

(51) International Patent Classification:
G06Q 10/00 (2006.01)(21) International Application Number:
PCT/US2011/030431(22) International Filing Date:
30 March 2011 (30.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/329,724 30 April 2010 (30.04.2010) US
12/831,104 6 July 2010 (06.07.2010) US(71) Applicant (for all designated States except US): **BANK OF AMERICA CORPORATION** [US/US]; 214 N. Tryon Street, Mailcode: NC1-027-20-05, Charlotte, North Carolina 28255 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ALVAREZ, Tammy** [US/US]; 3900 Berner Court, Waxhaw, NC 28173 (US). **MARGOLIS, Scott** [US/US]; 137 Trailwood Lane, Coppell, TX 75019 (US).(74) Agent: **BROWN-SANFORD, Christa**; Baker Botts LLP, 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

[Continued on next page]

(54) Title: INTERNATIONAL CROSS BORDER DATA MOVEMENT

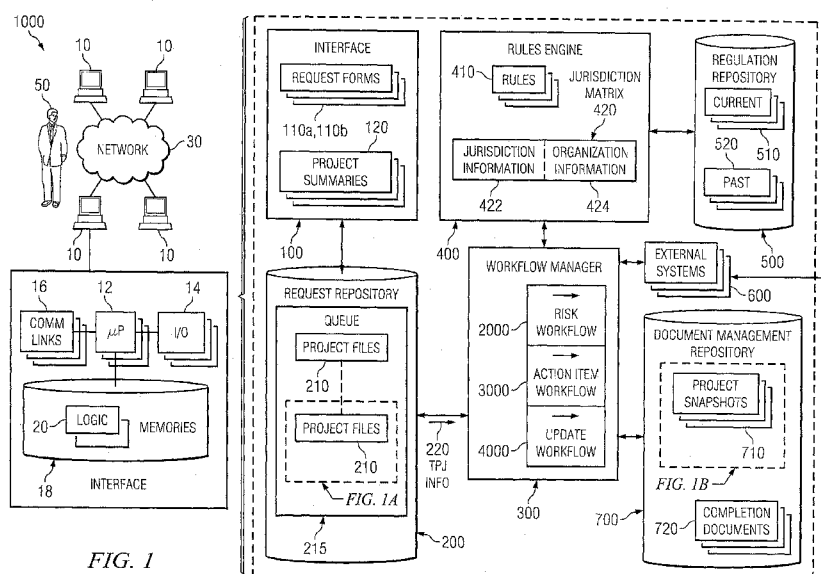


FIG. 1

(57) Abstract: In some embodiments, a data movement system comprises a rules repository configured to store rules associated with regulations of the first jurisdiction and the regulations of the second jurisdiction. A workflow manager is configured to determine jurisdictional complexity of the project as a function of the regulations of the first jurisdiction and the second jurisdiction. The workflow manager is configured to determine jurisdictional exposure of the project as a function of an organization's exposure to the first jurisdiction and the second jurisdiction. The workflow manager is configured to determine the risk of the project as a function of the jurisdictional complexity of the project and the jurisdictional exposure of the project.



Published:

— *with international search report (Art. 21(3))*

INTERNATIONAL CROSS BORDER DATA MOVEMENT

TECHNICAL FIELD

5 The present disclosure relates to data movement generally and more specifically to international cross border data movement.

BACKGROUND

10 Some jurisdictions may restrict an organization's ability to export certain types of data. These jurisdictions may promulgate regulations that either prohibit exportation of certain types of data or allow exportation subject to specified restrictions. The extent and complexity of these regulations may differ among jurisdictions.

SUMMARY

15 In some embodiments, a data movement system comprises a rules repository configured to store rules associated with regulations of the first jurisdiction and the regulations of the second jurisdiction. A workflow manager is configured to determine jurisdictional complexity of the project as a function of the regulations of the first jurisdiction and the second jurisdiction. The workflow manager is configured
20 to determine jurisdictional exposure of the project as a function of an organization's exposure to the first jurisdiction and the second jurisdiction. The workflow manager is configured to determine the risk of the project as a function of the jurisdictional complexity of the project and the jurisdictional exposure of the project.

25 Certain embodiments may provide one or more technical advantages. A technical advantage of one embodiment may include the capability to identify inherent risk associated with moving data out of one or more jurisdictions. A technical advantage of one embodiment may include the capability to identify action items in furtherance of regulatory compliance. A technical advantage of one embodiment may include the capability to reduce risk associated with moving data
30 out of a jurisdiction by identifying and completing action items. A technical advantage of one embodiment may include the capability to provide a quantitative expression of inherent risk that may allow an organization to appropriately allocate

resources towards minimizing the organization's risk in that jurisdiction. A technical advantage of one embodiment may include the capability to improve organization knowledge of project history and provide a trail for evaluators to assess the organization's compliance with jurisdictional regulations.

5 Various embodiments of the invention may include none, some, or all of the above technical advantages. One or more other technical advantages may be readily apparent to one skilled in the art from the figures, descriptions, and claims included herein.

10 BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present disclosure and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, in which:

FIGURE 1 shows a data movement system according to one embodiment;

15 FIGURE 1A shows an example project file of FIGURE 1 according to one embodiment;

FIGURE 1B shows an example project snapshot of FIGURE 1 according to one embodiment;

FIGURE 2 shows a risk workflow according to one embodiment;

20 FIGURE 3 shows an action item workflow according to one embodiment;

FIGURE 4 shows an update workflow according to one embodiment;

FIGURES 5A-5D show example request forms according to one embodiment;

FIGURE 6 shows a jurisdictional matrix according to one embodiment;

25 FIGURES 7A and 7B shows example decision grids for applying rules to a request according to several embodiments; and

FIGURE 8 shows an example project summary according to one embodiment.

DETAILED DESCRIPTION

30 It should be understood at the outset that, although example implementations of embodiments of the invention are illustrated below, the present invention may be implemented using any number of techniques, whether currently known or not. The present invention should in no way be limited to the example implementations,

drawings, and techniques illustrated below. Additionally, the drawings are not necessarily drawn to scale.

An organization may conduct activities and store data in multiple jurisdictions throughout the world. An organization may include any social arrangement that pursues collective goals. One example of an organization is a business. A business is an organization designed to provide goods or services, or both, to consumers, governmental entities, and other businesses. Examples of a business may include, but are not limited to, agriculture and mining businesses, financial institutions, manufacturers, real estate companies, retailers and distributors, service businesses, transportation companies, and utility companies. A business may include both for-profit and not-for-profit businesses. An organization may also include multiple businesses. For example, an organization may control businesses in multiple jurisdictions throughout the world. Examples of organizations are not limited to businesses. For example, an organization can itself be a government entity.

Some jurisdictions may restrict an organization's ability to export certain types of data. These jurisdictions may promulgate regulations that either prohibit exportation of certain types of data or allow exportation subject to specified restrictions. The extent and complexity of these regulations may differ among jurisdictions. For example, an organization may store personally-identifiable information in ten different jurisdictions, and each of them may have different restrictions on the organization's ability to move the personally-identifiable information. In another example, the ten different jurisdictions may have different definitions as to what constitutes personally-identifiable information (e.g., jurisdictions may disagree as to whether an individual's job title is personally-identifiable information).

Teachings of certain embodiments recognize the ability for an organization with a past, current, or future data-movement project to identify inherent risk associated with moving data out of one or more jurisdictions. Returning to the last example, teachings of certain embodiments recognize the ability to quantitatively assess risk associated with exporting data out of one or all of the ten jurisdictions. Teachings of certain embodiments also recognize the ability to identify action items in furtherance of regulatory compliance. Returning to the last example, teachings of

certain embodiments recognize the ability to identify actions that the organization may take in a step toward compliance with governing regulations (e.g., actions required for compliance with a jurisdiction's data-movement regulations).

As used throughout, a data-movement project may include any project that involves moving data out of at least one jurisdiction. A data-movement project may be associated with one or more requests to move data. A request to transfer data may include any information regarding a past, present, or proposed movement of data out of a jurisdiction. A request to transfer data may include both one-time and recurring data movements. A jurisdiction includes any territory or legal division that may have regulations restricting exportation of data out of the jurisdiction. Examples of jurisdictions may include, but are not limited to, countries, states, dependencies (e.g., the Isle of Man), territories (e.g., the Cayman Islands), unions (e.g., the European Union), and other national and international organizations. Data may refer to either plural data or singular datum.

FIGURE 1 shows a data movement system 1000 according to one embodiment. FIGURE 1A shows an example project file 210 of FIGURE 1 according to one embodiment. FIGURE 1B shows an example project snapshot 710 of FIGURE 1 according to one embodiment.

In general, system 1000 receives requests to transfer data out of one or more jurisdictions and then aids in determining jurisdictional restrictions on transferring the data. These requests to transfer data are associated with data-movement projects, which may include any effort by the organization to move data.

In some embodiments, system 1000 may identify inherent risk associated with moving data out of one or more jurisdictions. Two example types of risk are jurisdiction risk and project risk. Jurisdiction risk may approximately express the inherent risk associated with moving data out of a jurisdiction. For example, a jurisdiction with a highly complex regulatory structure may add to inherent risk because of the possibility that the organization fails to comply with the regulations of the jurisdiction. A jurisdiction in which the organization's exposure is high may add to inherent risk because of the ramifications to the organization for failure to comply with the regulations of the jurisdiction. Teachings of certain embodiments recognize that a quantitative expression of inherent risk may allow an organization to

appropriately allocate resources towards minimizing the organization's risk in that jurisdiction. If the inherent risk associated with a jurisdiction is unmanageable, the organization may even decide to abandon efforts to move data out of the jurisdiction.

Project risk may approximately express the inherent risk associated with moving data out of each of the jurisdictions identified in the data-movement project. For example, a project with a higher project risk may indicate that the project includes a large number of jurisdictions with a highly complex regulatory structure and/or a large number of jurisdictions where the organization's exposure is high. Teachings of certain embodiments recognize that a quantitative expression of inherent project risk may allow an organization to appropriately allocate resources towards minimizing the organization's risk associated with that project. If the inherent project risk associated with the project is unmanageable, the organization may even decide to abandon the project.

In some embodiments, system 1000 may also identify action items required for regulatory compliance. As one example, if a jurisdiction requires outsourcing agreements with third parties to include certain terms, then system 1000 may analyze a project to determine whether the organization needs to include the certain terms in its outsourcing agreements. Teachings of certain embodiments recognize that identifying action items and completing those action items may reduce risk associated with moving data out of a jurisdiction. Thus, if a jurisdiction has a high inherent jurisdiction risk or a project has a high inherent project risk, identifying and completing action items may mitigate risk. In this manner, identifying and completing action items may be analogous to an internal control system for minimizing risk.

An internal control may include any process effected by an organization that is designed to accomplish specific goals or objectives, such as reducing risk. Teachings of certain embodiments also recognize the ability to manage and track execution of action items as an additional mechanism for monitoring and mitigating risk. Action items may include specific actions that an organization may take to comply with a rule or regulation, or to otherwise mitigate risk associated with moving data out of a jurisdiction. Action items may be managed and tracked over time. For example, action items may include recurring actions to be completed, and action items may

change over time due to changes in the project or changes in any governing regulations. Teachings of certain embodiments also recognize that tracking execution of action items may allow an evaluator to later confirm that the project is complying with any governing regulations.

5 The example system 1000 of FIGURE 1 features an interface 100, a request repository 200, a workflow manager 300, a rules engine 400, a regulation repository 500, external systems 600, and a document management repository 700, that may be implemented by one or more computer systems 10.

10 Computer system 10 may include processors 12, input/output devices 14, communications links 16, and memory 18. In other embodiments, computer system 10 may include more, less, or other components. Computer system 10 may be operable to perform one or more operations of various embodiments. Although the embodiment shown provides one example of computer system 10 that may be used with other embodiments, such other embodiments may utilize computers other than
15 computer system 10. Additionally, embodiments may also employ multiple computer systems 10 or other computers networked together in one or more public and/or private computer networks, such as one or more networks 30.

20 Processors 12 represent devices operable to execute logic contained within a medium. Examples of processor 12 include one or more microprocessors, one or more applications, and/or other logic. Computer system 10 may include one or multiple processors 12.

25 Input/output devices 14 may include any device or interface operable to enable communication between computer system 10 and external components, including communication with a user or another system. Example input/output devices 14 may include, but are not limited to, a mouse, keyboard, display, and printer.

30 Network interfaces 16 are operable to facilitate communication between computer system 10 and another element of a network, such as other computer systems 10. Network interfaces 16 may connect to any number and combination of wireline and/or wireless networks suitable for data transmission, including transmission of communications. Network interfaces 16 may, for example, communicate audio and/or video signals, messages, internet protocol packets, frame relay frames, asynchronous transfer mode cells, and/or other suitable data between

network addresses. Network interfaces 16 connect to a computer network or a variety of other communicative platforms including, but not limited to, a public switched telephone network (PSTN); a public or private data network; one or more intranets; a local area network (LAN); a metropolitan area network (MAN); a wide area network (WAN); a wireline or wireless network; a local, regional, or global communication network; an optical network; a satellite network; a cellular network; an enterprise intranet; all or a portion of the Internet; other suitable network interfaces; or any combination of the preceding.

Memory 18 represents any suitable storage mechanism and may store any data for use by computer system 10. Memory 18 may comprise one or more tangible, computer-readable, and/or computer-executable storage medium. Examples of memory 18 include computer memory (for example, Random Access Memory (RAM) or Read Only Memory (ROM)), mass storage media (for example, a hard disk), removable storage media (for example, a Compact Disk (CD) or a Digital Video Disk (DVD)), database and/or network storage (for example, a server), and/or other computer-readable medium.

In some embodiments, memory 18 stores logic 20. Logic 20 facilitates operation of computer system 10. Logic 20 may include hardware, software, and/or other logic. Logic 20 may be encoded in one or more tangible, non-transitory media and may perform operations when executed by a computer. Logic 20 may include a computer program, software, computer executable instructions, and/or instructions capable of being executed by computer system 10. Example logic 20 may include any of the well-known OS2, UNIX, Mac-OS, Linux, and Windows Operating Systems or other operating systems. In particular embodiments, the operations of the embodiments may be performed by one or more computer readable media storing, embodied with, and/or encoded with a computer program and/or having a stored and/or an encoded computer program. Logic 20 may also be embedded within any other suitable medium without departing from the scope of the invention.

Various communications between computers 10 or components of computers 10 may occur across a network, such as network 30. Network 30 may represent any number and combination of wireline and/or wireless networks suitable for data transmission. Network 30 may, for example, communicate internet protocol packets,

frame relay frames, asynchronous transfer mode cells, and/or other suitable data between network addresses. Network 30 may include a public or private data network; one or more intranets; a local area network (LAN); a metropolitan area network (MAN); a wide area network (WAN); a wireline or wireless network; a local, regional, or global communication network; an optical network; a satellite network; a cellular network; an enterprise intranet; all or a portion of the Internet; other suitable communication links; or any combination of the preceding. Although system 1000 shows one network 30, teachings of certain embodiments recognize that more or fewer networks may be used and that not all elements may communicate via a network. Teachings of certain embodiments also recognize that communications over a network is one example of a mechanism for communicating between parties, and any suitable mechanism may be used.

Interface 100 may include any interface accessible by a user, such as a user 50. User 50 may include any individual, group of individuals, entity, machine, and/or mechanism that interacts with interface 100. Examples of users 5 include, but are not limited to, a manager, executive, review board, accountant, engineer, technician, contractor, agent, and/or employee or representative of an organization.

Interface 100 may include one or more forms for receiving information from user 50 and/or providing information to user 50 relating to a data-movement project. A data-movement project may include any project that involves moving data out of at least one jurisdiction. As one example, a data-movement project may involve moving data from a first jurisdiction to a second jurisdiction. As another example, a data-movement project may involve sharing data among multiple jurisdictions. Data-movement projects may include both one-time and recurring movements of data.

Data-movement projects may move data for any suitable purpose. As one example, a data-movement project may allow multiple business units or lines of business of an organization to share data housed in different jurisdictions. In this example, interface 100 may receive any information useful in determining whether and how the data-movement project implicates data privacy regulations promulgated by the different jurisdictions. Data privacy involves the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Example data privacy regulations

may include, but are not limited to, regulations restricting the collection and movement of personally identifiable information, which may be received from sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits and genetic material, residence and geographic records, and ethnicity.

As another example, data may be moved out of a jurisdiction in order to comply with a request from outside the organization, such as a subpoena. In this example, interface 100 may receive any information useful in determining whether and how the data-movement project implicates data secrecy regulations promulgated by the jurisdiction. Data secrecy involves ensuring that information is accessible only to those authorized to have access. One example of data secrecy is bank secrecy. Bank secrecy is a legal principle in some jurisdictions under which financial institutions are not allowed to provide to authorities personal and account information about their customers unless certain conditions apply. For example, bank secrecy regulations are prevalent in countries such as Switzerland, Singapore, and Luxembourg.

As yet another example, a data-movement project may involve outsourcing data out of a jurisdiction to an external organization, such as a third-party data processor. In this example, interface 100 may receive any information useful in determining whether and how the data-movement project implicates outsourcing regulations promulgated by the jurisdiction. Outsourcing involves the practice of hiring an external organization to perform some functions using an organization's data. Outsourcing regulations may include restrictions on what data may be outsourced and restrictions stipulating how outsourced data must be handled.

In one embodiment, interface 100 includes one or more request forms 110a and 110b and one or more project summaries 120. Example request forms 110a and 110b are shown in FIGURES 5A-5D, and an example project summary 120 is shown in FIGURE 8.

Request forms 110a and 110b provide a form for receiving information regarding requests to transfer data out of one or more jurisdictions. In one embodiment, information received through request forms 110a and 110b is stored in a project file 210 in request repository 200. In this example embodiment of FIGURE

1A, the information received through request forms 110a and 110b includes project information 212, data movement information 214, and jurisdiction information 216. Project information 212 may include any information regarding a data-movement project, such as a project name, a project identifier, a requestor name and contact information, and a project type. Data movement information 214 may include any information regarding the proposed data movement, such as a type of data to be moved, a purpose for the data movement, and information identifying whether the data movement will be one-time or recurring. Examples of data type may include personal data (e.g., customer, client, or associate specific identifiable data), background data, transaction data (e.g., individual transaction level data), government data (e.g., data about or controlled by a sovereign entity), medical data (e.g., information containing personal medical records), sensitive data (e.g., religious or political affiliations), and anti-money laundering information (e.g., trending to identify anti-money laundering transactions). Teachings of certain embodiments recognize that categories of data types may differ among jurisdictions. As one example, some jurisdictions consider an individual's job title to be personally-identifiable information, whereas other jurisdictions do not. Examples of movement purposes include anti-money laundering, sales, servicing, marketing, financial reporting, fulfillment, data storage, testing, associate access, reporting, processing, and document storage. Jurisdiction information 216 may include information identifying one or more jurisdictions hosting the data to be moved. Additional examples of request forms 110a and 110b, project information 212, data movement 214, and jurisdiction information 216 are described with respect to FIGURES 5A-5D.

Referring back to FIGURE 1, project summary 120 provides a form for reporting information regarding requests to transfer data out of one or more jurisdictions. In one example, such reported information includes the project information 212, the data movement information 214, the jurisdiction information 216, and results information 218. Results information 218 may include any information regarding jurisdictional restrictions on transferring the data, such as information regarding regulations promulgated by one or more jurisdictions, actions that facilitate with the regulations promulgated by one or more jurisdictions (e.g., action items), and actions completed towards compliance with the regulations

promulgated by one or more jurisdictions. Examples of the regulations promulgated by one or more jurisdictions include current regulations 510 and past regulations 520, which is described in greater detail with regard to regulation repository 500. Additional examples of project summary 120, project information 212, data movement 214, jurisdiction information 216, and results information 218 are described with respect to FIGURE 8.

Request repository 200 may include any repository for storing information regarding requests to transfer data out of one or more jurisdiction. In the illustrated embodiment, request repository 200 stores one or more project files 210. Each project file 210 includes information regarding one request to transfer data out of one or more jurisdictions. Each project file 210 may also be assigned a unique record locator for identifying the project file 210. In the illustrated embodiment, project file 210 information includes project information 212, data movement information 214, jurisdiction information 216, and results information 218. Request repository 200 may receive project information 212, data movement information 214, and jurisdiction information 216 from interface 100 and may receive results information 218 from workflow manager 300.

In some embodiments, project files 210 may be ordered in a queue for processing. Project files 210 may be arranged in any suitable order. In one embodiment, project files 210 are arranged according to a time stamp (e.g., in the order received). In some embodiments, a user 50 associated with the organization may manually change the order of project files 210 within queue 215. In another embodiment, project files 210 are automatically prioritized according to factors such as project type (e.g., proposed or active), data type, project deadlines, line of business, number of jurisdictions, regulation complexity, project purpose, project phase and/or project risk. One example of overall project risk is described with regards to FIGURE 2, which shows a risk workflow 2000 for calculating jurisdictional risk and project risk.

In one embodiment, request repository 200 may provide T-P-J information 220 to workflow manager 300. In this example, T-P-J information 220 includes three types of information about a project: a data type, a project purpose, and a jurisdiction hosting the data. T-P-J information 220 may be extracted from one or more project

files 210. Workflow manager 300 may use at least some of the T-P-J information 220 as inputs to one or more workflows.

The illustrated embodiment features three example workflows: risk workflow 2000, an action item workflow 3000 for identifying action items that facilitate regulatory compliance, and an update workflow 4000 for updating jurisdictional restrictions on a project. As one example, risk workflow 2000 may assess risk for a project that involves moving first data from a first jurisdiction and second data from a second jurisdiction. The first and second jurisdictions may be identified by T-P-J information 220, and the regulations of those jurisdictions may be collected from current regulations 510 stored on regulatory repository 500. Risk workflow 2000 may also use rules 410 in lieu of or in addition to current regulations 510. In this example, the project may be determined based on the jurisdictional complexity of the project and the jurisdictional exposure of the project. The jurisdictional complexity of the project may be determined based on the regulations of the first jurisdiction and the second jurisdiction. The jurisdictional exposure of the project may also be determined based on the organization's volume of business activity in the first jurisdiction and the second jurisdiction.

As another example, action item workflow 3000 may determine information for moving data from one or more jurisdictions. T-P-J information 220 may identify request information including a data type, a jurisdiction from which the data is to be moved, and a purpose for moving the data. A set of data movement rules may be identified and applied against the request to identify an action item to be completed in order to comply at least in part with the regulations.

As yet another example, update workflow 4000 may update jurisdictional information for a project that involves moving data from a first jurisdiction. T-P-J information 220 may identify request information including a data type, a jurisdiction from which the data is to be moved, and a purpose for moving the data. An update to the request may be received changing some part of the T-P-J information 220. A set of data movement rules may be identified and applied against the updated request to identify an updated action item to be completed in order to comply at least in part with the regulations.

As yet another example, update workflow 4000 may update jurisdictional information for moving data across jurisdictional borders. T-P-J information 220 may identify request information including a data type, a jurisdiction from which the data is to be moved, and a purpose for moving the data. An update to the rules associated with the jurisdiction may be received. The update may represent a change to at least one regulation of the jurisdiction. The updated data movement-rules may be applied against the request to identify an updated action item to be completed in order to comply at least in part with the regulations.

Risk workflow 2000, action item workflow 3000, and update workflow 4000 are described in greater detail with regards to FIGURES 2, 3, and 4.

Rules engine 400 stores and applies rules 410. Rules 410 are associated with regulations of a jurisdiction. In the illustrated embodiment, rules 410 are developed from current regulations 510 stored in a regulation repository 500. Rules 410 may be developed dynamically from regulations 510 or may be compiled ahead of time based on regulations 510. In one embodiment, rules 410 may include if/then/else scenarios developed from regulations 510 to identify whether and/or how the regulations restrict movement of data out of a jurisdiction. Teachings of certain embodiments recognize that rules 410 may provide a structured mechanism for applying regulations of a jurisdiction to a project and may reduce the need to refer to the regulations directly. In one example, a regulation may be relevant if the project involves moving “data type A” data. In this example, a regulation may apply to data type A, and a corresponding rule may be applied against those projects that have data type=data type A. Thus, in this example, the relevant rule may be identified without searching the regulations for regulations that may implicate “data type A” data. Example rules 410 are described in greater detail with regard to FIGURES 7A and 7B.

Rules engine 400 may also store a jurisdiction matrix 420. Jurisdiction matrix 420 provides a snapshot view of multiple jurisdictions, the jurisdiction risk scores associated with the multiple jurisdictions, and a list of those factors and corresponding weights that are used to determine the jurisdiction risk scores. Thus, a jurisdiction matrix 420 may aggregate information assessing inherent risk associated with an organization that operates in a jurisdiction and may move data out of that jurisdiction. Jurisdiction matrix 420 includes at least two categories of information: jurisdiction

information 422 and organization information 424. Jurisdiction information 422 includes information regarding regulatory complexity of the jurisdiction and/or the jurisdiction's penalties for failing to comply with the jurisdiction's regulations. Organization information 424 includes information regarding an organization's exposure in the jurisdiction. Organization information 424 may include, for example, the organization's volume of business activity in the jurisdiction and/or the organization's volume of data in the jurisdiction. In some embodiments, jurisdiction matrix 420 may be populated dynamically by reference to rules 410 or compiled ahead of time based on rules 410 or regulations 510. For example, in one embodiment, rules 410 are applied to jurisdiction information in a manner similar to that described with regard to action item workflow 3000 to determine whether rules exist restricting data movement in a variety of regulatory arenas but without actually analyzing individual project information to identify action items. An example jurisdiction matrix 420 is described in greater detail with regard to FIGURE 6.

Regulatory repository 500 may include any repository for storing regulations promulgated by one or more jurisdictions. In the illustrated embodiment, regulatory repository 500 stores current regulations 510 and past regulations 520. Current regulations 510 are regulations promulgated by a jurisdiction and that are either in effect or expected to be in effect in the future. Past regulations 520 are regulations once promulgated by a jurisdiction but that are no longer effective.

In some embodiments, external systems 600 may facilitate transmitting or receiving information from an organization's information systems. As one example, request forms 110a and 110b may use external systems 600 to auto-populate information fields. As another example, project snapshots 710 may include references to an organization's document management system, and external systems 600 may be used to access documents stored on the document management system. As yet another example, external systems 600 may transmit information regarding a project to other organizational software tools. As one example, external systems 600 may include an email server configured to send information regarding a project to organizational employees associated with the project.

Document management repository 700 may include any repository for storing project snapshots 710 and completion documents 720. Project snapshots 710 are data

records that archive information relating to a project, as described below. Each project snapshot 710 may be associated with a project identifier, a timestamp, and/or a snapshot identifier. Completion documents 720 are documents created during execute of an action item. Each completion document 720 may be associated with a project snapshot 710. For example, a project snapshot 710 that lists completed action items may identify the completion documents 720 that provide evidence that the action items were indeed completed. Project snapshots 710 and completion documents 720 together represent a searchable collection of organizational knowledge regarding past and current projects.

Teachings of certain embodiments recognize that archiving information relating to a project may improve organizational knowledge of project history and provide a trail for evaluators to assess the organization's compliance with jurisdictional regulations. For example, one project may be associated with multiple project snapshots 710 that allow evaluators to review the project at different points at time, such as after set periods of time or after the project or regulations change. An evaluator may review project snapshots 710 for any purpose, such as ascertaining the validity and reliability of the information contained in the project snapshots 710 or evaluating the organization's internal controls.

Returning to FIGURE 1B, information archived in project snapshots 710 may include, but is not limited to, regulations applied to the project (e.g., current regulations 510 or past regulations 520), rules applied to the project (e.g., rules 410), action items identified for the project (e.g., action items identified through action item workflow 3000), actions performed in response to the identified action items (e.g., references to completion documents 720), and other project details (e.g., project information 212, data-movement information 214, and jurisdiction 216). Project snapshots 710 may also include references identifying archived information stored elsewhere. As used throughout, references may include any identification of documents or information. As one example, project snapshots 710 may include a reference to current regulations 710 or past regulations 720 without necessarily including copies of those regulations; such references may identify the regulations and/or provide information on how to locate copies of the regulations. As another

example, project snapshots 710 may include references to completion documents 720 instead of actual copies of those documents.

Returning back to FIGURE 1, completion documents 720 represent documents created during execution of an action item. As one example, if an action item requires the organization to obtain customer consents, then completion documents 720 may include copies of the customer consents. As another example, if an action item requires the organization to enter into outsourcing agreements with third parties subject to certain terms, then completion documents 720 may include a copy of the outsourcing agreements. Teachings of certain embodiments recognize that storing completion documents 720 may allow an evaluator to efficiently assess the organization's compliance with regulations 510. Teachings of certain embodiments also recognize that completion documents 720 may be reused in future projects. For example, if an action item requires the organization to obtain customer consents, a future project may reuse some or all of the stored customer consent documents if facing a similar action item. For example, if the customer consents include language requested by a jurisdiction, then future customer consents used in that jurisdiction may reuse the that language.

A project may be associated with multiple project snapshots 710. For example, a project snapshot 710 may be stored every time a project is updated. Update events may include, but are not limited to, times when action items are identified, when action items are completed, when action items are changed, when regulations or rules have changed, and when any other project information has changed. As one example, if a project is directed to moving data out of a first jurisdiction, a first project snapshot 710 may include a reference to current regulation 510. If the referenced current regulation 510 is replaced with a new regulation, the current regulation 510 may be stored as a past regulation 520, and the new regulation may be stored as a current regulation 510. The first project snapshot 710 would then have a reference to the stored past regulation 520, and a second project snapshot 710 would have a reference to the new current regulation 510.

In operation, according to one embodiment, request forms 110a and 110b are prepared. A user 50 may complete request forms 110a and 110b by providing project information 212, data-movement information 214, and jurisdiction information 216,

which may then be stored in a project file 210 on request repository 200. Project files may be organized in a queue 215, and a user 50 may review and prioritize the project files 210 before projects proceed to workflow manager 300. Workflow manager 300 selects a project from project file 210 and receives T-P-J information 220. Using this T-P-J information 220, workflow manager 300 may initiate different workflows. Risk workflow 2000 may populate jurisdiction matrix 420 to calculate jurisdictional risk and project risk based on the organization and the jurisdictions identified by jurisdiction information 216. Action item workflow 3000 may apply rules 410 to the T-P-J information 220 to identify action items required for the project to comply with each jurisdiction's regulations. Update workflow 4000 may update rules 410 and/or action items for the project in response to changes to the jurisdiction's regulations or changes to the T-P-J information 220. Identified action items may be reviewed and validated by a user 50 to ensure they accurately represent the governing regulations. Document management repository 700 may store project snapshots 710, which archive changes and developments to the projects.

FIGURE 2 shows risk workflow 2000 according to one embodiment. FIGURE 3 shows action item workflow 3000 according to one embodiment. FIGURE 4 shows update workflow 4000 according to one embodiment. Workflows 2000, 3000, and 4000 are described with reference to an example data-movement project. The example data-movement project includes an organization's request to move data out of an example Jurisdiction A and an example Jurisdiction B. Workflows 2000, 3000, and 4000 are also described with reference to FIGURES 6-8.

According to one embodiment, workflow 2000 may assess jurisdictional risk and project risk associated with a project that involves moving first data from a first jurisdiction and second data from a second jurisdiction. Jurisdictional risk may approximately express the inherent risk associated with moving data out of a jurisdiction. Project risk may approximately express the inherent risk associated with moving data out of each of the jurisdictions identified in the project.

Risk workflow 2000 starts at step 2100. At step 2200, jurisdiction information 216 is received. In this example, jurisdiction information 216 identifies Jurisdiction A and Jurisdiction B. At step 2300, the complexity of the regulations of Jurisdiction A and Jurisdiction B is determined. In this example, jurisdiction matrix 6000 of

FIGURES 6A-6B may be used to determine regulatory complexity. FIGURES 6A-6B will be described in the following paragraphs.

FIGURES 6A-6B shows jurisdictional matrix 6000 according to one embodiment. Jurisdictional matrix 6000 represents one example of the jurisdictional matrix 420 of FIGURE 1. In this example embodiment, jurisdictional matrix 6000 includes rows of jurisdictions 6100 and columns of matrix factors 6200. Example jurisdictions 6100 include Jurisdiction A and Jurisdiction B.

Example matrix factors 6200 include regulatory information 6210, regulatory oversight factors 6220, data volume factors 6230, and business criticality factors 6240. Regulatory information 6210 identify whether each jurisdiction 6100 restricts movement of data in the areas of data privacy, secrecy, and outsourcing. Example regulatory information 6210 include requirements related to the regulatory areas of data privacy, data secrecy, and outsourcing.

Regulatory oversight factors 6220 identify the regulatory activity of each jurisdiction 6100 and the penalties that may be incurred for failing to obey regulations of each jurisdiction 6100. Example regulatory oversight factors 6220 include the civil and criminal penalties for failure to comply with data movement regulations and the activity level of the jurisdiction's regulatory body. For example, a jurisdiction that requires many regulatory filings and has an enforcement division may increase the chances that an organization would be prosecuted for failure to comply as compared to a jurisdiction that has a passive regulatory structure.

Data volume factors 6230 assess the volume of an organization's data within each jurisdiction. Example data volume factors 6230 may include the number of data centers located in a jurisdiction, whether there are any large-volume data operations in the jurisdiction, and whether the organization considers the jurisdiction to be a "critical outsourcing location." Business criticality factors 6240 assess the criticality of the jurisdiction to the organization's overall business. Example business criticality factors 6240 may include the number of lines of business the organization has in the jurisdiction, the organization's revenue attributable to activities in the jurisdiction, and whether the organization is considering new market entry or expansion into the jurisdiction.

Jurisdictional matrix 6000 also includes weights 6300. Weights 6300 define a relative value for each matrix factor 6200. As one example, acquiring customer consent may be more complex than providing customer notification; accordingly, the weight assigned to the customer consent regulatory information 6210 is higher than the weight assigned to the customer notification regulatory information 6210. Applying weights 6300 to regulatory information 6210, regulatory oversight factors 6220, data volume factors 6230, and business criticality factors 6240 yield corresponding regulatory information scores 6410, regulatory oversight scores 6420, data volume scores 6430, and business criticality scores 6440, as shown in FIGURE 6. Additionally, in this example, regulatory information scores 6410 may be added to yield an overall regulatory information score 6510; regulatory oversight scores 6420 may be added to yield overall regulatory oversight score 6520; data volume scores 6430 may be added to yield overall data volume score 6530; and business criticality scores 6440 may be added to yield overall business criticality score 6540.

In addition, for each jurisdiction, the regulatory information scores 6410, regulatory oversight scores 6420, data volume scores 6430, and business criticality scores 6440 may be added to yield a jurisdiction risk score 6600. Teachings of certain embodiments recognize that a jurisdiction risk score 6600 may approximately express the inherent risk associated with moving data out of a jurisdiction. In this example, a higher jurisdiction risk score 6600 indicates that a jurisdiction has a highly complex regulatory structure and/or the organization's exposure in the jurisdiction is high. Teachings of certain embodiments recognize that a quantitative expression of inherent risk may allow an organization to appropriately allocate resources towards minimizing the organization's risk in that jurisdiction.

In one embodiment, the jurisdiction risk scores 6600 identified in jurisdictional matrix 6000 may be compared to a break value, set at 255 in the exemplary jurisdictional matrix 6000. The break value represents a threshold that may be used to classify the jurisdictional risk scores 6600 as either high or low. Although the break value in this example is set at 255, teachings of certain embodiments recognize that the break value may be set to any suitable value. As one example, the break value may be set at the median or mean of all jurisdiction risk

scores 6600. In some example embodiments, multiple threshold values may be used to categorize jurisdictional risk scores 6600 into different tiers.

Returning to risk workflow 2000 of FIGURE 2, step 2300 may include steps 2310 and 2320. At step 2310, weights 6300 may be applied to regulatory information 6210 to yield regulatory information scores 6310 and overall regulatory information score 6410. In one example, the regulatory information 6210 include “yes” or “no” answers, with a “yes” answer having a value of 1 and a “no” answer having a value of 0. In this example, applying weights 6300 to the regulatory information 6210 converts the yes/no answers into numerical values that express both the existence of a factor in a jurisdiction and the importance of that factor as compared to the other factors.

At step 2320, weights 6300 may be applied to regulatory oversight factors 6220 to yield regulatory oversight scores 6320 and overall regulatory oversight score 6420. In one example, the regulatory oversight factors 6220 include “yes” or “no” answers, with a “yes” answer having a value of 1 and a “no” answer having a value of 0. In this example, applying weights 6300 to the regulatory oversight factors 6220 converts the yes/no answers into numerical values that express both the existence of a factor in a jurisdiction and the importance of that factor as compared to the other factors.

At step 2400, the organization’s exposure in Jurisdiction A and Jurisdiction B may be determined. In this example, step 2400 may include steps 2410 and 2420. At step 2410, weights 6300 may be applied to data volume factors 6230 to yield data volume scores 6330 and overall data volume score 6430. In one example, the to data volume factors 6230 include “yes” or “no” answers, with a “yes” answer having a value of 1 and a “no” answer having a value of 0. In this example, applying weights 6300 to the to data volume factors 6230 converts the yes/no answers into numerical values that express both the existence of a factor in a jurisdiction and the importance of that factor as compared to the other factors.

At step 2420, weights 6300 may be applied to business criticality factors 6240 to yield business criticality scores 6340 and overall business criticality score 6440. In one example, the business criticality factors 6240 include “yes” or “no” answers, with a “yes” answer having a value of 1 and a “no” answer having a value of 0. In this

example, applying weights 6300 to the business criticality factors 6240 converts the yes/no answers into numerical values that express both the existence of a factor in a jurisdiction and the importance of that factor as compared to the other factors.

At step 2500, jurisdiction risk scores 6600 for Jurisdiction A and Jurisdiction
5 B may be determined. As explained above, a jurisdiction risk score 6600 may approximately express the inherent risk associated with moving data out of a jurisdiction. In this example, jurisdiction risk score 6600 may be determined by adding regulatory information scores 6410, regulatory oversight scores 6420, data volume scores 6430, and business criticality scores 6440, as shown in FIGURE 6.

10 At step 2600, a project risk score 6700 may be determined. Teachings of certain embodiments recognize that a project risk score 6700 may approximately express the inherent risk associated with moving data out of each of the jurisdictions identified in the project. In this example, a higher project risk score 6700 indicates that the project includes a large number of jurisdictions with a highly complex
15 regulatory structure and/or a large number of jurisdictions where the organization's exposure is high. Teachings of certain embodiments recognize that a quantitative expression of inherent risk may allow an organization to appropriately allocate resources towards minimizing the organization's risk associated with that project.

An example project risk score 6700 is shown by reference to example project
20 summary 120, as shown in FIGURE 8. Project summary 120 identifies different jurisdictional and organizational risk factors 6710 and counts the number of jurisdictions that have a high, medium, or low value for each risk factor. In the embodiment shown in FIGURE 8, the example jurisdictional and organizational risk factors 6710 include overall regulatory information score 6410, overall data volume
25 score 6430, overall business criticality score 6440, and weighed revenue factor score (selected from among the business criticality scores 6440). In this example, the project risk score 6700 is calculated as a function of the number of jurisdictions that have a high, medium, or low value for each of the identified jurisdictional and organizational risk factors 6710. In one example embodiment, the project risk score
30 6700 is calculated by applying weights to the totals of high, medium, and low values and then added to yield a composite score. The example project summary 120 of FIGURE 8 will be described in greater detail below.

FIGURE 3 shows action item workflow 3000 according to one embodiment. Action item workflow 3000 may determine restrictions on moving data from one or more jurisdictions. In some embodiments, workflow 3000 may identify action items in an effort to reduce risk associated with moving data out of a jurisdiction. For example, if a jurisdiction has a high inherent risk or a project has a high inherent risk, identifying and completing action items may mitigate inherent risk. In addition, workflow 3000 may provide a structured mechanism for applying regulations of a jurisdiction to a project and may reduce the need to refer to the regulations directly through the application of rules 410.

Action item workflow 3000 starts at step 3100. At step 3200, T-P-J information 220 is received. In this example, T-P-J information 220 identifies a request to move personally identifiable information (PII) out of Jurisdiction A. At step 3300, a set of data rules 410 are identified based on the T-P-J information 220. In this example, data rules 410 corresponding to Jurisdiction A regulations concerning data privacy are identified because the T-P-J information 220 identified Jurisdiction A and an intent to move PII data. The identified data rules 410 may include if/then/else scenarios developed from regulations of Jurisdiction A related to data privacy that identify whether and/or how the Jurisdiction A restricts movement of PII data out of a jurisdiction. In different embodiments, the identified data rules 410 may include all regulations of Jurisdiction A related to data privacy or a subset. As one example, the identified data rules 410 may include initial rules that, when applied, will lead to other rules and action items. At step 3400, the identified data rules 410 are applied against the request. FIGURE 7A shows an example decision grid 415a for applying rules 410 to the request at step 3400 according to one embodiment. FIGURE 7A will be described in the following paragraph.

FIGURE 7A shows an example decision grid 415a. Decision grid 415a illustrates one example method for applying rules 410. Applying rule 1.0 to the T-P-J information 220 reveals that data privacy “regulatory restrictions [are] present” and that “specific restrictions” should be determined at rule 2.0. Applying rule 2.0 to the T-P-J information 220 reveals that “sensitive data elements” are involved, as that term is defined under the regulations of Jurisdiction A, and that the “sensitive data elements” should be determined at rule 2.1. Applying the rule 2.1 to the T-P-J

information 220 reveals that “sensitive data elements are present in the project request” and that “regulatory compliance requirements” should be determined at rule 2.2. Applying the rule 2.2 reveals that “compliance requirements exist” and should be defined at rule 2.2a. Applying the rule 2.2a reveals that “customer notice [is] required” and that the organization should complete an action item: “deliver customer notice.”

Returning to action item workflow 3000 of FIGURE 3, step 3400 answered whether the request is allowed under the regulations of Jurisdiction A and what action items may facilitate compliance. In the example of FIGURE 7A, decision grid 415a revealed that the requested data movement is allowed if customer notice is delivered.

At step 3500, the answer produced at step 3400 is analyzed to determine whether the rules 410 allow the requested data movement under any circumstances. In this example, the requested data movement is allowed if customer notice is delivered, so the action item workflow 3000 proceeds to step 3600. However, if the requested data movement had been prohibited in all circumstances, a response denying the request may be generated at step 3510. The response may be provided in any suitable form. In one example, a project summary 120 may indicate that the requested data movement is denied under any circumstances. In another example, external systems 600 may generate an email alerting the organization that the requested data movement is denied under any circumstances.

At step 3600, the answer produced at step 3400 is analyzed to determine whether the rules 410 require action items to be completed for compliance. In this example, the rules 410 require the organization to deliver customer notice to those customers required by the jurisdiction, so the action item workflow 3000 proceeds to step 3700. However, if the requested data movement had been allowed in all circumstances, a response allowing the request may be generated at step 3610.

At step 3700, the request and the action item are stored. In one example, the action item is stored as part of results 218. In another example, a project snapshot 710 is generated and records the request and the action item. In some embodiments, the results 218 and/or project snapshot 710 may be updated to record that the action item is completed. In this example, when the organization delivers the required customer notification, results 218 may be updated, project snapshot 710 may be updated, and

copies of the customer notices may be stored at the document management repository as completion documents 720. A response reporting that the requested data movement is allowed subject to an action item may also be generated.

5 Teachings of certain embodiments recognize the capability to include verification steps to ensure that the identified action items accurately reflect the requirements of the governing regulations. As one example, a review board may determine whether a project will comply with each jurisdiction's regulations once the action items are completed. As an organization validates action items for projects over time, the organization may develop confidence that the action items and
10 associated rules accurately reflect the governing regulations. Accordingly, teachings of certain embodiments recognize the capability to validate action items without submitting the action items for human review. For example, when an action item is generated, the request repository 200 may be searched for project records 210 that include similar action items. In one example, two action items may be considered
15 similar if they require the organization to perform the same steps but to different data sets. If the search of request repository 200 reveals a similar action item that has been verified, in some embodiments the new generated action item may be deemed verified without human review. In an alternative embodiment, a new generated action item may be deemed verified without human review if searching the request repository 200
20 revealed a sufficient number of similar action items that have been verified (e.g., ten or more).

FIGURE 4 shows update workflow 4000 according to one embodiment. Update workflow 4000 may update jurisdictional information for a project that involves moving data from a first jurisdiction. For example, action items may change
25 over time due to changes in project information and/or changes in jurisdictional regulations. Teachings of certain embodiments recognize that update workflow 4000 may provide a structured mechanism for updating, adding, and removing action items through the application of rules 410 against existing projects and action items. Thus, workflow 4000 may update those actions that the organization should complete to
30 maintain compliance with governing regulations.

Update workflow 4000 starts at step 4100. At step 4200, T-P-J information 220 and an associated action item are stored. In this example, T-P-J information 220

identifies a request to move personally identifiable information (PII) out of Jurisdiction A, and the associated action item requires the organization to provide customer notice, as identified by the decision grid 415a of FIGURE 7A.

At step 4300, an update to the T-P-J information 220 or the rules 410
5 corresponding to Jurisdiction A is received. In this example, the update is to rules 410: as part of the update, Jurisdiction A now requires “customer consent” instead of “customer notice.” Accordingly, in this example, step 4450 requires that update workflow 4000 proceed to step 4550. At step 4550, projects that involve moving data out of Jurisdiction A are identified. In this example, request repository 200 and/or
10 document management repository 700 are searched to identify the T-P-J information 220 and action item stored at step 4200. At step 4650, the update to rules 410 are applied against the request. FIGURE 7B shows an example method for applying updated rules 410 to the request at step 4650 according to one embodiment. FIGURE 7B will be described in the following paragraph.

FIGURE 7B shows an example decision grid 415b. Decision grid 415b
15 proceeds to rule 2.2a similar to the decision grid 415a of FIGURE 7A. However, rule 2.2a of decision grid 415b is different from rule 2.2a of decision grid 415a. Applying rule 2.2a reveals that “customer consent” is required and that the organization should “validate [that] customer consent is on file.” If the “customer consent” is not on file,
20 decision grid 415b proceeds to rule 2.2b, which identifies a new action item: “obtain customer consent.” If “customer consent” is on file, decision grid 415b proceeds to rule 2.3. Applying rule 2.3 once “customer consent” is obtained reveals another action item: “obtain regulatory notification.” Once “regulatory notification” is obtained, decision grid 415b proceeds to rule 2.4, which identifies another action
25 item: “file regulatory notification with XYZ regulator.” Once the “regulatory notification” is filed, decision grid 415b ends.

Returning to update workflow 4000 of FIGURE 4, step 4650 answered whether the request is allowed under the updated regulations of Jurisdiction A and what action items may be required for compliance. At step 4750, the request and the
30 updated action items are stored. In one example, the updated action items are stored as part of results 218. In another example, a project snapshot 710 is generated and records the request and the action items; this second snapshot 710 may be in addition

to any project snapshot 710 generated at step 3700 of the action item workflow of FIGURE 3.

Returning to step 4300 of update workflow 4000, if the received update is an update to T-P-J information 220, then step 4400 would indicate that the update workflow 4000 proceed to step 4500. At step 4500, a set of data rules 410 are identified in a manner similar to that described above with regard to step 3300 of action item workflow 3000. At step 4600, the identified data rules 410 are applied against the updated request in a manner similar to that described above with regard to step 3400 of action item workflow 3000. At step 4700, the request and the action item are stored in a manner similar to that described above with regard to step 3700 of action item workflow 3000 and/or step 4750 of update workflow 4000.

FIGURES 5A-5D show example request forms 110a and 110b according to one embodiment. In the illustrated example, request forms 110a and 110b include intake form 110a and assessment form 110b. Together, request forms 110a and 110b include several fields for receiving project information, including project information 212, data movement information 214, and jurisdiction information 216. As one example, data movement information 214 may be derived in part from the identified “purpose of using the above mentioned data” in Question 6 of intake form 110a. In this example, the purpose information may be included in T-P-J information 220.

FIGURE 8 shows an example project summary 120 according to one embodiment. As explained above, project summary 120 may display project risk score 6700 and organizational risk factors 6710. Project summary 120 may also show action item summary information. For example, FIGURE 8 shows action item summary information derived from decision grid 415b. In this example, Jurisdiction A included a data privacy regulation requirement that “regulatory notification be filed with XYZ regulation.” According to this example project summary 120, the task of filing the regulatory notification has been assigned within the organization to “Mr. Person,” and Mr. Person has one month to complete the task. The example project summary 120 also includes high, medium, and low values derived from the overall regulatory information score 6510, the overall regulatory oversight score 6520, the overall data volume score 6530, and the overall business criticality score 6540 of

FIGURE 6. As explained above, these high, medium, and low values may be derived by comparing each score to one or more threshold values.

In some embodiments, updates to a project may yield new and/or updated project summaries 120. Update events may include, but are not limited to, times when action items are identified, when action items are completed, when action items are changed, when regulations or rules have changed, and when any other project information has changed. As one example, if updated action items are identified through update workflow 4000, the updated action items may be shown on updated project summaries 120. As another example, if Jurisdiction A changes their regulatory requirements, the changes may result in different values for: the project risk score 6700; the organizational risk factors 6710; the identified action items; and/or the high, medium, and low values derived from the overall regulatory information score 6510, the overall regulatory oversight score 6520, the overall data volume score 6530, and the overall business criticality score 6540 of FIGURE 6.

Modifications, additions, or omissions may be made to the systems and apparatuses described herein without departing from the scope of the invention. The components of the systems and apparatuses may be integrated or separated. Moreover, the operations of the systems and apparatuses may be performed by more, fewer, or other components. The methods may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order. Additionally, operations of the systems and apparatuses may be performed using any suitable logic. As used in this document, "each" refers to each member of a set or each member of a subset of a set.

Although several embodiments have been illustrated and described in detail, it will be recognized that substitutions and alterations are possible without departing from the spirit and scope of the present invention, as defined by the appended claims.

To aid the Patent Office, and any readers of any patent issued on this application in interpreting the claims appended hereto, applicants wish to note that they do not intend any of the appended claims to invoke paragraph 6 of 35 U.S.C. § 112 as it exists on the date of filing hereof unless the words "means for" or "step for" are explicitly used in the particular claim.

WHAT IS CLAIMED IS:

1. A data movement system for assessing inherent risk associated with a project that involves moving first data from a first jurisdiction and second data from a second jurisdiction, wherein the first jurisdiction and the second jurisdiction each have corresponding regulations that restrict the movement of data out of that jurisdiction, the system comprising:

a rules repository configured to store rules associated with the regulations of the first jurisdiction and the regulations of the second jurisdiction; and

a workflow manager configured to:

determine jurisdictional complexity of the project as a function of the regulations of the first jurisdiction and the second jurisdiction, wherein at least some portion of the regulations involve data privacy, data secrecy, and data outsourcing;

determine jurisdictional exposure of the project as a function of an organization's exposure to the first jurisdiction and the second jurisdiction, wherein at least some portion of the organization's exposure involves the organization's volume of business activity in the first jurisdiction and in the second jurisdiction; and

determine the risk of the project as a function of the jurisdictional complexity of the project and the jurisdictional exposure of the project.

2. The data movement system of Claim 1, wherein:

the first jurisdiction and the second jurisdiction comprise two of a plurality of jurisdictions associated with the project; and

the workflow manager is configured to determine the risk of the project by:

determining a number of the plurality of jurisdictions that have a high jurisdictional complexity,

determining a number of the plurality of jurisdictions that have a low jurisdictional complexity,

determining a number of the plurality of jurisdictions that have a high jurisdictional exposure,

5 determining a number of the plurality of jurisdictions that have a low jurisdictional exposure, and

10 determining the risk of the project as a function of the number of jurisdictions that have a high jurisdictional complexity, the number of the plurality of jurisdictions that have a low jurisdictional complexity, the number of the plurality of jurisdictions that have a high jurisdictional exposure, and the number of the plurality of jurisdictions that have a low jurisdictional exposure.

3. The data movement system of Claim 2, wherein:

15 the workflow manager is configured to determine the number of plurality of jurisdictions that have a high jurisdictional complexity by:

identifying a complexity number for each of the plurality of jurisdictions, each complexity number representing complexity of one of the plurality of jurisdictions,

20 identifying a break value, the break value defining a number above which complexity numbers are deemed high, and

counting the number of complexity numbers higher than the break value; and

25 the workflow manager is configured to determine the number of plurality of jurisdictions that have a low jurisdictional complexity by counting the number of complexity numbers lower than the break value.

4. The data movement system of Claim 1, wherein the jurisdictional complexity of the project is a function of the first jurisdiction's extent of regulatory oversight and a function of the second jurisdiction's extent of regulatory oversight.

5 5. The data movement system of Claim 1, wherein the jurisdictional exposure of the project is a function of a volume of data that is stored in the first jurisdiction and a volume of data that is stored in the second jurisdiction.

10 6. The data movement system of Claim 1, wherein the jurisdictional exposure of the project is a function of a criticality of the first jurisdiction to the organization and a function of a criticality of the second jurisdiction to the organization.

15 7. The data movement system of Claim 1, wherein the jurisdictional exposure of the project is a function of the organization's revenues attributable to the organization's activities in the first jurisdiction and the second jurisdiction.

8. The data movement system of Claim 1, wherein the jurisdictional exposure of the project is a function of:
20 potential civil damages for failing to comply with the regulations, and
potential criminal penalties for failing to comply with the regulations.

9. A risk assessment computer for assessing inherent risk associated with a project that involves moving first data from a first jurisdiction and second data from
25 a second jurisdiction, wherein the first jurisdiction and the second jurisdiction each

have corresponding regulations that restrict the movement of data out of that jurisdiction, the system comprising:

a processor configured to:

5 determine jurisdictional complexity of the project as a function of the regulations of the first jurisdiction and the second jurisdiction, wherein at least some portion of the regulations involve data privacy, data secrecy, and data outsourcing;

10 determine jurisdictional exposure of the project as a function of an organization's exposure to the first jurisdiction and the second jurisdiction, wherein at least some portion of the organization's exposure involves the organization's volume of business activity in the first jurisdiction and in the second jurisdiction; and

 determine the risk of the project as a function of the jurisdictional complexity of the project and the jurisdictional exposure of the project; and

15 a memory configured to store:

 a quantitative value representing the risk of the project.

10. The risk assessment computer of Claim 9, wherein:

20 the first jurisdiction and the second jurisdiction comprise two of a plurality of jurisdictions associated with the project; and

 the processor is configured to determine the risk of the project by:

 determining a number of the plurality of jurisdictions that have a high jurisdictional complexity,

25 determining a number of the plurality of jurisdictions that have a low jurisdictional complexity,

determining a number of the plurality of jurisdictions that have a high jurisdictional exposure,

determining a number of the plurality of jurisdictions that have a low jurisdictional exposure, and

5 determining the risk of the project as a function of the number of jurisdictions that have a high jurisdictional complexity, the number of the plurality of jurisdictions that have a low jurisdictional complexity, the number of the plurality of jurisdictions that have a high jurisdictional exposure, and
10 the number of the plurality of jurisdictions that have a low jurisdictional exposure.

11. The risk assessment computer of Claim 10, wherein:

the processor is configured to determine the number of plurality of jurisdictions that have a high jurisdictional complexity by:

15 identifying a complexity number for each of the plurality of jurisdictions, each complexity number representing complexity of one of the plurality of jurisdictions,

identifying a break value, the break value defining a number above which complexity numbers are deemed high, and

20 counting the number of complexity numbers higher than the break value; and

the processor is configured to determine the number of plurality of jurisdictions that have a low jurisdictional complexity by counting the number of complexity numbers lower than the break value.

12. The risk assessment computer of Claim 9, wherein the jurisdictional complexity of the project is a function of the first jurisdiction's extent of regulatory oversight and a function of the second jurisdiction's extent of regulatory oversight.

5 13. The risk assessment computer of Claim 9, wherein the jurisdictional exposure of the project is a function of a volume of data that is stored in the first jurisdiction and a volume of data that is stored in the second jurisdiction.

10 14. The risk assessment computer of Claim 9, wherein the jurisdictional exposure of the project is a function of a criticality of the first jurisdiction to the organization and a function of a criticality of the second jurisdiction to the organization.

15 15. A method for assessing risk for a project that involves moving first data from a first jurisdiction and second data from a second jurisdiction, wherein the first jurisdiction and the second jurisdiction each have corresponding regulations that restrict the movement of data out of that jurisdiction, the method comprising:

20 determining jurisdictional complexity of the project as a function of the regulations of the first jurisdiction and the second jurisdiction, wherein at least some portion of the regulations involve data privacy, data secrecy, and data outsourcing;

determining jurisdictional exposure of the project as a function of an organization's exposure to the first jurisdiction and the second jurisdiction, wherein at least some portion of the organization's exposure involves the organization's volume of business activity in the first jurisdiction and in the second jurisdiction;

25 determining the risk of the project as a function of the jurisdictional complexity of the project and the jurisdictional exposure of the project.

16. The method of Claim 15, wherein:

the first jurisdiction and the second jurisdiction comprise two of a plurality of jurisdictions associated with the project; and

determining the risk of the project comprises:

5 determining a number of the plurality of jurisdictions that have a high jurisdictional complexity,

determining a number of the plurality of jurisdictions that have a low jurisdictional complexity,

10 determining a number of the plurality of jurisdictions that have a high jurisdictional exposure,

determining a number of the plurality of jurisdictions that have a low jurisdictional exposure, and

15 determining the risk of the project as a function of the number of jurisdictions that have a high jurisdictional complexity, the number of the plurality of jurisdictions that have a low jurisdictional complexity, the number of the plurality of jurisdictions that have a high jurisdictional exposure, and the number of the plurality of jurisdictions that have a low jurisdictional exposure.

20 17. The method of Claim 16, wherein:

determining the number of plurality of jurisdictions that have a high jurisdictional complexity comprises:

25 identifying a complexity number for each of the plurality of jurisdictions, each complexity number representing complexity of one of the plurality of jurisdictions,

identifying a break value, the break value defining a number above which complexity numbers are deemed high, and

counting the number of complexity numbers higher than the break value; and

5 determining the number of plurality of jurisdictions that have a low jurisdictional complexity comprises counting the number of complexity numbers lower than the break value.

10 18. The method of Claim 15, wherein the jurisdictional complexity of the project is a function of the first jurisdiction's extent of regulatory oversight and a function of the second jurisdiction's extent of regulatory oversight.

15 19. The method of Claim 15, wherein the jurisdictional exposure of the project is a function of a volume of data that is stored in the first jurisdiction and a volume of data that is stored in the second jurisdiction.

20 20. The method of Claim 15, wherein the jurisdictional exposure of the project is a function of a criticality of the first jurisdiction to the organization and a function of a criticality of the second jurisdiction to the organization.

1/14

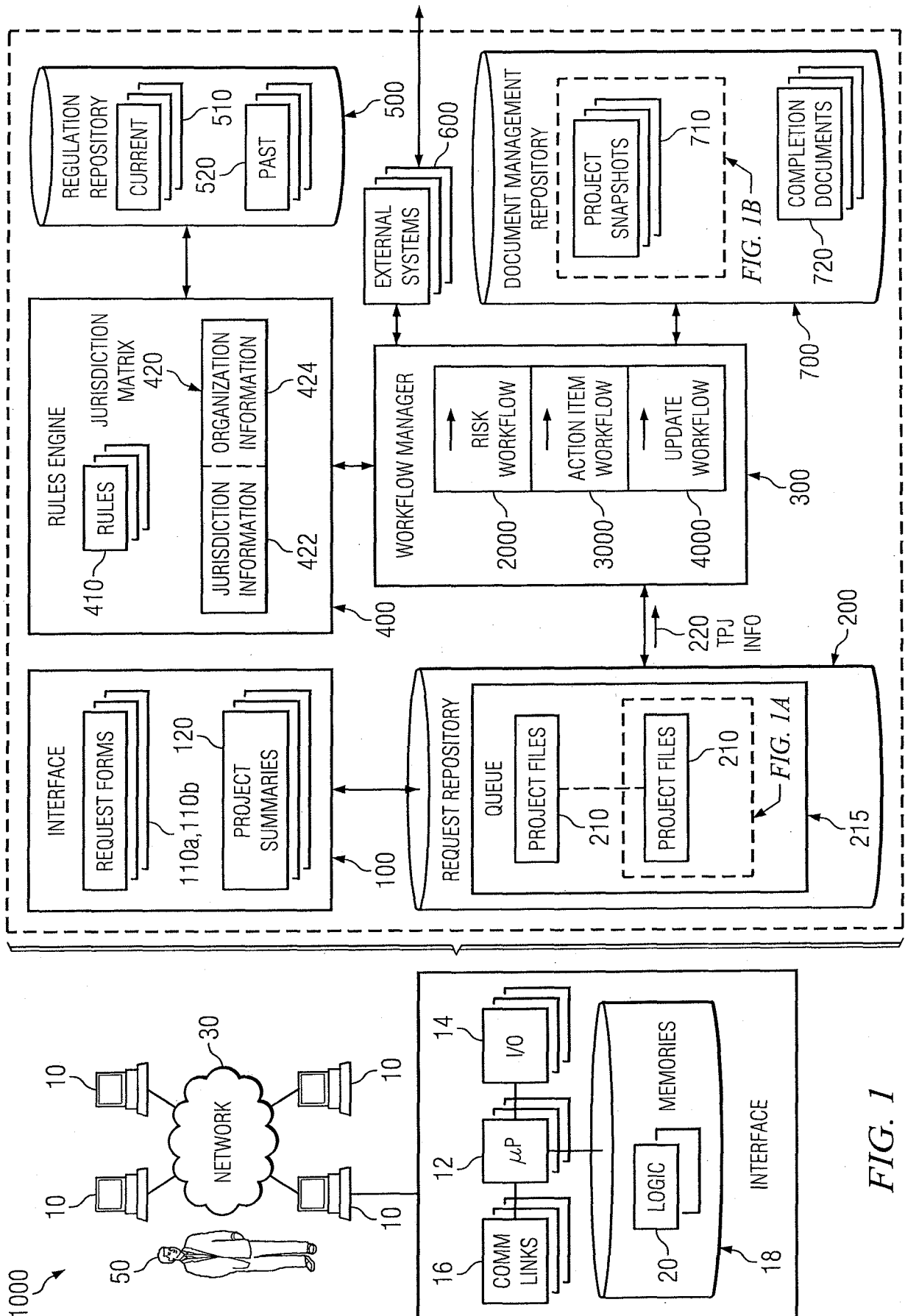
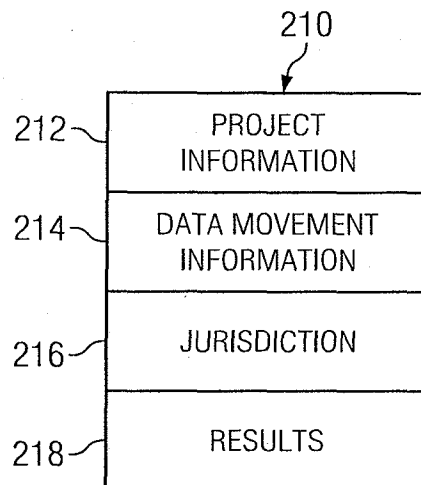
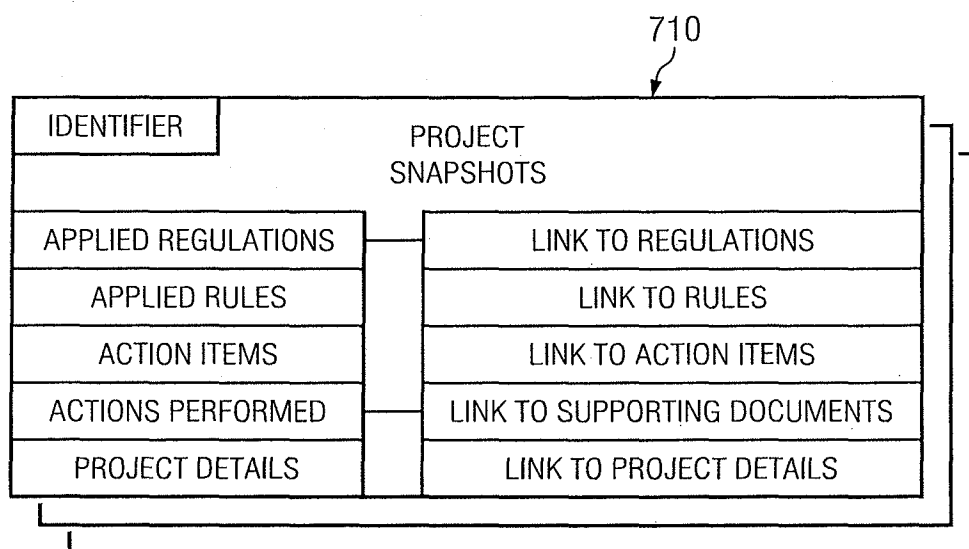


FIG. 1

2/14

*FIG. 1A**FIG. 1B*

3/14

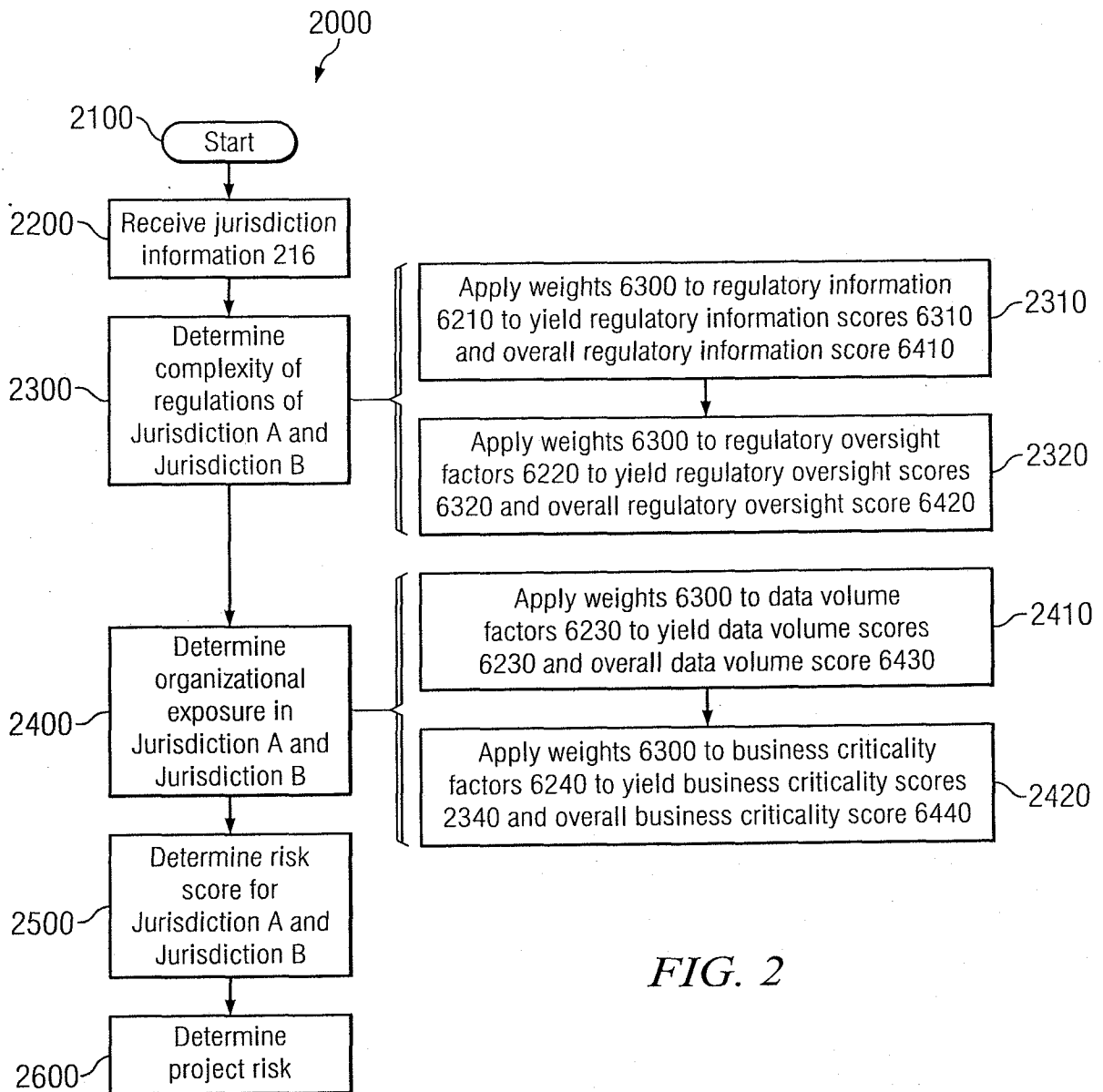


FIG. 2

4/14

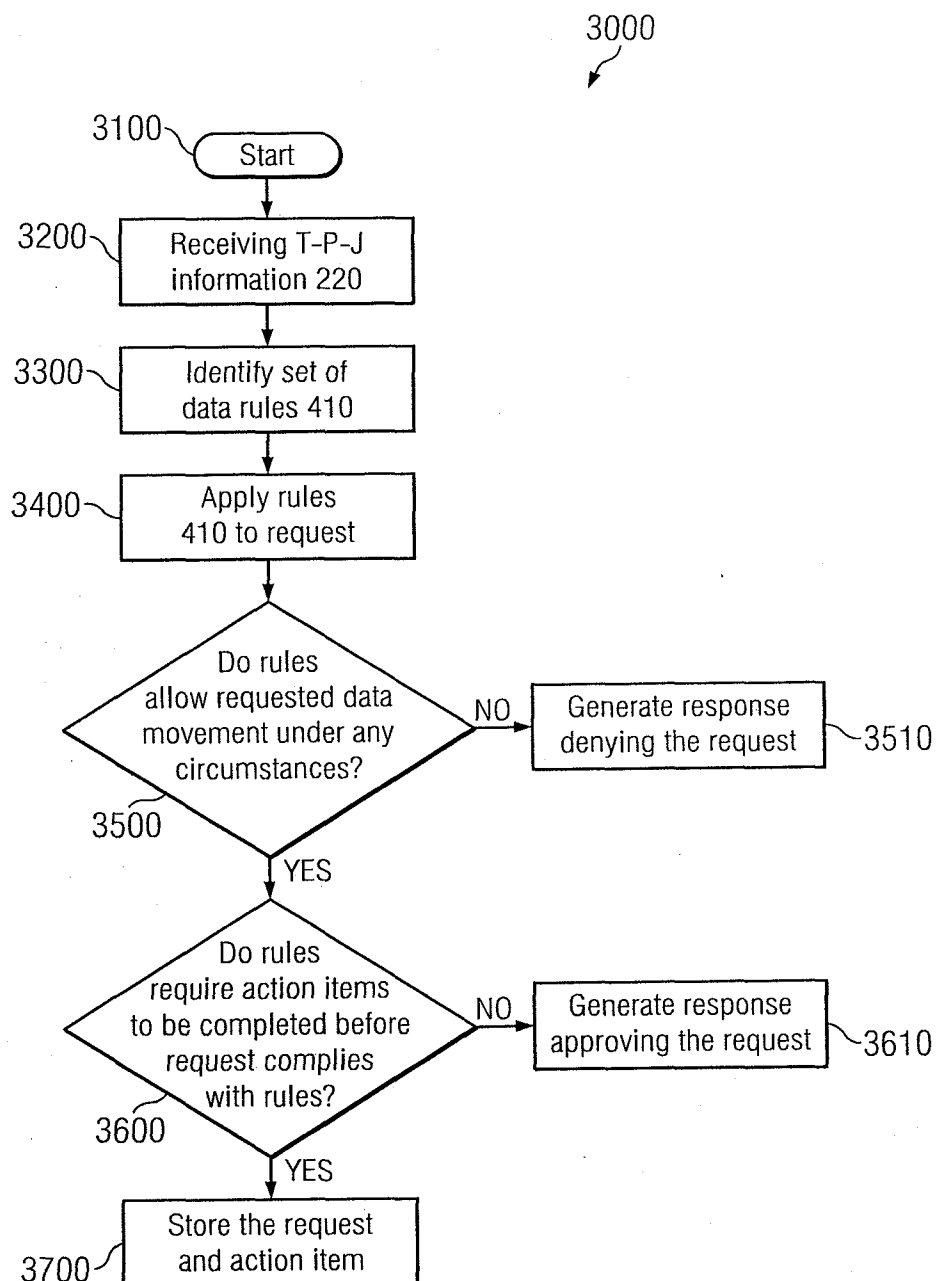


FIG. 3

5/14

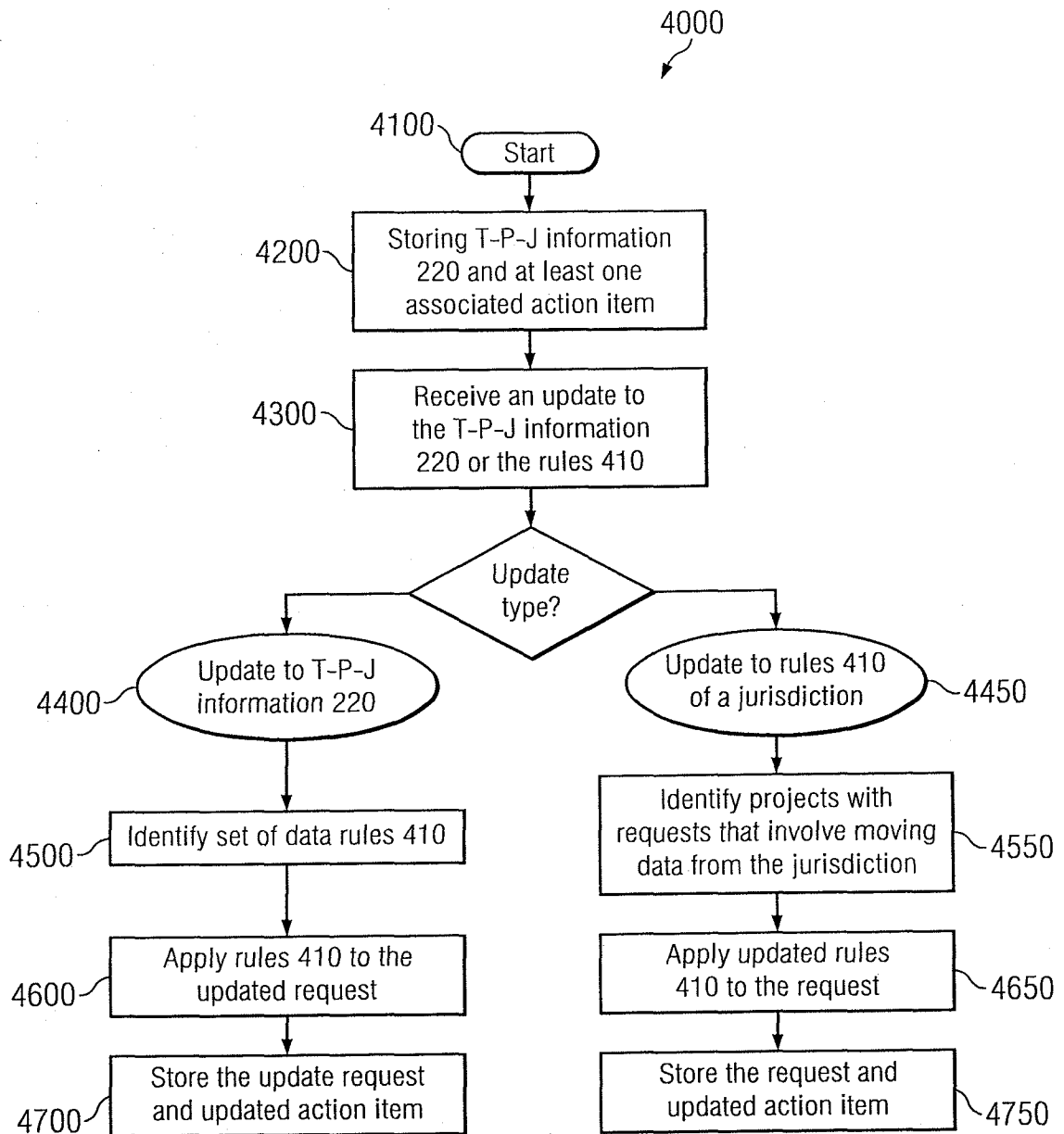


FIG. 4

Standard Questions		Project Responses	
Q1	Confirm information on the registration form	Complete	
Q2	Can you tell me more information about the project? (Review project charter, what capabilities will it enable etc)		
Q3	Lets discuss business drivers. Why are we doing this? What capabilities will this enable for the business? Are we doing this already? If we are - are we enabling new countries, new functionality or both?		
Q4	Can you walk me through the timeline of the project? Is this part of a multi-generational plan? When did the business case get approved? Have you had to push your dates forward or back for any reason?		
Q5	What data elements are involved in this project? (Please be sure to discuss any and all that may apply)	Personal Data Background Data Transaction Data Government Medical Sensitive AML AML Sales Servicing Marketing Financial Reporting Fulfillment Data Storage Testing Associate Access Reporting Processing Document Storage	Customer/client specific identifiable data Individual transaction level data Any sovereign data of any type Information containing personal medical records Religious or political affiliations Trending to identify AML transactions
Q6	What is the purpose of using the above mentioned data elements?		

TO FIG. 5B

FIG. 5A

6/14

110a

FROM FIG. 5A

110a

7/14

Q7	Who will be using this data?	
Q8	How frequently will they be using this data?	
Q9	How long will they be using this data?	
Q10	Will the source and target countries be able to do what they want with the data independent of one another?	
Q11	Does one group have to instruct other groups on what needs to be done with the data?	
Q12	Have you been engaged with internal legal partners on this project?	
Q13	Have you been engaged with external counsel on this project?	
Q14	Have you been engaged with compliance or risk partners on this project?	
Q15	Is there project funding?	
Q16	Do you have funding for the use of external counsel on the project?	

ASSESSMENT SCOPING DETAIL

Business Purpose?		Controller to Controller	
Privacy Regulatory Review?		Controller to Processor	
Bank Secrecy Regulatory Review?		Banking Regulations	
Outsourcing Regulatory Review?		Securities Regulations	
All Country Requests the Same?			
If no - detail out the variability by country at a high level			

FIG. 5B

8/14

INITIAL REQUEST ASSESSMENT			
	Customer or Client Data	☐	Associate Data Request Referred to
	Data Moving within Multiple Jurisdictions	☐	
	Associate Data	☐	Date Project Notified ☐ Date Interview Scheduled ☐
(1)	Project Name		
(2)	Overview		
(3)	Requestor Name		
(4)	Requestor Phone		
(5)	Requestor Email		
(6)	Request Date		
(7)	Type		
(8)	Funded		
(9)	Clarity ID		
(10)	ECMS ID		
(11)	PCM Record		
(12)	Testing Date		
(13)	Implementation Date		
(14)	Requesting Line of Business	☐	LoB1
		☐	LoB2
		☐	LoB3
		☐	LoB4
		☐	LoB5
(15)	Project Type		
(16)	Project Phase		
(17)	Outside Counsel Review		
(18)	Project Sponsor Email		
(19)	Change Manager Email		
(20)	Technology Delivery Manager Email		
(21)	Legal Partner Email		
(22)	Compliance Partner Email		
(23)	Risk Partner Email		
(24)	Business Areas Impacted		
(25)	Related to Transition	☐	If Yes
(26)	Involve AML/KYC		
(27)	Are you aware of client contractual restrictions?		
(28)	Who can confirm these restrictions?		
(29)	Are mitigating controls in place for these restrictions?	☐	Explain

FIG. 5C

9/14

FIG. 5D

(30)	Does this project involve customer/client data of any type?		☐
(31)	Is this project subject to Banking or Securities Regulations?		☐
(32)	Source Countries	Target Countries	
	Argentina	Argentina	☐
	Australia	Australia	☐
	Austria	Austria	☐
	Bahrain	Bahrain	☐
	Belgium	Belgium	☐
	Brazil	Brazil	☐
	Canada	Canada	☐
	Cayman Islands	Cayman Islands	☐
	Chile	Chile	☐
	People's Republic Of China (PRC)	People's Republic Of China (PRC)	☐
	Columbia	Columbia	☐
	Costa Rica	Costa Rica	☐
	Czech Republic	Czech Republic	☐
	Denmark	Denmark	☐
	Finland	Finland	☐
	France	France	☐
	Germany	Germany	☐
	Greece	Greece	☐
	Hong Kong	Hong Kong	☐
	Hungary	Hungary	☐
	India	India	☐
	Indonesia	Indonesia	☐
	Ireland	Ireland	☐
	Isle of Man	Isle of Man	☐
	Israel	Israel	☐
	Italy	Italy	☐
	Japan	Japan	☐
	Jersey	Jersey	☐
	Korea	Korea	☐
	Lebanon	Lebanon	☐
	Luxembourg	Luxembourg	☐
	Malaysia	Malaysia	☐
	Mexico	Mexico	☐
	Monaco	Monaco	☐
	Netherlands	Netherlands	☐
	Norway	Norway	☐
	Panama	Panama	☐
	Philippines	Philippines	☐
	Portugal	Portugal	☐
	Romania	Romania	☐
	Russia	Russia	☐
	Saudi Arabia	Saudi Arabia	☐
	Singapore	Singapore	☐
	Slovakia	Slovakia	☐
	South Africa	South Africa	☐
	Spain	Spain	☐
	Sweden	Sweden	☐
	Switzerland	Switzerland	☐
	Taiwan	Taiwan	☐
	Thailand	Thailand	☐
	Turkey	Turkey	☐
	United Arab Emirates (inc DIFC)	United Arab Emirates (inc DIFC)	☐
	United Kingdom	United Kingdom	☐
	United States	United States	☐
	Uruguay	Uruguay	☐
	Vietnam	Vietnam	☐
	Number of Countries	Number of Countries	☐

FIG. 6A

[illegible]

TO FIG. 6B

12/14

415a

(PII = PERSONALLY IDENTIFIABLE INFORMATION/PERSONAL DATA)

RULE	JURISDICTION	RULE TYPE	ATTRIBUTE	WHEN CONDITION	THEN ACTION	ELSE/ END
1.0	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	REGULATORY RESTRICTIONS PRESENT	DETERMINE SPECIFIC RESTRICTIONS	2.0
2.0	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	SENSITIVE DATA ELEMENTS ARE INVOLVED	DEFINE SENSITIVE DATA ELEMENTS	2.1
2.1	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	SENSITIVE DATA ELEMENTS ARE PRESENT IN PROJECT REQUEST	DETERMINE REGULATORY COMPLIANCE REQUIREMENTS	2.2
2.2	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	COMPLIANCE REQUIREMENTS EXIST	DEFINE REQUIREMENTS	2.2a
2.2a	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	CUSTOMER NOTICE REQUIRED	DELIVER CUSTOMER NOTICE	END

FIG. 7A

13/14

415b

(PII= PERSONALLY IDENTIFIABLE INFORMATION/PERSONAL DATA)

RULE	JURISDICTION	RULE TYPE	ATTRIBUTE	WHEN CONDITION	THEN ACTION	ELSE/ END
1.0	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	REGULATORY RESTRICTIONS PRESENT	DETERMINE SPECIFIC RESTRICTIONS	2.0
2.0	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	SENSITIVE DATA ELEMENTS ARE INVOLVED	DEFINE SENSITIVE DATA ELEMENTS	2.1
2.1	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	SENSITIVE DATA ELEMENTS ARE PRESENT IN PROJECT REQUEST	DETERMINE REGULATORY COMPLIANCE REQUIREMENTS	2.2
2.2	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	COMPLIANCE REQUIREMENTS EXIST	DEFINE REQUIREMENTS	2.2a
2.2a	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	CUSTOMER CONSENT REQUIRED	VALIDATE CUSTOMER CONSENT IS ON FILE	YES 2.3 NO 2.2b
2.2b	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	CUSTOMER CONSENT REQUIRED	OBTAIN CUSTOMER CONSENT	2.3
2.3	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	CUSTOMER CONSENT IS ON HAND	OBTAIN REGULATORY NOTIFICATION	2.4
2.4	JURISDICTION A	DATA PRIVACY	MOVE PII DATA	REGULATORY NOTIFICATION REQUIRED	FILE WITH XYZ REGULATOR	END

FIG. 7B

120

14/14

RISK FACTORS 6710

FIG. 8

Project Name											
Project Overview											
Risk Summary											
Country Complexity		# of High Complexity		# of Low Complexity		# of "Hot" Complexity					
Data Volume		# of High Countries		# of Medium Countries		# of Low Countries					
Business Criticality		# of High Countries		# of Medium Countries		# of Low Countries					
External Factors		# of High Countries		# of Medium Countries		# of Low Countries					
Country Revenue		# of High Countries		# of Medium Countries		# of Low Countries					
Inherent Project Level Risk		6700									
Country	Regulation	Action Required	Assigned To	Completion Time	Country Complexity (H,L)	Data Volume (H,M,L)	Business Criticality (H,M,L)	External Factors (H,M,L)	Revenue (H,M,L)		
Jurisdiction A	Data Privacy	File w/ XYZ Regulator	Mr. Person	One Month	L	L	H	H	M		
.	.	.	.	.	.	.	.	.	.		
.	.	.	.	.	.	.	.	.	.		
Critical Assumptions											
Key Risks											
Critical Actions											
Recommendations											
Residual Risk	Legal Review	Compliance Review	LOB Review	Final Decision							

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2011/030431

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 10/00 (2011.01)

USPC - 705/7.28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - G06Q 10/00, 30/00, 40/00 (2011.01)

USPC - 705/38, 39, 7.28, 7.27, 7.23, 7.21, 7.34, 14.2, 26.25, 301, 405; 707/665, 748

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

USPTO WEST System (US-PGPUB; USPAT; USOCR; EPO; JPO), Google Patents, PatBase

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0100744 A1 (WU) 03 May 2007 (03.05.2007) entire document	1-20
Y	US 2010/0106645 A1 (PECKOVER) 29 April 2010 (29.04.2010) entire document	1-20
A	US 2004/0098285 A1 (BRESLIN et al) 29 May 2004 (20.05.2004) entire document	1-20
A	US 2008/0015913 A1 (COUTRNEY et al) 17 January 2008 (17.01.2008) entire document	1-20

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

17 May 2011

Date of mailing of the international search report

26 MAY 2011

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774