Hospital Name:

Application Area	Application Name	Stores PHI? (Y/N)
Accounting		
Admitting		
Appointment/Resrouce Sch		
Biomed		
Call Accounting		
Cardiology		
Central Supply		
Chart Reservation/Tracking		
Coding		
Contract Services		
Dietary		
Education		
Emergency Department		
Employee Equal Opportunity		
Employee Health		
Environmental Management		
Facilities Management		
Finance		
HIV Clinic		
Home Health		
Human Resources		
Immunization		
Infection Control		
Information Systems		
Inventory Control		
JCAHO Compliance		
Lab		
LSUHSC-MD Billing		
Medical Records		
Medical Staff		
Medical Staff		
Nursing		
Nursing In-Service		
Patient Accounting		
Payroll		
Performance Improvement		
Pharmacy		
Property Control		
Psychiatric Services		
Purchasing		
Radiation Onocolgy		
Radiology		
Respiratory		
Surgery Scheduling System		
Time/Attendence		
Trauma Registry		

Enterprise Survey

E1: Does the enterprise use a security standard for implementing IT security?
E2: Was this security standard developed internally or is it a set of published standards (e.g. ASTM 1869)
E3: Does the enterprise have a written security plan? If so please attach copy of it.
E4: Does the enterprise have a written security policy? If so, Please attach a copy.
E5: Who is responsible for enterprise IT security?
E6: Does the enterprise certify or accredit security procedures against a set of standards? If so, how frequently is this done? Who performs the certification? Is that person internal to LSUHSC?
E7:Is there a written policy covering requirements for backups for the enterprise? If so, please attach a copy.
E8: Does the enterprise have a written workstation use policy? If so, please attach a copy.
E9: Does the enterprise have a written policy governing the termination of employees? If so, please attach a copy.
E10: Does this termination policy include a requirement to notify the IT department so that access to all systems and IT related areas for that employee can be removed? How quickly is this usually accomplished?
E11: Do new employees (including management and IT) receive instruction on IT security including virus protection and password management at orientation? Is this instruction repeated? If so, how frequently?
E12: Do new physicians, residents, and medical students receive instruction on IT security including virus protection and password management? Is this instruction repeated? If so, how frequently?
E13: Does the enterprise have an ongoing security awareness program that includes IT security and confidentiality of patient information? If so, please describe and attach information about the program
Business Impact Analysis
Recovery Strategy
Recovery Plan
Return Migration Plan
Test Plan
Policies and Procedures
E15: How frequently is the disaster recovery plan revised and tested?
E16: Does the enterprise have a diagram documenting the network? If so, please attach a copy. Is it up-to-date?
E17: What security training do contract personnel receive?
E18: Does the enterprise have a formal process for developing security policy that includes IT? If so please describe. Please attach copies of pertinent documents.
E19: Is there a procedure to provide emergency access? If so, please attach a copy of the procedure.
E20: Please attach any policies/procedures applicable to automatic logoff.
E21: Who is responsible for the users' initial system training?
E22: What is taught to users regarding security and confidentiality of data?
E23: What type of clearance procedures must an employee undergo to obtain access to the enterprise network?
E24: How is a user's authorization to access the enterprise network determined?
E25: Is a record of these authorizations maintained? By whom?
E26: How are user id's assigned?
E27: Who maintains the list of user id's? Who has access to it?
E28: Who assigns the initial password, and when is it first changed by the user?
E29: How often must a user change his/her password?
E30: Are there any generic user id's and/or passwords (e.g., user id DOCTORDOCTOR)?
E31: Is logon/logoff activity tracked with a security log or audit trail?
E32: What data is kept by the security log/audit trail?
E33: What is user access based upon (e.g., need-to-know, job function)?
E34: Are IT personnel restricted access to patient data? How?

E35: Are vendors, consultants, and other third parties restricted from access to patient data? How?
E36: Does the enterprise network operating system support automatic logoff?
E37: What is the time limit for inactivity prior to logoff?
E38: Please attach any policies/procedures applicable to automatic timeout (screensaver).
E39: If a screensaver timeout was employed, what problems would it create?
E40: Are there any user accounts and passwords that are not assigned to an individual person? (e.g. a terminal or a program?) How are these secured?
E41: How are network electronics secured against unauthorized use?
E42: Are all network electronics (routers, switches, hubs, etc.) on a UPS? Are they all connected to emergency power? If not, list those that are not and reasons for not connecting them to emergency power.
E43: What precautions have you taken to prevent tampering with the data traveling over enterprise network?
E44: Is wireless networking being used anywhere at the enterprise? If so, what steps have been taken to prevent unauthorized interception of, and tampering with, data?
E45: Do you maintain an inventory of computer hardware for the enterprise? If so, is it in addition to that maintained by Property Control?
E46: Does any part of the enterprise network make use of publicly (i.e. non-LSUHSC employees) accessed networks (e.g. LANET, Internet) to transport patient data? If so, what steps have been taken to prevent interception and tampering of the data?
E47: What steps have been taken to prevent access to the enterprise network by unauthorized persons? (e.g. hackers)
E48: How frequently are backups performed? To what media?
E49: Are these backups full or incremental? , How frequently are full backups performed?
E50: Has the system recovery process been tested? How frequently?
E51: How many generations of backup are retained, and where?
E52: Who has access to the backup media?
E53: Is the backup storage location hardened against possibly disasters? (e.g. fire, flood, collapse, etc.)
E54: Are all servers on a UPS? Are they all connected to emergency power? If not, list those that are not and reasons for not connecting these servers to emergency power.
E55: When an operating system is installed either as an upgrade or as part of a new machine, is the configuration of operating system checked for maximum security or is it installed with the default configuration in place?
E56: Do all workstations and servers have a virus-checking program running on them? If so which one? How frequently is the virus data file updated? How do you insure that each workstation and server has an up-to-date copy?
E57: Does the enterprise have a QC checklist the tech completes at the end of a service call? If so please attach a copy.
E58: When new software is installed on a workstation or server, what steps are taken to insure that the security features have not been altered by the installation?
E59: How are servers secured at the enterprise to prevent tampering by unauthorized individuals?
E60: Do any workstations have patient identifiable health information stored on their local hard drives? If so, what special precautions are taken to insure that this information is not revealed to unauthorized persons?
E61: What steps are taken to insure that the enterprise security measures in place are effective?
E62: Are the workstations configured to go to a screen saver after a period of time?
E63: What is the time limit for inactivity prior to the screen saver timeout?
E64: How does the user return to the application from the screen saver?
E65: Who is responsible for applying upgrades and patches to the system?
E66: Who supervises and reviews their work?
E67: On what media are upgrades and patches received? How frequently?
E68: What precautions are taken to prevent unauthorized tampering with upgrade and patch files?
E69: How timely are upgrades and patches applied after being received from the vendor?
E70: Is this system up-to-date with all upgrades and patches? If not, please explain.
E71: How is the network operating system tested to determine if upgrades and patches were applied correctly? Are the users involved?
E72: Are upgrades and patches loaded to a test system or directly into the production system?
E73: How are modifications to a user's access authorized?

E74: Have the security practices of the enterprise been audited? If so, by whom? How frequently does this occur?
E75: Do you maintain an inventory of all software installed on workstations and servers at your site?
E76: How would a security breach be detected? How long would take to detect a security breach?
E77: Are security logs available? What data is kept by them? Are they reviewed regularly? Is the review manual or automatic?
E78: Who reviews the security logs or audit trails?
E79: Is security review of the information system part of someone's job description? If so, please attach job description.
E80: Who would normally report a security breach?
E81: Who would investigate the claim?
E82: How would system access be restricted during the investigation?
E83: How would the guilty party be disciplined?
E84: How is the incident documented?
E85: What procedures are used to track the movement of hardware in the enterprise?
E86: What procedures are used to track software within the enterprise?
E87: What records are kept on the maintenance of enterprise hardware? (workstations, servers, network electronics, etc.)
E88: What records are kept on the upgrades and patches to network operating system software?
E89: How is the physical access to sensitive IT areas by personnel, visitors, contractors, etc. controlled?
E90: Does the enterprise make use of portable devices (e.g. laptops, PDA's) ? If so, what precautions do you take to prevent such devices from unauthorized use? Please attach copies of any policies that apply.
E91: How are network problems detected? Is there in automatic event monitoring processes in place?
E92: How are remote access services provided?
E93: How is access to the Internet provided? Do you use an ISP?
E94:What percentage of the workforce has access to the internet? Who determines if an employee gains access?
E95: What is the firewall infrastructure in place for the internet gateway?
E96: What encryption services are in place for intra-network communications?
E97: Under what circumstances are non-employee individuals provided access to the LSUHSC network? Is a record kept of these individuals? How is notification of termination of their access handled?
E98: Please attach any policies or other written documentation pertaining to the security infrastructure of the network.
E99: Are electronic signatures employed on the enterprise network?
E100: Who maintains the virus protection software signature files?
E101: What is the procedure for alerting users to new viruses?
E102: Does network management include capacity monitoring for processor bottlenecks, memory bottlenecks, network bandwidth bottlenecks and storage bottlenecks?
E103: What availability statistics are kept on the enterprise network? Provide an example.
E104: Who is responsible for monitoring this utilization management process?
E105: What is the procedure for responding to capacity problems?
E106: Have capacity plans been made for the long-term goals of the enterprise? If so, please attach a copy of such plans.
E107: Describe the physical security of the enterprise data center.
E108: Who determines and grants access to the various parts of the data center?
E109: Are all servers and computing platforms located in the data center? If not, is the same level of physical security applied to all locations?
E110: Can you provide a log of all individuals who were granted to the data center in the last six months?
E111: Who is responsible for policies and procedures applicable to enterprise security practices?
E112. What is the procedure for handling change requests for this system? Please attach a copy of the procedure.
E113. How are the users impacted by the change identified?
E114. How are the users impacted by the change request notified of the change?

E115: Do the users who are impacted by changes in the system provide input on the change prior to its implementation?
E116. How is the change request documented? Please attach a copy of an example.

Site/Campus Survey

Site:
Application:
Vendor:
Name of Vendor Contact:
Phone Number of Vendor Contact:
Functions Supported:
Security manager for this Application:
Completed By:
Date Completed:
AS1. How is a user's authorization to access the system determined?
AS2: Is a record of these authorizations maintained? By whom?
AS3. How are user id's assigned?
AS4. Who maintains the list of user id's? Who has access to it?
AS5. Who assigns the initial password, and when is it first changed by the user?
AS6. How often must a user change his/her password?
AS7. Does this system synchronize user names and passwords with the Windows NT network?
AS8. Are there any generic user id's and/or passwords (e.g., user id DOCTORDOCTOR)?
AS9. Is logon/logoff activity tracked with a security log or audit trail?
AS10. Are logon failures documented in a security log or audit trail?
AS11. When an employee is terminated, what is the procedure for de-activating the user id? How quickly is this accomplished?
AS12. Are any other access control methods in use on this system? (e.g. cardkeys, callbacks, PIN's, etc.) If so, please describe.
AS13. How frequently is the user list reviewed for inactive accounts?
AS14. What type of clearance procedures must an employee undergo to obtain access to this system?
AS15. Are there any user accounts which are not assigned to an individual person? (e.g. a terminal or a program?) How are these secured?
AS17. Is user access to patient data restricted? How?
AS18. What is user access based upon (e.g., need-to-know for treatment, job function)?
AS19. Are IT personnel supporting this application restricted access to patient data? How?
AS20. Are vendors, consultants, and other third parties working with this application restricted access to patient data? How?
AS21. Who has full access to all patient data in this application?
AS22. Is data access tracked with a log or audit trail? What type of information is kept by the audit trail?
AS23. Is there a procedure to provide emergency access? If so, please attach a copy of the procedure.
AS24. Are there written policies and procedures for the routine handling of data for this system covering receipt, manipulation, storage, dissemination, transmission, and/or disposal of data for this system? If so, attach copies of all policies and procedures that apply.
AS25. Are there written policies and procedures for the ***non***-routine handling of data for this system covering receipt, manipulation, storage, dissemination, transmission, and/or disposal of data for this system? If so, attach copies of all policies and procedures that apply.
AS26. How is authorization to modify a user's access to data determined?
AS28. Does the system support automatic logoff?
AS29. What is the time limit for inactivity prior to logoff?
AS30. Can the system keep track of where a user left the system and return him/her to the same location after automatic logoff?
AS32. Does the system go to a screen saver after a period of time?
AS33. What is the time limit for inactivity prior to the screen saver timeout?
AS34. How does the user return to the application from the screen saver?
AS36. How frequently is the **data** backed up? To what media?
AS37. How many generations of **data** backup are retained, and where?
AS38. Is it necessary to bring the system down during **data** backups?
AS39. Are the **data** backups full or incremental? How frequently is a full backup of the data performed?
AS40. How frequently are the **programs** backed up? To what media?
AS41. How many generations of **program** backup are retained, and where?
AS42. Is it necessary to bring the system down during **program** backups?
AS43. Are the **program** backups full or incremental? How frequently is a full backup of the programs performed?
AS44. Has the **data** recovery process been tested? How often?
AS45 Has the **program** recovery process been tested? How often?
AS46. When is **data** archived? To what media?
AS47. How is **data** recovered from archives?
AS48. When is **data** permanently purged?

AS49. How is it purged?
AS50. How are the backups stored.
AS51. Is the storage location hardened against disasters? (e.g. fire, flood, plumbing damage, etc.)
AS52. Are backups stored in multiple locations?
AS53. Who has access to the backup storage location(s)
AS54. Has the criticality to LSUHSC's operation of this application been evaluated? If so, what was the result of that evaluation?
AS56. Who is responsible for applying upgrades and patches to the system?
AS57. Who supervises and reviews their work?
AS58. Where is the equipment located that supports this system? How is that location secured?
AS59. On what media are upgrades and patches received? How frequently?
AS60. What precautions are taken to prevent unauthorized tampering with upgrade and patch files?
AS61. Where are the media stored after the upgrade is completed?
AS62. How timely are upgrades and patches applied after being received from the vendor?
AS63. Is this system up-to-date with all upgrades and patches? If not, please explain.
AS64. How is the system tested to determine if upgrades and patches were applied correctly? Are the users involved?
AS65. Are upgrades and patches loaded to a test system or directly into the production system?
AS66. Is a log maintained of all upgrades and patches received and applied? Who maintains the log? Please attach a copy.
AS67. Where is this application's technical documentation stored? How many copies are retained? On what media?
AS68. Is this application's technical documentation up-to-date with all upgrades and patches? If not, explain.
AS69. If the vendor or a third party apply the upgrades or patches, who is responsible for supervising and reviewing their work?
AS70. What steps are taken to insure that the system's security features have not been adversely affected by the upgrade or patch?
AS71: How are changes handled? Who has input? How is the impact of the change assessed? How are users notified of changes?
AS72. Is there a downtime procedure for this application. If so, please attach.
AS73. Does the downtime procedure include steps to update the data with information acquired during the downtime? If not, why?
AS74: What is the average availability of this application over the last 12 months?
AS75. Is the equipment necessary to run this application connected to a UPS? Is it connected to emergency power? If not, why?
AS77. Who is responsible for the users' initial system training?
AS78. Who is responsible for the users' training on subsequent upgrades and patches?
AS79. What is taught to users regarding application security and confidentiality of data?
AS80. What training do IT personnel receive regarding the application's security features?

Data Being Sent	***Receiving System***

AS83. If the transfer of data is not electronic (i.e., it is not being sent via an interface), what media is used? How is the media handled? Is this information recorded in a log. If so, please attach a copy of a sample log.
AS84. Is data being transferred to a non-LSUHSC system? If so, attach copy of contract or policy governing each transfer.
AS85: What mechanisms are in place to log the transmission/reception of data to organizations outside LSUHSC.
AS87. Is the system accessed via the 155.58.x.x network? If not, how is it accessed?
AS88. Does the system have dial-in or dial-out capability?
AS89. Does the system have any other method of access?
AS90. What is the procedure for handling change requests for this system? Please attach a copy of the procedure.
AS91. How are the users impacted by the change identified?
AS92. How are the users impacted by the change request notified of the change?
AS93: Do the users who are impacted by the change in the provide input on the change prior to its implementation?
AS94. How is the change request documented? Please attach a copy of an example.
AS95. How would a security breach be detected? How long would take to detect a security breach?
AS96. Are security logs or audit trails available? Are they reviewed regularly? Is the review manual or automatic?
AS97. Who reviews the security logs or audit trails?
AS98. Is security review of this application part of someone's job description? If so, please attach the job description.
AS99. Who would normally report a security breach?
AS100. Who would investigate the claim?
AS101. How would system access be restricted during the investigation?
AS102. How would the guilty party be disciplined?
AS103. How is the incident documented?
AS104. Have security processes on this system ever been audited? If so, how frequently are they audited.

Change Request Form

Part 1 to be completed by requesting person.
Request Id: _____
Emergency: □
Date of Request: _____ Date Change Needed:_____
Name of Requestor:_____ Requesting Department:_____
Requestor Phone #:_____
Requestor Location:_____ Location needed:_____

System as exists now:

Work or change to be implemented:

Expected outcome / Benefits / Cost Analysis for change / Why Emergency:

Hospital Operations / Systems Impacted by Change:

Success Criteria:

Affected Department 1:_____Authorization 1:_____
Affected Department 2:_____Authorization 2:_____
Affected Department 3:_____Authorization 3:_____
Affected Department 4:_____Authorization 4:_____
Affected Department 5:_____Authorization 5:_____

Part 2 to be completed by Information Systems.
Category and Resource:

External Cat 1: □	Maintenance: □	
Internal Cat 2: □	External Cat 2: □	Ad – Hoc : □
Single Cat 3: □	Internal Cat 3: □	External Cat 3: □

Management Control Level:
Priority: High Medium Low
Back out / Fallback Procedures if Success Criteria are not met within Downtime Limits:

Downtime needed:
Analysts Assigned:
Project Plan Produced: □ Project Plan File Name:_____
Estimated Time Project Completed:
Proper Parties Notified of Completed Project Plan: □ Notified by:_____

Instructions

Part: 1 To be completed by Requestor. If a section is not large enough for your response, please attach extra pages.

Change Definition: Change is a request for a new system or an alteration to an existing system that is beyond normal reporting and maintenance. This includes projects, upgrades, new reports, etc. Not included are preventive maintenance, ad hoc reporting and statistics, user password and access request, etc.

Request id is assigned by IS to track requests.

Emergency is checked if this is an emergency request or left blank for normal requests.

Date of Request is today's date.

Date Change Needed is the date you would like to see the change implemented.

Name of Requestor is your name.

Requesting Department is your department.

Requestor Phone # is a phone number where you can be reached. Please include any means of contacting you.

Requestor Location is your building and room number.

Location needed is the building and room number of where you would like the equipment / software installed.

System as exists now is a brief description of your current situation.

Work or change to be implemented is a description of what you want done. Please continue on extra sheets if necessary. Please note that if this is a major change, we will go through a requirements definition step in the project. At this step, we'll define in minute detail the changes to be made.

Expected outcome / Benefits / Cost Analysis for change / Why Emergency is a justification for the change. By describing what you expect the modified system to do and the benefits, IS will better understand how to prioritize this request. By adding a cost analysis, the IS steering committee and CIO can better justify the funds for this request. If you marked this request as an Emergency, please explain why. Not all requests will warrant a full detailed explanation of each point. Sound judgement serves best here. Please continue on extra sheets if necessary.

Hospital Operations / Systems Impacted by Change is a description of what operations or systems could possibly be impacted by the change directly or indirectly during implementation. For example, we may have to take a piece of the system out or service for an hour to implement this change. Who do you think might lose service.

Success Criteria is how you would measure an up and running completed change. This would include the things the systems is doing and how long should we monitor for correct operation. An example could be – the interface is sending ADT records with no more than a 100 record backlog monitored for 3 hours of successful running. We will use this information to either trigger a back out of the change or to signoff on the request as complete.

Affected Department 1 – 5 is a list of departments affected by this change.

Authorization 1 – 5 is the respective department signatures approving the change for their department.

Part: 2 To be completed by Info Systems. If a section is not large enough for your response, attach extra pages.

Category and Resource is marked according to the Systems Decision Algorithm Charts.

Management Control Level is the name and position of the IS personnel responsible for planning this change.

Priority is based on IS determination of how important the project is to the business of the hospital, the IS strategic plan, etc. We use the Hospital and IS strategy plans and missions statements for direction in this determination.

Back out / Fallback Procedures if Success Criteria are not met within Downtime Limits is what we need to do to back out this change if it fails. As part of a project, we'll review and formalize this right before implementation. Failure is defined as the success criteria are not hit and sustained for the period of time defined by the requestor.

Downtime needed is how long will the system be down to implement and test this change.

Analysts Assigned is a list of the analysts assigned to this project.

Project Plan Produced is a check off that a project plan has been produced. A check means that a plan is either produced or not needed, while a blank means that a project plan is needed but not yet produced.

Project Plan File Name is the name and location of the project plan. If one is not needed then write Not Applicable.

Estimated Time Project Completed is either the time to complete a really short project or the estimated date the project will be completed.

Proper Parties Notified of Completed Project Plan is checked when the project plan is finished, distributed, and agreed on by the affected departments.

Notified by is the name of the IS person that was responsible for notifying the affected departments.

Definitions

Change – is a request for a new system or an alteration to an existing system that is beyond normal reporting and maintenance. This includes projects, upgrades, new reports, extending current systems to new departments, etc. Not included are preventive maintenance, ad hoc reporting and statistics, user password and access request, etc.

Resource Single - problem that can be solved by a single analyst.

Resource Internal – a problem whose solution involves HIS staff and / or one department.

Resource External – a problem whose solution involves HIS staff and coordination of multiple departments.

Category 1 – Formal Project – project needing attention of IS steering committee or having a large enterprise wide impact. Tends to be a major change with medium to high impact with documentation and training allowed.

Category 2 – Major Change – change that has a medium to high impact with documentation and training allowed.

Category 3 – Minor Change – change that has a low impact on a system with no documentation or training required.

Emergency – Unpredictable failure of critical production system that must be fixed immediately.

Valid Combinations

A request must have a Category and Resource assignment. Some combinations are not valid. The following grid demonstrates this.

	Single	Internal	External
Category 1	Invalid	Invalid	Valid
Category 2	Invalid	Valid	Valid
Category 3	Valid	Valid	Valid

As the grid progresses from bottom to top from Category 3 to Category 1 the following increases:

- Funding / Resources
- Management involvement
- Project Planning
- Communication Requirements

As the grid progresses left to right from Single to External the following increases:

- Formality
- Communication Requirements
- Project Planning
- Management Involvement

As the grid progresses right to left and top to bottom, the distributed empowerment and decision making increases.

General Algorithm

1) Log request / start a Request Sheet.

2) Assign or adjust Category and Resource designation using the following evaluation criteria.

- **Application Systems See attachment A.**
- **Technical Systems See attachment B.**
- Cost
- Guessed Work / Time to complete
- Impact
- Current workload for Single Analyst if at a Level of Single.
- Education for technical / application staff
- Education for End User
- Documentation changes needed

3) Is issue currently being coordinated at the proper IS Management level? If not then bump up or down based on following list.

Single Cat 3:	Analyst
Internal Cat 3:	Analyst / Front line Manager
Internal Cat 2:	Front Line Manager / Analyst
External Cat 3:	Front Line Manager / Analyst
External Cat 2:	CIO / Front Line Manager
External Cat 1:	IS Steering – Executive Management / CIO
Emergency:	Judgement Call with communication at all appropriate levels

4) Set priority to request.

5) Schedule resources and time to perform work.

6) Follow appropriate checklist for project planning purposes for each of Technical, Applications, Operations, and Communications.

7) Communicate/Document schedule, priority, project plan, timeframes to management, requestor, and other users.

8) Complete work and file project folder.

Note: Emergencies are by nature the exceptions to the above rules. Priority should be given to performing the work, coordinating with the change gatekeeper for proper handling, and communication of what is done to all levels of the organization.

Attachment A: Resource and Category for Applications

		External Cat 1: • Needs HIS, Multiple Department coordination, and IS Steering Committ Review/Prioritization • Tends to be a Major change - Medium high impact on system • Affects users in more than one departn with training requirements allowed • Changes to current documentation allo • May have training needed for analysts • May have significant Back-out proced production implementation were to fai [possible High Risk] • Work completed in time frame to be determined by Project plan and IS Ste Committee • Put financial and man-hour requiremer here.
	Internal Cat 2: • Needs more than one analyst with one department coordination • Major change - Medium to high impact on system • Affects users in one department with training requirements allowed • Changes to current documentation allowed • May have training needed for analyst • Minimal Back-out procedures if production implementation were to fail [Medium risk] • Work completed in less than 45 working days (I.E. 2 months){this is an example}	**External Cat 2**: • Needs HIS and Multiple Department coordination • Major change - Medium to high impac system • Affects users in more than one departn with training requirements allowed • Changes to current documentation allo • May have training needed for analysts • Minimal Back-out procedures if produ implementation were to fail [Medium • Work completed in less than 45 worki days (I.E. 2 months){this is an exampl
Single Cat 3: • Can be complete by single analyst with one department coordination • Minor change - Low impact on system • Affects users in one department with no training requirements • No changes to current documentation • No training needed for analyst • Little to No Back-out procedures if production implementation were to fail [low risk] • Work completed in less than 11 working days (I.E. 2 weeks){this is an example}	**Internal Cat 3:** • Needs more than one analyst with one department coordination • Minor change - Low impact on system • Affects users in one department with no training requirements • No changes to current documentation only • No training needed for analyst • Little to No Back-out procedures if production implementation were to fail [low risk] • Work completed in less than 22 working days (I.E. 1 month){this is an example}	**External Cat 3**: • Needs HIS and Multiple Department coordination • Minor change - Low impact on system • Affects users in more than one departn with no training requirements • No changes to current documentation • No training needed for analyst • Little to No Back-out procedures if production implementation were to fai risk] • Work completed in less than 22 worki days (I.E. 1month){this is an example

Emergency:

- Production system is inoperable.

Attachment B: Resource and Category for Technical

		External Cat 1: • Users, MCLNO & LSUMC Analysts c man-days; • System or Network outage > 120 minu • Impacts Multiple Departments; • Infrastructure impact involves comple planning; • Follow formal project plan and implementation scripts; • Create Standards; • Coordinate production lead times at pr meetings; • e.g. SunQuest, UH Infrastructure, Thir Client, etc. • IS Steering/CIO Coordinate
	Internal Cat 2: • Both MCLNO & LSUMC Analysts up to 22 man-days; • System or Network outage < 60 minutes; • Expected System impacts known, simple back out; • Follow formal project plan and implementation scripts; • Develop/revise documentation; • 3 days planned lead time to put into production; • e.g. Gateway Cut-Overs, Network Switch Firmware Upgrades, etc. • Manager / Analyst Coordinate	**External Cat 2**: • Users, MCLNO & LSUMC Analysts l than 22 man-days; • System or Network outage < 120 minu • Impacts multiple Departments; • Uncertain System Impacts or Complex Out required; • Follow formal project plan and implementation scripts; • Develop/revise documentation; • 3 days planned lead time to put into production; • e.g. Email Project, IPX over 75071, et • CIO/Front Line Manager Coordinate
Single Cat 3: • One MCLNO/LSUMC Analyst limited to 5 man-days • System or Network Outage < 15 Minutes; • Impacts 1 Department • System impact known; • Follow existing implementation scripts and project check list; • Update existing documentation; • No planned lead time required to put into production; • e.g. Enabling Existing Network Ports, Granting Access to Existing Servers • Analyst Coordinates	**Internal Cat 3:** • Both MCLNO & LSUMC Analysts up 5 man-days; • System or Network Outage < 15 Minutes; • Expected System impacts known, simple back out; • Follow new implementation script and project checklist; • Append existing documentation; • 1 day planned lead time to put into production; • e.g. Router Table Upgrades, Single Function Server Upgrades, etc. • Manager / Analyst Coordinate	**External Cat 3**: • Users, MCLNO & LSUMC Analysts u man-days; • System or Network Outage < 15 Minu • Impacts Multiple Departments • Expected system impacts known, simp back out; • Follow implementation scripts and pro checklist; • Append existing documentation; • 1 day planned lead time to put into production; • e.g. Client Software Upgrades, Mass Emailing, Virus Checking • Manager / Analyst Coordinate

Emergency:

- Production system is inoperable.

Attachment C: Application Checklist

- Organize project team together and identify project leader.
- Hold kickoff meeting with analysts and department representatives – decide meeting schedule and logistics.
- Develop application and technical requirements from request sheet in conjunction with users.
  - Do you need any equipment?
  - Include requirements for on-going support and maintenance.
  - Document interdependencies to other systems. Does this change cause changes to other systems?
  - Any training for analysts needed.
- User / Departmental / IS Steering Committee / Executive sign off on requirements.
  - Consider budgetary resources – cost analysis.
  - Consider project priority level.
- Communicate technical requirements to tech group and schedule .
  - Make sure new equipment, network drop, cabling, network configuration, software, or tools are ordered.
  - Follow technical checklist with technical analysts to ensure proper handling of request.
- Schedule and conduct analyst training.
- Develop task list or detailed project plan for work to be performed.
- Obtain clearance for development environment – coordinate with the change and development gatekeepers.
  - Is the copy you are changing the most current one? If not get most current copy of source.
- Follow work plan / project plan.
- Alpha Test.
  - Test your screen, flow functionality.
  - Test integration with system.
  - Document system errors found.
  - Fix system errors found.
- Beta Test.
  - Users test screen and flow functionality.
  - Users test integration.
  - Users test system compared to requirements.
  - Document errors found.
  - If error is promised in requirement package then fix.
  - If error not covered in requirement package then negotiate with user to fix and adjust timeframes or add to enhancement list.
- Produce installation, reference, error message, and user's guides.
- Produce Administration guide for help desk, operations, restart procedures, and etc.
- Gamma Test Plan.
  - This is a plan of comparison of adjusted requirements to software.
- Obtain clearance for test from gatekeeper.
- Migrate to test environment.
- Gamma Test.
  - Compare system to requirements.
  - Verify hardware working in conjunction with software.
  - Fix requirement shortcomings.
  - Add other errors to enhancement list.
  - User sign off of Gamma.
- Conduct training for user community.
- Produce documentation needed for production.
  - Consider system downtime.
  - Consider back-out procedures if needed.
  - Consider security access, user-ids, and passwords.
  - Consider disaster recovery.
  - Consider capacity planning and information growth.
  - Document Go Live Plan.
- Obtain clearance for production from gatekeeper and production monitor.
- Migrate to production.
- Monitor application in production.
- Set up on-going support and maintenance.