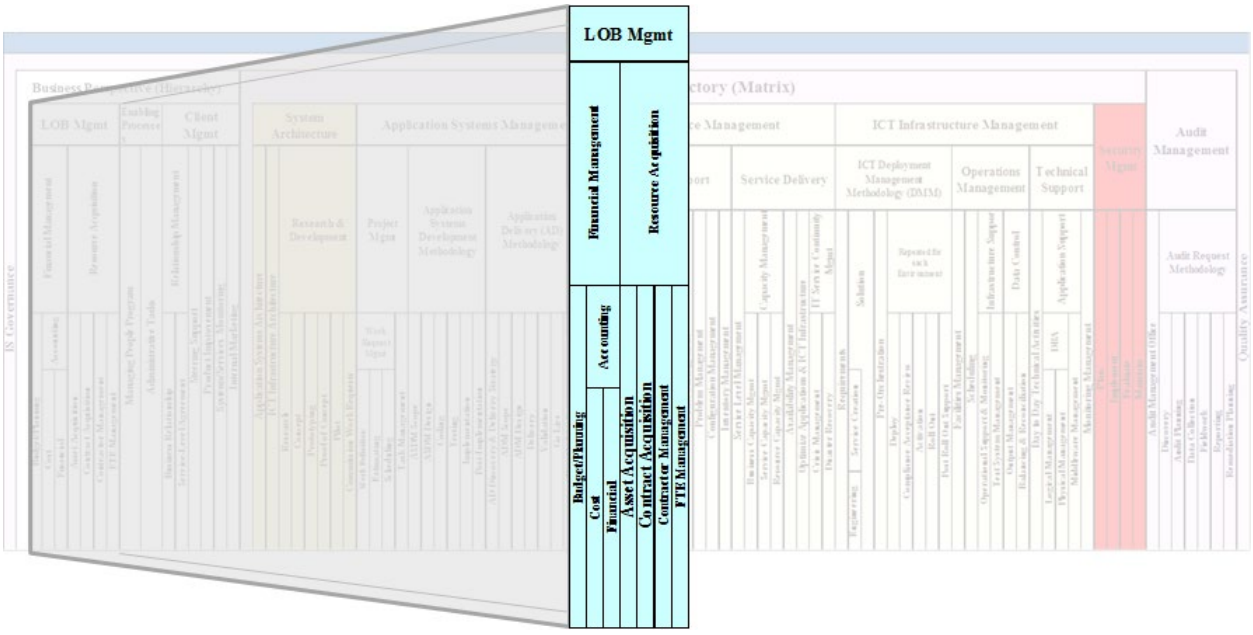
South Carolina

BlueCross BlueShield of South Carolina is an independent licensee of the Blue Cross and Blue Shield Association

imagination to Implementation

INFORMATION TECHNOLOGY

LOB Management



Information Systems Standards Manual

Table of Contents

Table of Figures

List of Tables

There are currently no tables in this volume.

Chapter 1 Line of Business Management

1.1 Line of Business Management

Management of Lines of Business (LOBs) is carried out through the LOB Manager. The LOB Manager is a selected senior I/S manager who is financially accountable for all the cost the I/S Organization expends on a given client. The LOB Manager reviews the annual budget with senior customer management ensuring there is agreement. During the year, the LOB Manager must approve additional unbudgeted expenditures for any area within the I/S organization that will be charging to a given client.

Chapter 2 Financial Management

2.1 Budgeting & Cost Control

2.1.1 Accounting and System Codes

System account codes are five (5) digit numeric fields, and system prefixes are four (4) digit alphanumeric character fields. They are used shop-wide to allocate costs for systems resource usage to the appropriate business area. Job cards use a system prefix as the first four (4) digits of the job name parameter. A system account code is the first parameter in the job card inside the parentheses.

A manager needs to initiate a system account code or system prefix add, delete, or change action by filling out a System Account Code Transmittal Form, available on the I/S Portal. (Refer to My e-Work > I/S Portal > Tools > Forms > Work Request Initiation > System Account Code Transmittal Form.). All System Account Code Transmittal Forms should be sent directly to I/S Finance via email.

New system account codes are assigned by I/S Finance and added to the Generalized Table Maintenance (GTM) "AS" table. They also manage the association of system account codes with system prefixes. Computer Operations adds new system prefixes to the CDMSP.VSYSIDNZ table.

All system prefixes also need to have corresponding records in the System Master Index (SMI). The system owner is responsible for ensuring that this occurs. (Refer to *Systems Architecture* > *General Architectural Standards* > *System Master Index* for further details.)

2.1.2 I/S Employee ID Codes

The I/S employee ID code is used to identify a given employee to the computer system. Variations of the employee ID code are given based on an access need to specific applications or networks.

2.2 Work Request Code Definition and Activity Overview

This is a summary of how projects and change sheets are defined and how time should be recorded against them.

2.2.1 Project Codes (XX999 or XX9999)

All time charged within ETKS is associated with a project code within our costing systems. A project is defined by a two character cost allocation prefix followed by either a three (3)- or four (4)-character suffix. There are five major types of project codes used in I/S. Standard, LOE, System Support, Training, and Leave/Other Non-Project codes.

2.2.2 Standard Project Codes

Standard project codes, which involve greater than 450 hours of work, are defined with a four (4)-character suffix for a total length of six (6) characters. The first two characters define the cost allocation method and the last four characters identify a specific project. With one exception involving TRICARE Reimbursable Work Requests, standard project codes do not have change sheets defined under them.

All authorized project work hours should be logged directly to the appropriate project code, from the initial discussions through closure. If there is production support work related to a project or change sheet, the Work Request team should charge time to it — not to the regular System Support codes used outside of project-related work.

2.2.3 LOE Project Codes

Level of Effort (LOE) project codes group like activities together and are defined with a three (3)-character suffix. LOE project codes are typically associated with customer-steerable work and usually have *030* as their suffix.

For LOE project codes, time is not charged against the project code directly, but to the change sheets, which are defined under the project code.

LOE Work Requests are received by I/S staff from Client Management, who have worked with the customer to authorize and prioritize the work activity. Sometimes customer requested work activities come directly to I/S Applications staff without Client Management's review and approval. It is mandatory for all I/S Applications staff to keep Client Management informed of all such requests so that Client Management can verify authorization to proceed and set the work activity priority.

The team assigned to the work effort should charge any production support efforts during Post Go-Live to the Work Request ETKS code, not to a System Support ETKS code.

Customer initiated work activity can also be created through a Technology Support Center (TSC) ticket. These are known as Service Requests. These TSC calls could include researching problems, education, answering general questions, vendor package upgrades, and new employee setup or changes. These customer-driven work activities have designated ETKS codes under LOE project codes.

2.2.4 System Support Project Codes

System Support project codes are codes defined to group like activities together. System Support project codes are driven and initiated by I/S Management and not the customer.

System Support task activity is defined below and is not determined based on organizational structure. Anyone performing these tasks should charge to the appropriate System Support project code.

System Support activities are grouped into five project codes, which are described below:

1. **Production Systems Maintenance & Monitoring (Host)**
   All tasks performed to keep the production Host environment up and running and resolving I/S to I/S Service Requests. This includes tasks such as:

   a. Production environment maintenance, monitoring and performance tuning tasks.
   b. Required/Mandatory code and JCL moves, for Work Requests.
   c. Disaster Recovery tasks.
   d. Production Quality & Process Improvement tasks.
   e. Reporting & Metrics tool creation tasks.
   f. Production Problem Management tasks.
   g. Production I/S to I/S Service Request Management tasks.

2. **Production Systems Maintenance & Monitoring (Non-Host)**
   All tasks performed to keep the production Non-Host environments up and running and resolving I/S to I/S Service Requests. This includes tasks such as:

   a. Production environment maintenance, monitoring and performance tuning tasks.
   b. Required/Mandatory code and JCL moves, for Work Requests.
   c. Required/Mandatory hardware server builds, for Work Requests.
   d. Disaster Recovery tasks.
   e. Production Quality & Process Improvement tasks.
   f. Reporting & Metrics tool creation tasks.
   g. Production Problem Management tasks.
   h. Production I/S to I/S Service Request Management tasks.

3. **Production Incident Management**
   All tasks performed to resolve production problems by System Support and Application Development staff for both software and hardware. This includes tasks such as:

   a. Production Emergency or Break/Fix code fixes.
   b. Code moves.
   c. JCL moves.
   d. Server fixes.
   e. Error Correction Requests (ECRs)

NOTE In support of the Problem Management activities, change sheets related to ECRs will be created. All time spent by the Application Development areas in the correction of the issue identified by an ECR should be logged against these change sheets. The System Support areas will also log to the appropriate

change sheet unless performing defined System Support activities. For Commercial Systems, the tickets for ECRs come through and either get added to an I/S Commercial change sheet or get sent back to the initiating customer steering to open a change sheet — as it is considered a system change (not an ECR).

4. **Production Customer Service Requests**
   All tasks performed to resolve customer requests for System Support service. This includes tasks such as:

   a. Critical research tasks performed by the System Support and the Application Development areas.
   b. Production customer Service Request resolution.
   c. Job execution requests.
   d. Security access setups.

5. **Test Environment & Developer Support**
   All tasks performed to keep the test environments up and running and to develop new test environments. This includes tasks such as:

   a. Test environment maintenance, monitoring and performance tuning tasks.
   b. Test environment Service Requests.
   c. Moving Work Request software updates through the various test environments.
   d. Optional/Discretionary code and JCL moves, for Work Requests.
   e. Optional/Discretionary hardware server builds, for Work Requests.
   f. Validate Emergency or Break/Fix code fixes, code moves, JCL moves and server fixes performed by System Support and Application Development staff for both software and hardware.

NOTE If a new test environment development effort is large enough to require a Project Manager (PM), then a change sheet must be opened under an LOB Steering LOE code for the PM to log their time. All other time will be charged to System Support codes.

The commercial FEP Systems Group is an exception. They will log FEP System Support task time to an FEP Production Systems & Maintenance (Host) code and an FEP Production Incident Management code. Other FEP support tasks will be logged to the common codes.

Efforts such as vendor application new installation, upgrade and maintenance are not System Support task activities. They are application development task activities and will be tied to a Work Request. Both Application Development areas and System Support areas will log time to the Work Request for non-System Support task activities. System Support areas will continue to perform code/JCL moves for these efforts, and this time will be logged to the appropriate System Support code.

2.2.5 Training Project Codes

Training project codes are defined for all training activities. Training project codes are driven and initiated by I/S Training and not the customer. The I/S Training Framework is part of the processes of

the I/S Managing People Program. Training is only provided to contractors for new applications or development tools introduced into the programming environment.

2.2.6 Leave/Other Non-Project Codes

Leave/Other Non-Project codes are project codes defined for non-work hours or hours not related to projects, change sheets, System Support or training. Non-project work is defined by I/S senior management and includes activities like the I/S Gathering and support of the United Way.

Chapter 3 Resource Acquisition

3.1 Requesting Resources

The IT Asset Inventory Management Life Cycle (Figure 3-1) begins with the submission of a document containing a list of approved resources needed by a Line of Business (LOB) and the legal authorization to spend money to acquire the resources.

NOTE Items not yet approved must go through the approval process before ever submitting a request.

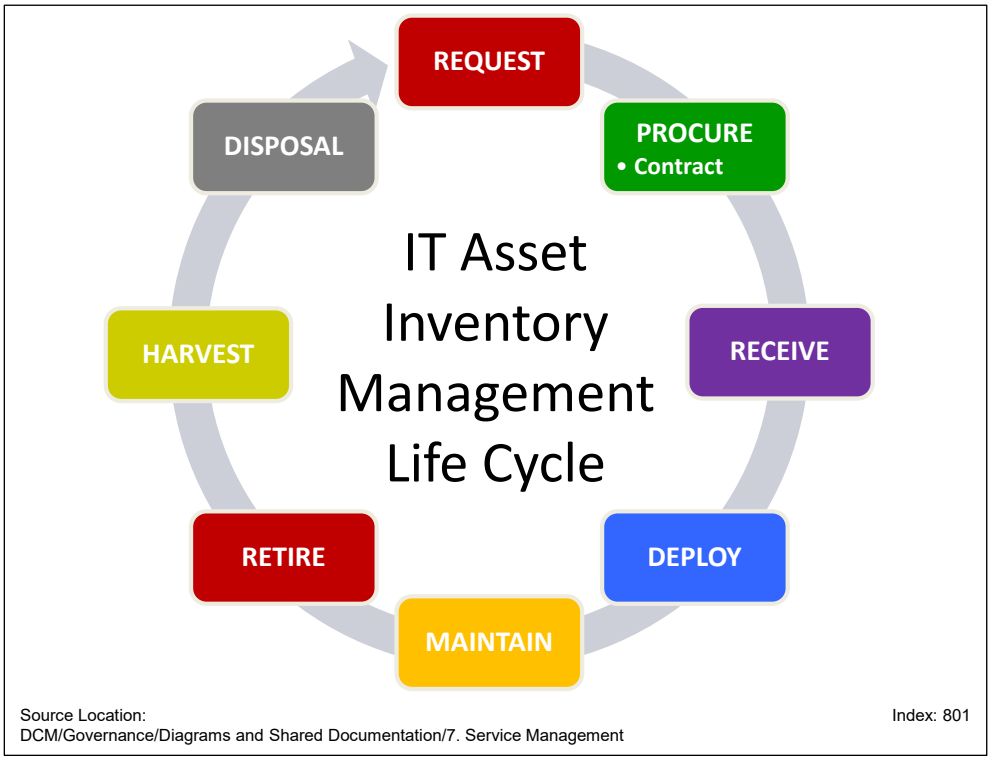


Figure 3-1 IT Asset Inventory Management Life Cycle

For additional details, refer to the introductory text of *ICT Infrastructure Management > Deployment Management Methodology* and the section *Requirements Phase*.

3.1.1 Procure

With agreement on the correct resources to fill the LOB's need, the Procure Phase of the IT Asset Inventory Management Life Cycle begins.

Working with I/S Contract Management (ISCM) early prevents unwanted delays and lays the groundwork for a smooth purchase. BlueCross BlueShield of South Carolina (BlueCross) requires contracts for acquisitions involving any of the following factors:

- Legally binding negotiations, which require a fully executed agreement signed by a Company VP or higher
- Specific terms of service (e.g., service start date, maintenance end date)
- Specific conditions of use (e.g., Service Level Agreement, government regulation)
- Statement of Work (SOW) (e.g., consulting work, services)
- Ongoing hardware maintenance or software support
- A product schedule or license agreement
- Total spend of $100,000 or more

In addition to contracts, Service Requests provide a way to request resources. When an operational device malfunctions, an Incident Ticket may result in a request for repair parts. Also, managers may request non-infrastructure items (e.g., desk phones, headsets, laptop computers, Visio licenses) through a signed purchase requisition.

Corporate Policy 65286 — Fiscal Disbursement requires management spending authorization to acquire resources (Refer to My e-Work > OurHRConnect > Corporate Policies.). The signature of a manager appropriate for the cost of the resources requested must always be provided.

3.2 Contract Management

ISCM negotiates and manages all I/S-related contracts to ensure their compliance with Federal Acquisition Regulations for Government business, corporate policies, and departmental procedures.

3.2.1 Lease/Purchase/Software/Maintenance Contracts

ISCM negotiates and manages all lease, purchase, software support and hardware maintenance contracts. Also, ISCM collaborates with the owners of the equipment to determine if they wish to renew the lease, purchase, software support or hardware maintenance contract.

There are several scenarios that may occur at the end of a lease depending on the stipulated terms and conditions (T&Cs):

- We may renew the lease for a new term or enter into a month-to-month extension of the lease.
- We may return the leased equipment to the vendor.
- We may purchase the leased equipment outright.

Software contracts may cover support for perpetual licenses or software subscriptions. When software subscriptions expire, the Technology owners responsible for use of the software will no longer be able to utilize the software unless renewed. If not renewed, the owners will follow required procedures for retiring and removing the subscribed software installed on the hardware.

When equipment is no longer covered by a maintenance contract, the owners responsible for the equipment must retire it from use or work with the Line of Business (LOB) System Security Officer (SSO)/Information Security Officer (ISO) to accept in writing the risk of using equipment without maintenance in production. Software without support requires the same written acceptance of risk from the LOB SSO/ISO.

3.2.2 Contract Management & Legal Review

I/S Contract Management (ISCM) in conjunction with the Corporate Law Department reviews and negotiates contractual agreements with technology vendors and internal stakeholders. Prior to actual purchase or agreement acceptance, any I/S acquisition-related document, excluding Purchase Orders, that involves legal T&Cs and a signature (e.g., software license, lease, Statement of Work, change order, or order form) shall be routed through the contract review process. ISCM works with the Corporate Law Department, Security, Risk and Compliance Assurance (SRCA), the Open Source Review Board (OSRB), Technology Owner and other areas as needed to conduct a thorough review of the contract and subsequent negotiations with the vendor. New vendor reviews include the RFS or RFP packages; additional compliance documents like the Security Questionnaire provide vital insight into key security and vulnerability concerns under consideration to govern the vendor. ISCM is not the subject matter expert (SME) on these topics but works with internal SME areas to ensure that the proposed solution receives proper consideration to govern the vendor's performance. ISCM reviews acquisition documents for factors like pricing, legal, data privacy, Blue Cross and Blue Shield Association mandates, information security, compliance with Government regulations, mandates and contractual obligations. For clarity, all parties involved contribute to determining the relationship of the proposed solution to government contracts. The relationship determines any flowdown requirements, which specific clauses, as well as other T&Cs necessary to ensure BlueCross BlueShield of South Carolina (BlueCross) compliance with government regulations and contractual obligations.

3.2.3 Prohibition of Outsourcing Overseas

Federal government regulations prohibit any external software or service vendors having access to or providing software development involving government data or systems from outsourcing services or transmission of data to locations outside of the United States or its Territories. ISCM works with the Law Department; Security, Risk and Compliance Assurance (SRCA); and the Technology Owner to ensure appropriate language is included in acquisition documents, such as the software license agreement or the services agreement for government projects, to enforce the above prohibition.

3.2.4 Medicare Security Standards Compliance

The following documents provide security guidelines for external software or service vendors (Contractors) having access to or providing software development involving Centers for Medicare & Medicaid Services (CMS) data or systems associated with CMS data:

- CMS Publication IOM 100-25. *CMS Information Security (IS) Acceptable Risk Safeguards (ARS). Appendix A - CMSR High Impact Level Data.*
- CMS Publication IOM 100-17. *Centers for Medicare & Medicaid Services (CMS) Business Partners Systems Security Manual.*

As appropriate, ISCM works with the Law Department, SRCA and the Technology Owner so that any contractual agreement with a vendor includes T&Cs to obligate vendor compliance.

The contractual agreement should also include the right for BlueCross to audit the Vendor Contractor's security and physical security measures; the vendor agrees to cooperate with such an audit.

3.2.5 Vendor Security Assessment Survey

Compliance Oversight & Risk Reporting (CORR) will conduct a security assessment survey of vendors of software applications or services involved with BlueCross BlueShield of South Carolina (BlueCross) data. The security screening will evaluate, at a high level, the vendor's familiarity and ability to comply with acceptable security standards. The following standards will be reviewed based on the Line of Business involved during the survey:

- CMS Publication IOM 100-17. *Centers for Medicare & Medicaid Services (CMS) Business Partners Systems Security Manual*. Available at: http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs.html.
- CMS Publication. *Acceptable Risk Safeguards 5.0x.* Available at: https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/information/acceptable-risk-safeguards-50x
- For Medicare Lines of Business: National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4. *Security and Privacy Controls for Federal Information Systems and Organizations*. Applicable elements from Appendix J, *Privacy Control Catalog*. Available at: https://doi.org/10.6028/NIST.SP.800-53r4.
- For PGBA Lines of Business: National Institute of Standards and Technology (NIST) Special Publication 800-171, Revision 1. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Applicable elements from Appendix D, *Mapping Tables*. Available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

- Security assessments for Commercial Lines of Business evaluate the compliance with BlueCross security policies along with other commonly accepted technical practices. A blended approach is taken and assessments may include controls from NIST, Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technologies (COBIT) or other appropriate control sources.
- Information technology products associated with Personal Identity Verification (PIV) capabilities must be on the approved products list per FIPS PUB 201-3. *Personal Identity Verification (PIV) of Federal Employees and Contractors*. Available at: https://csrc.nist.gov/publications/detail/fips/201/3/final. For an example of approved products, refer to https://aplits.disa.mil/processAPList.action.
- Additional standards may be added or substituted for the above, as applicable.

Such screening may include a review of the vendor's responses regarding: logical and physical access controls, system acquisition process, information system documentation, physical and environmental controls, incident response plan, contingency plans, data encryption methodology, personnel background checks, and software development controls. CORRn shall provide a report that summarizes the vendor's security controls and security performance to the assessment requestor, Vendor Owner and ISCM. Assessments will be executed during the initial vendor review process and ongoing as requested by the LOB SSO/ISO, Vendor Owner or ISCM.

The following government controls may be relevant during the survey process: SA-4 Acquisition Process, SA-5 Information System Documentation, SA-9 External Information System Services and SA-12 Supply Chain Protection.

3.2.6 Government Contract Supply Chain Threat Screening

Software, hardware or service vendors providing services or having access to or providing software development involving CMS data or systems shall be subject to an additional security screening to identify and analyze supply chain threats. The I/S Vendor Management Office (VMO) meets periodically with strategic vendors to review contractual obligations, performance data, and how the vendor mitigates supply chain threats to protect the flow of resources into BlueCross.

For additional details, refer to government controls NIST SA-9 and SA-12.

3.2.7 HIPAA Business Associate Agreement

The Law Department will require vendors or suppliers of software or services that have access to or provide software development involving receipt or maintenance of any Protected Health Information (PHI) from or on behalf of BlueCross or its subsidiaries or both, to execute a Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associate Agreement and to otherwise cooperate in all respects with the company's efforts to comply with federal and state laws and rules governing privacy.

3.2.8 Information Privacy & Security Controls

I/S vendors having access to government program Personally Identifiable Information (PII) shall agree to comply with the applicable privacy and security controls of the *Privacy Control Catalog*, which is Appendix J of the NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. To ensure that privacy requirements will be satisfied in a comprehensive, cost-effective, and risk-based manner, the Law Department and ISCM include in acquisition documents, such as software license agreements or services agreements, a clause requiring conformance with applicable Appendix J privacy assurance controls.

NOTE For additional information, refer to *Service Management* > *Service Support* > *Inventory Management* > *Resource Acquisition Standards*.