characterizing the solution), then the bidder should describe the solution.
- 7.6 The bidder is to fully describe the information security solution with emphasis on the following points:
 - 7.6.1 Standards – beyond the required ISO 27002:2013 standard, with what additional standards does the bidder comply.
 - 7.6.2 Information storage – A description by the supplier of the infrastructures in which the information is stored, with attention paid to the information required to be stored within Israel.
- 7.7 Data security**
 - 7.7.1 Is it possible to synchronize data between the customer's personal computers and how that synchronization is accomplished;
 - 7.7.2 A description of how the bidder verifies that his other customers cannot read or change another customer's data by means of the application/service;

7.7.3 A description of the possibility of accessing the data of customers not by way of the application but by way of a different interface (API) and how the bidder secures the provision of such access.

7.7.4 A description of the encryption in the customer's' encryption key if there is one.

7.8 Application security:

7.8.1 A description of the methodology according to which developers receive guidance/instruction in secure development (SDLC, OWASP).

7.8.2 A description of identification for the application by MFA.

8. Ongoing warranty and maintenance services

8.1 If the winner is not the producer of the system or parts of it, he will be required to obtain confirmation that all of the components for which the Bank has acquired maintenance services are to found in a back2back agreement with the producer, including a description of the components, within 14 business days from the receipt of the order from the bank, in other to, among other things, ensure an accessible inventory of parts for failures of various types.

8.2 If the producer declares an end-of-service date for the license or a particular device, the winner will notify the Bank of this at least 360 days ahead of time.

8.3 Since the systems are used on an ongoing basis by the Bank, some of the installation work will be carried out after hours, according to the sole discretion of the Bank, without any additional proceeds.

8.4 The work on the system will be carried out only on the premises of the Bank and an external connection to Bank's system will not be possible, whether in order to deal with a failure or the retrieval of logs from the system.

8.5 For each of the products to be acquired, the winner will provide warranty services, starting from the end of the installation of the product at the Bank and for a period of one year, without any additional proceeds (hereafter: the "warranty period" or the "**warranty services**"), as defined below and they will be provided in the manner described in this paragraph and with the same response times, even if the producer of the product, despite his obligation, decides to terminate his support.

8.6 The maintenance service will include a guarantee of the system and the applications that were developed, including software updates, revisions and the correction of bugs, with the goal of ensuring the integrity and continuity of the system's operations, including overall support and preventative maintenance activity in the system.

8.7 The winner will provide efficient and continuous maintenance services, while using manpower to the satisfaction of the Bank.

8.8 In order to remove any doubt, it is hereby clarified that during the warranty and maintenance periods all of the agreement instructions will apply to its appendices.

8.9 The maintenance services will include the following:

8.9.1 **Corrections** – A correction of errors and problems that emerge in the operation of the system.

- 8.9.2 **Routine maintenance** – Any action required in order for the system to operate in a normal manner and on a continuous basis.
- 8.9.3 **Support services** – Providing a response to the Bank's requests by means of a manned support center and providing a response (by telephone, fax, email, etc.) in order to obtain routine assistance, advice, instructions, solutions to problems, information on possible new options and their implementation, the optimal operation and configuration of licenses and the existing devices in the Bank, consultation regarding technological alternatives and providing responses to any other question that arises among the Bank's users and which is required for the efficient and optimal operation of the system.
- 8.9.4 **Installation of versions or upgrades to the system's hardware and software** – The guarantee of the provision and installation of new versions or upgrades of software and hardware components (including upgrades to the operating system, the backup software, etc.) will apply to the winner as part of the maintenance services on a quarterly basis. The upgrades will include software updates. The date for carrying out updates / upgrades to more advanced versions (including the decision of whether to carry out an update / upgrade) will be decided on by the Bank, such that sufficient time prior to the update, the winner will provide the Bank with the details of the update and its timing. In order to remove any doubt, the Bank will have the right not to adopt the upgrade if there is concern about damage to the system's ongoing functioning or the absence of full compatibility of the version to the Bank's systems that are involved in the business processes.
- 8.9.5 The maintenance services include updates of hardware, software, and licenses, as well as the upgrade of software and of firmware for hardware devices.
- 8.10 The winner is obligated to carry out the required corrections or repairs in a timely manner without delay and to complete them within as short a time as possible.
- 8.11 For the purpose of providing maintenance services, the winner will make available to the Bank a manned call center with various means of communication (telephone, fax and email) that are available to receive messages, from Sunday to Thursday from 8:00–17:00 and on Friday from 8:00–13:00, apart from Jewish holidays as defined in paragraph 1 above. When opening a call at the center, the problem / question will be recorded in an organized fashion and it will be possible to track by means of a call number that will be received on opening the call.
- 8.12 The maintenance services will include a support center for the Bank's suppliers that operates from Sunday to Thursday, from 8:00–17:00, for the provision of support, instruction and consultation services to the Bank's suppliers, in both Hebrew and English.
- 8.13 The winner is obligated to provide reaction times as follows:

- a. Breakdowns – A professional telephone response will be provided within 30 minutes of the receipt of the call and a telephone response will be provided by a product expert within one hour. The product expert will arrive at the Bank’s premises and will begin to deal with the problem within 4 hours of the call.
 - b. Problems other than breakdowns – A professional telephone response will be provided within one regular working hour from the time of the call and similarly a telephone response from a product expert will be provided within two hours of the time of the call. In the event that the problem remains unresolved for more than 120 hours, the Bank will have the right to demand that the winner send a technician to the Bank’s premises. The Sabbaths and Jewish holidays will not be included in the 120 hours for purposes of this paragraph.
 - c. A call by the bank’s representative or someone authorized to do so by the Bank to the call center will receive a human response within 10 minutes.
- 8.14 In the event of a breakdown in a hardware device that is not resolved within 96 hours, the winner will provide replacement equipment until the correction of the problem. The winner will activate a hardware replacement procedure within 12 hours of the report of the problem. The repaired or replacement system must operate in its previous format within 168 hours. Sabbaths and Jewish holidays will not be included in the number of hours for the purposes of this paragraph.
- 8.15 If the problem is not a breakdown and was not resolved within 72 hours, the Bank will have the right to demand that the winner open a call with the producer. Sabbaths and Jewish holidays and their eves will not be taken into account for the purposes of this paragraph.
- 8.16 The winner can attempt to provide a telephone response in order to solve problems that arise; however, this does not exempt him from providing a solution or delaying the timetable appearing above.
- 8.17 The representative of the Bank or anyone authorized by the Bank for this purpose will classify the problems according to his sole discretion and he will provide confirmation that the problem has been dealt with. The aforementioned does not detract from the winner’s responsibility to identify the problems and resolve them.
- 8.18 The winner will employ, whether directly or via a subcontractor, at least two workers who have undergone training in the system installed at the Bank, during the entire period of contractual relations.
- 8.19 The workers designated to support the Bank’s system must undergo security checks as described in paragraph 8 of the agreement.
- 8.20 The winner will appoint a contact person on his behalf to provide a response to the Bank’s representative. The aforementioned does not detract from the winner’s obligation to provide a response by means of the support center.

- 8.21 The winner will provide the Bank's representative with a list of contact people for the purpose of escalation in the event that a problem is not properly resolved. The winner will ensure that the list possessed by the Bank remains up to date for the entire period that services are provided.
- 8.22 The maintenance services will be provided at all sites of the Bank at which the devices or software are operated. It should be emphasized that the provision of remote support to the site of the Bank **will not be possible**.
- 8.23 If the winner's experts do not succeed in solving the problem, the winner will use the expert services of the producer as needed.
- 8.24 In order to remove any doubt, it is hereby clarified that a service call by a technician to the Bank's premises in order to solve a problem within the framework of maintenance services as defined above will not result in any additional proceeds.
- 8.25 If the connection between the producer and the Company is terminated, whether due to the Company's decision or the producer's decision, the Bank can, according to its sole discretion, terminate the relationship with the winner and acquire the services from a different company.

Two-Stage Automated Public Tender no. 31/23

For the provision of a system for the management of Internal Audit and Risk Management

Appendix D1 – The System Requirements

- This section describes the functionality requirements of the system in order to assess the quality of the bid as described in the tender documents. The Bank will have the right to verify the fulfillment of these conditions in the stage of the feasibility check as described in the procedure for evaluating bids.
- The bidder is to relate to each paragraph and to clearly state how the solution he is proposing fulfills each of the requirements and sub-requirements appearing below.

Description of the main processes

1. The Audit task / the audit follow-up task / the employees' complaint task (ombudsman role)

Requirement	Description	Comments/examples
Opening of an Audit task / assessment / employee or anonymous complaint file task / other task	<ul style="list-style-type: none"> • Opening of a task in the system by the Chief Audit Executive. 	
Letter of notification to the auditee	<ul style="list-style-type: none"> • Notification of an opening of an audit task. • Request for a contact person. • Request and receipt of material. • In the case of employees' complaints – a request for a response to the complaint letter. 	
Pre-survey and audit plan	<ul style="list-style-type: none"> • Structured paragraphs in the presurvey. • Some of the audit plan items are structured. • Retrieval risk survey data and failure events' data from the risk survey module. • Possibility for an audit follow-up report. • Manager's approval. 	

Fieldwork	<ul style="list-style-type: none"> • Filing of working papers and discussion summaries. • Possibility of email correspondence within the system. • Manage of a request and receipt of material from the auditee. • Task management – what has been carried out in the audit plan, including a list of minor tasks. 	
Draft report	<ul style="list-style-type: none"> • A fixed format for the draft structure, including main headings. • The ability to retrieve findings from the fieldwork. • Design of an identical draft: <ul style="list-style-type: none"> a. Audit tasks; b. Follow-up audit tasks; c. Examination report following a complaint. d. Summary of the examination following a complaint. • Comments by the Internal Audit management. • Approval by the Internal Audit management. • Sending a request for a response from the auditee with a click. • Response of the auditee by way of the system. 	<ul style="list-style-type: none"> • If there are findings in the document received / the summary of the discussion, there will be the possibility of classifying them into the correct section of the draft. • Font, letter size, alignment. • A fixed form letter for responding to the auditee.
Reminders	<ul style="list-style-type: none"> • Reminder to the auditee to submit their response, comments and/or material. 	

Final report	<ul style="list-style-type: none"> • Sending a final report to the relevant list of correspondences with a click. • Response to the complainant (in the complaint file). 	<ul style="list-style-type: none"> • The Governor, the Secretariat of the Supervisory Council, the Chairperson of the Supervisory Council / the Chairperson of the Audit Committee, the Deputy Governor, the Director General, the Audit Committee, Risk Management, Executive Management, the auditee.
Documentation and filing of documents	<ul style="list-style-type: none"> • Possibility of filing according to the audit plan items. • Storage without the possibility of making changes to the original document. 	In paragraph 1 of the audit plan, it is written to obtain procedures / material; when the procedures are received, there will be an option to file them in paragraph 1 with a click.
Audit task dashboard	<ul style="list-style-type: none"> • Dashboard for managers. • Dashboard for auditors. • Dashboard for the auditees. • Dashboard for Risk Management. 	<ul style="list-style-type: none"> • Task status. • Detailed task status. • Meetings that were held, meetings that are scheduled; dates when materials or responses are meant to arrive. • Sending of reminders. • Monitoring of the receipt of requested materials.

2. Follow-up of implementation of Audit recommendations

Requirement	Description	Comments/examples
List of reference persons	<ul style="list-style-type: none"> • Creation of a reference person for each division / department. • Change of reference persons by the individuals responsible for following-up. 	
List of findings and recommendations attached to the report	<ul style="list-style-type: none"> • Retrieval of findings and recommendations from the final audit report, including degree of importance, division responsible, person responsible for implementation, and the date for implementation of the recommendations. • Additional fields that are not found in the report (such as professional classification). 	Ability to easily change data for a number of recommendations. For example: a new employee is appointed as responsible for follow-up, such that the change can be made in all of the recommendations in which the previous employee was responsible of.
List of findings and recommendations in the audit follow-up report	<ul style="list-style-type: none"> • Transfer of recommendations automatically from the original report to the follow-up report for the purpose of checking the implementation of the recommendations. 	

Inputting of updates	<ul style="list-style-type: none"> • Management of requests for updating the recommendations' implementation status from reference people / system participants. • Inputting of updates by all of the participants in the system. • Approval of Internal Audit to close a finding. • Possibility of attaching documents to recommendations. 	Attachment of a document by the person responsible for implementation as a proof that the recommendation was implemented.
Reminders	<ul style="list-style-type: none"> • Reminders to the person responsible for implementation, the reference person, the auditor and the person responsible for following-up at set intervals to input updates into the system. 	
Recommendations' follow-up dashboard	<ul style="list-style-type: none"> • Dashboard for Internal Audit management. • Dashboard for auditor. • Dashboard for reference person. • Dashboard for person responsible for implementation. • Dashboard for Risk Management. 	<ul style="list-style-type: none"> • A list of open and closed reports. • A list of open and closed recommendations. • Possibility for a reference person to see the reports under the responsibility of his Division with a click, as well as the findings and recommendations from outside his division.

3. Internal Audit workplans

Requirement	Description	Comments/examples
Preparation of a multiyear workplan	<ul style="list-style-type: none"> • Support for the process to formulate risk-based workplans. • Dashboard for viewing data from the Risk Survey and failure events from the risk management module. • Comparison to previous multiyear workplan. • Linkage to the Bank's objectives. • Coverage of all of the Bank's divisions. • Possibility to set the frequency of an Audit task in each process. • Resource planning according to the workplan (human resources). 	Option of retrieving relevant data from the risk management module (relevant risks, relevant failure events, etc.).
Preparation of an annual workplan	<ul style="list-style-type: none"> • Retrieval of data from the multiyear workplan. • Linking a task in the workplan to the auditee responsible. • Planning of support budget resources. 	
Updating of annual workplan	<ul style="list-style-type: none"> • Option of updating the plan. • Writing of arguments in favor of changes within the system. 	
Workplan dashboard	<ul style="list-style-type: none"> • Dashboard for Internal Audit management. • Dashboard for auditors. • Dashboard for auditees. • Dashboard for Risk Management. 	Retrieval of data from the Internal Audit dashboard with respect to the status of a task in the workplan – the current stage of the task.

4. Annual/semi-annual Internal Audit report

Requirement	Description	Comments/examples
A list of the various Audit tasks, divided according to the Audit tasks' plan, the follow-up plan, the quality plan, other tasks, employee complaints and public complaints.	<ul style="list-style-type: none"> • Status of execution. • Executed tasks – dates of the report publication, discussion in the Audit Committee and discussion in the Supervisory Council. • Possibility of presenting planned vs actual. 	Retrieval of data from the workplan dashboard.
Presentation of data on the recommendations for following-up according to the date of their recording	<ul style="list-style-type: none"> • Recommendations being followed up at the beginning of the year – how many were closed and how many remain under follow-up, by division. • Recommendations that were added during the year – how many were closed and how many remain under follow-up by division. • Summary of all of the followed-up recommendations by division. 	Retrieval of data from the recommendations' follow-up dashboard.

<p>Recommendations whose implementation date arrived</p>	<ul style="list-style-type: none">• Recommendations that were closed – according to implemented / not implemented / closed / being followed-up.• Breakdown of the number of recommendations by division and degree of importance, how many were deferred and how many were implemented, including the rate of deferral and a graph, as well as a comparison to the previous two years.• The range of recommendation deferrals that were carried out and of the recommendations that have not yet been implemented, by degree of importance.• Number of recommendations that were deferred for two years or more, by division and degree of importance.• Reports and the subjects of recommendations that were deferred for two years or more.	
--	---	--

<p>Appendices – a summary of the recommendations</p>	<ul style="list-style-type: none"> • Recommendations arising from complaint reports that were closed and under follow-up, by division and report, as well as a list of recommendations that were deferred. • Recommendations that were closed / are followed-up. • Recommendations with a high degree of importance that were deferred for more than a year. • Recommendations that were deferred for two years or more. 	
<p>Publication and distribution of the final report</p>	<ul style="list-style-type: none"> • Sending to the relevant addressees with a click. 	<p>The Governor, the Chairperson of the Supervisory Council / the Chairperson of the Audit Committee, the Deputy Governor, the Director General, the Audit Committee, Risk Management, Executive Management, Auditees.</p>

5. Public enquiries to Internal Audit – Ombudsman Role concerning the activity of the Bank of Israel

Requirement	Description	Comments/examples
Files under the authority of Internal Audit and the Ombudsman role	<ul style="list-style-type: none"> • Name of the complainant. • Date of receipt of the complaint. • Date on which confirmation of receipt was sent. • Status of the complaint (open/closed). • Date on which a final answer was sent to the complaint. • The target of the complaint in the Bank of Israel. • The subject of the complaint. • Classification of the complaint: justified / not justified / not relevant / handled without taking a position. • Comments to the file. • Across-the-board issues. 	Structured enquiry form in the system that includes these fields.
Followed-up files	<ul style="list-style-type: none"> • Name of the complainant. • Date of receipt of the complaint. • Date on which the file was closed. • Status of the complaint (open/closed). • Handler of the complaint in the Bank of Israel. • Comments to the file. • Across-the-board issues. 	Structured enquiry form in the system that includes these fields.

Files that were opened as the result of an enquiry / complaint from the public and which are not under the responsibility of Internal Audit	<ul style="list-style-type: none"> • Name of the complainant. • Date of receipt of the complaint. • Date on which the file was closed. • Comments to the file. 	Structured enquiry form in the system that includes these fields.
Annual and semiannual report	Presentation of a list of enquiries received during a specific period, all of the enquiries that were closed during a specific period, by various cross sections (the target of the complaint, classification of the complaint, etc.). Information should also be provided with respect to subjects that were classified as systemic.	Retrieval of data from the structured forms.
Documentation and filing of documents	<ul style="list-style-type: none"> • Documentation of documents for every type of enquiry, which can be accessed from the enquiry itself. • Storage without the possibility of changing the original document. 	
Public enquiries dashboard	<ul style="list-style-type: none"> • Dashboard for managers. • Dashboard for the targets of complaints. 	<ul style="list-style-type: none"> • Status of the enquiry. • Due date material or a response meant to arrive • Sending of reminders.

6. Risk management

Requirement	Description	Comments/examples
Management of the process life cycle	Creation of new processes, changes in process status, changes in the level of the process, editing ability and approval of all information in the process.	

Management of risk life cycle	<p>Creation of new risks, changes in risk status (and approval of a change that was made by others), changes in the level of the risk (and approval of the change that was made by others), ability to edit all of the information on the risks and internal controls and the status of the internal controls. Ability to view changes (which the system will automatically tag) made to information on risk.</p> <p>A methodology for risk ranking is: ranking a root risk of the process and ranking of risk related to the process according to likelihood and a scale of magnitude (residual risk given the internal controls).</p> <p>Comment: the system should support the management of more than one scale of impact– under the management of a business administrator. Storage of a static copy (“freezing”) of risk data for each division as of the end of the reporting period.</p>	
Documentation of internal controls	<p>Creation of new controls and their linkage to a risk, changes in control status (and approval of change that was made by others), changes in the ranking of a control (and approval of the change that was made by others), ability to edit all of the information on the controls and their status. Ability to view the changes (which the system will automatically tag) that were made to information on the controls.</p>	
Event documentation (failure events)	<p>Reporting and creation of new events (authorization for all employees) and their linkage to a risk, changes in event status (including the status that a particular event is not a failure event), changes in an event’s level of impact, editing ability and approval of all information about an event.</p>	

<p>Management of the life cycle of a risk realization event (failure events)</p>	<p>Support for reporting and creation of new events in the operational stage of the event's management (flow of the relevant information to the office holders that need to act in order to manage the event). Possibility of reporting the actions carried out during the event as part of the reporting processes needed in the case of failure events. The system will make it possible for business users to deal with events, starting from the stage of detection until the completion of the event. The system will make it possible to create a distribution list of relevant entities who should know about and deal with the event. The reporting of a failure event will include all of the information gathered in the stage of dealing with the event. Not all events are necessarily failure events and they will be given the appropriate status.</p>	
<p>Management of the life cycle of an event examination</p>	<p>Reporting and creation of new examinations and their linkage to an event, linkage of an examination to an event, changes in the status of an examination, editing ability and approval of all of the information on an examination.</p>	
<p>Management of the life cycle of recommendations and decisions</p>	<p>Creation of new recommendations and decisions, changes in recommendation status (and approval for the completion of handling of a recommendation carried out by others or a reopening), editing ability and approval of all information on the recommendation (every employee linked to the recommendation can update information on the recommendation). The recommendations will be linked to an entity, such as: process, risk, internal control, examination, event and audit report.</p>	

Documentation and filing of documents	Possibility to document an attached document to every entity in the system: process, risk, event, examination and recommendation.	
Dashboard management	Dashboard tailored to the main functions: risk management, key reference persons for risk management, division managers, "regular" employees, and key users from Internal Audit.	
Workflow processes	The system will facilitate controlled changes that are accomplished by a chain of signatures of the relevant office holders to change selected status values in the system, such as: processes, risks, events and recommendations. According to the chain of signature, the information will be transferred to and from the risk management entities and the divisions.	
Risk appetite	The system will include a risk appetite module in accordance with accepted methodologies: general declaration of risk appetite, appetite for risk at the risk level and at the process level. The system will support KRI management.	
Connection between Internal Audit and Risk Management (and other functions: compliance, Israeli SOX, etc.)	The system will facilitate various functions: internal audit, risk management, other second-line defense functions, such as: compliance and Israeli SOX, which will be independent and separate from other functions, and will facilitate the sharing of data according to a specific requirement.	

7. Management of organizational structure in the system in order to provide information to the relevant office holders

Requirement	Description	Comments/examples
Management of the organizational structure and the office holders in the system	<ul style="list-style-type: none">• Interfacing and link with the Bank's organizational management systems.• Management of the organizational structure and office holders in the risk management and internal audit system according to the interfaces.• Possibility of defining groups and office holders on the basis of need-to-know authorization management.	