|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Details | | | | |
| Family Name: | Ferro | | | |
| Given Name: | Alessandro | | | |
| Subject Details | | | | |
| Qualification: | Diploma of Web Development | | | |
| Unit Code and Title: | ICTICT503 – Validate quality and completeness of system design specifications | | | |
| Trainers’ Name: | Ida Ho | | | |
| Assignment Details | | | | |
| Due Date: |  | Assessment No:  (If applicable) | |  |
| Date Submitted: |  | | | |
| Checklist | | | | |
| * I have kept a copy of my assignment before submitting * I have completed and signed this page * I have answered all questions in the assignment * I have attached any relevant evidence/documentation, as required for the assessment | | | | |
| Declaration | | | | |
| I have been advised of the assessment requirements and have been made aware of my rights and responsibilities as an assessment candidate.  I declare that, to the best of my knowledge and belief, this assignment is my own work, all sources have been properly acknowledged, and the assignment contains no plagiarism. This assignment or any part thereof has not previously been submitted for assessment **at this or any other RTO**. | | | | |
| Student’s signature:  Alessandro Ferro | | | Date:  05/08/2020 | |
|  | | |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| **Assessment Feedback** | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
| **Result** | **Satisfactory** | **Not Satisfactory** | **RPL** | **RCC** |
| **NYC – New assessment date scheduled or FIR – Further information Required** | | | **Date:** | |
| Trainers/Assessors signature: | | | Date: | |
| **Student Comments** | | | | |
|  | | | | |
|  | | | | |
|  | | | | |
| * I have received my assessment result and am satisfied with the feedback given on this assessment | | | | |
| Student’s signature: | | | Date: | |

**Activities**

1.1

List some documents required as input to understanding the system. List at least two items are required to understand the system to be audited.

**Answer**

* **Functional Requirements:** Describe the functionalities that the sytems is expected to perform.
* **Technical Requirements:** Describes the technical aspects of the product.
* **Initial Design:** Describes how the software will be implemented.
* **Business requirements specification:**  Describes the characteristics of the systems from the point of view of the end users.
* **Project charter:** A first overview of the project. It defines roles and responsibilities and outlines goals and objectives.
* **SRS:** A detailed description of the software solution, including fucntional requirements, non-functional requirements, technical specifications, initial design and project plans.

1.2

The Information Systems Audit and Control Association (ISACA) suggest that audit objectives should be based on seven information criteria and then agreed upon by the organisation. Brief explain what they are.

**Answer**

* + The objective that an audit should achieve are well summarized by the seven information criteria as reported by The Information System and Control Association (ISACA) and are as follow:
* **Effectiveness:** Information should be relevant and pertinent to the business process and is expected to be correct, consistent, usable and delivered in time.
* **Efficiency:** Information should be provisioned with consideration for the optimal use of resources.
* **Confidentiality:** Sensitive information should be protected from unauthorised disclosure.
* **Integrity:** Information should be accurate and complete and its validity should be aligned with business values and expectations.
* **Availability:** Information should be available when required by the business process, which also involves safeguarding resources and associated capabilities.
* **Compliance:** Compliance with laws, regulations and contractual arrangements to which the business is subject, should always been respected.
* **Reliabbility of Information:** Information should be reliable and appropriate to allow management to exercise their financial and compliance reporting responsibilities.

1.3

Why is it generally better to have the audit team external to the development team? Which of the computer controls are we interested in for the Bazaar Ceramics Project? What are the subsets of the computer control.

**Answer**

An auditor removed from the development team guarantees a fresh, unbiased eye that is more likely to catch non-conformances in the system.

For a development team member, personally involved in the development of the product, it may be hard, if not impossible to objectively gather evidences, make judgement and reach conclusions based on those evidence.

For an auditor, credibility and reputation are tightly linked to the quality and accuracy of the reports produced for the management and being independent from the development team allows for an impartial analysis.

For the Bazaar Ceramics Project we are interested in the “System Development and Application Maintenance” control.

Its subset include:

* Corporate Policies and Practices
* User Requirements
* Feasibility Analysis
* Systes Design
* Systems Specifications
* Systems Development
* Implementation
* Post-Implementation

1.4

In order to develop the audit criteria, you should review? What are the most common legislative requirements for a website? Give a brief description of each.

**Answer**

The following is a list of the documents that should be reviewed to identify the audit criteria.

* Functional Requirements
* Technical Specifications
* Initial Design Documentation

This documents can provide the information needed to identify the criteria involved in the audit of a system, such as:

* Cost
* technical aspect
* performance
* overall quality.

There are also some legislative requirements that must be met.

* **Privacy:** The transmission, publishment, solicitation and collection of personal information on the internet is subject to the relevant privacy policies.
* **Restricted content:** Define the boundaries that identify sensitive or offensive content that may be restricted in some circumstances.
* **Copyright:** Regulates the use of copyrighted material on the internet, under the Cpyright Act.
* **Encryption and security:** Sensitive information and transaction transmitted over the internet may require security measures to ensure their protection.
* **Accessibility:** The 1992 Australian web accessibility law requires equal access to the web for people with disabilities, also reinforced in the 2014 Disability Discrimination Act Advisory Notes of the Australian Human Rights Commission.

1.5

Design a scope of Audit Criteria into metric for classification.

**Answer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Area of Audit** | **Scope of Audit** | **Audit Criteria** | **Testing** |
| **Website Implementation and Maintenace** | **Systems Development**  New website is developed consistent with management intentions and client expectations | The appropriate formal methodology or process is used to guide the development or maintenance of websites | * Identify if a development methodology is used * Sight a copy of the methodology or precedures * Request documentation to demonstrate adherence to a methodology |
|  |  | Skills and experience of the development team are adequate | * Interview the people involved in the development * Request training records * Review previous projects if available. |
|  |  | Version control is used effectively | * Identify if version control tools are used * Review the version control procedures * Examine file changes |
|  |  | Development time is reasonably close to estimates | * Compare documented timelines with development timelines. * Identify procedures to cope with requirements changes * Review damage control procedures |
|  |  | Changes to specifications are apported accordingly to a formal procedure | * Identify procedures to cope with requirements changes * Review damage control procedures |
|  |  | Resources allocated to development are adequate to accomplish the development’s objectives | * Review project plan * Identify resources allocation |
|  | **Specifications**  The website is implemented appropriately and fulfill the functional requirements and specifications | Websites are tested in accordance with test plan | * Identify if a test plan has been developed * Sight results of tests conducted * Re-perform tests on website objects |
|  |  | The project team has established formal procedures to ensure that before changes are made to the website, all stakeholders are contacted and the timing of modifications is coordinated with them, to ensure minimum disruptions. | * Identify contact procedures * Review contacts for completeness |
|  |  | The development and implementation of a website is monitored by the project team or management to ensure that the project meets the technical requirements | * Identify the technical requirements for the website * Identify how the project team monitor adherence and conformance to each technical requiremnts * Re-perform techniques |
|  |  | Websites development and maintenace occurs using a set of standards approved by project management (or client) to ensure consistency of development and maintenance activities | * Identify if a set of standards are used to ensure consistency * Identify methods of achieving consistency * Confirm consistency between website objects |
|  |  | Access to test and production environments are restricted appropriately | * Identify if development, test and production (live) environments exist * Attempt to access the test |
|  |  | Test are performed using a complete and representative set of test data | * Review functional requirements. * Technical specifications * Identify data set used to perform the testing |
|  |  | Implementation procedures include ensuring that operations, technical and user documentation are kept current and made available for appropriate personnel | * Interview people * Review documentation * Review accessibility policies |
|  |  | Websites are developed, modified and tested in an environment separate from the production or live environment | * Review version control procedures * Identify if development, test and production (live) environments exist * Attempt to access the test |
|  |  | Specifications are documented well and clearly | * Review User Requirements Specifications * Review Technical Requirements Specification |
|  |  | Hardware and software configurations are specified | * Review Technical Requirements Specification * Identify the hardware and software specified |
|  | **Design**  Websites are maintained and supportable | Website development and maintenace occurs using a set of standards approved by project management (or client) to ensure consistency of development and maintenance activities | * Identify company’s standards and regulations * Review previous projects procedures |
|  |  | Development staff are familiar with the standards, technologuy and tools used by the project team or organisation | * Identify company’s standards and regulations * Interview staff and personnel * Review records of distributed documentation |
|  |  | The design is flexible enough to cope with change. | * Review the design documentation * Review procedures to cope with change |
|  |  | The design produced meets the user requirements | * Review the user requirements specification * Review the test report |

On a general level, metrics are indicators that allow to evaluate the health of a product or a process. Following are some examples of what should be considered:

* **Capacity indicators:** Production / Time required
* **Input/Output indicators:** Input (Resources used) / Output (Quantity produced)
* **Quality indicators:** Total outputs / Standard conform outputs
* **Profitability indicators:** Profit / Total sale
* **Return on Investment (ROI) indicators:** Profit / Investment
* **Competitiveness indicators:** Company’s relationship with competition market
* **Effectiveness:** A combination of efficacy with efficiency
* **Value indicators:** Perceived value of something / Amount spent to obtain it

More in depth some of the metrics important to track for the development of a software product are:

* **Schedule variance:** Difference between scheduled and actual completion of an activity
* **Effort variance:** Difference between planned and actual effort required to comlete a task
* **Size variance:** Difference between estimated and actual size of a project
* **Requirement stability index:** Indicate the impact of a change in the requirements
* **Output - Productivity (Project):** Measure the output from a related process for a unit of input
* **Productivity (Test case preparation):** Actual number of test cases / Actual effort expended in testing
* **Productivity (Test case execution):** Actual number of test cases / actual effort expended in testing
* **Productivity (Defect detection):** Number of defects fixed / effort spent on defect fixation
* **Schedule variancce for a phase:** Deviation between planned and actual schedule for a project phase
* **Effort variance for a phase:** Deviation between planned and actual effort for a project phase
* **Cost of quality:** It measures the performance of quality initiatives in monetary terms.
* **Cost of poor quality:** Cost of the implementation of imperfect processes and products
* **Defect density:** Number of defects detected during development / size of the product
* **Review efficiency:** Efficiency in harnessing and detecting review defects during verification stage
* **Testing efficiency:** 1 – (Number of defects found during acceptance / total number of defects) X 100
* **Defect removal efficiency:** Efficiency of preventing defects to reach the customer
* **Residual defect density:** Total number of defects found by client / total number of defects found.

1.6

Determine audit methods and process to undertake review an Audit Assessment.

**Answer:**

There are different audit methodologies that can be adopted to perform an audit, which are as follow:

* Substantive approach
* System-based approach
* Transaction cycle approach
* Directional testing
* Risk-based approach

For the scope of this assignment the **risk-based** approach is reviewed in more depth.

In risk-based assessment, the focus is on those areas where the risk is more prominent rather than checking compliance with existing controls.

The risk-based approach allows to chose the subjects to examine, allowing to concentrate the usually limited resources in that field.

Audith Process:

* **Selection Phase:** Risk assessment. It may involve looking at the relevant documentation and previous audit result. It leads to the development of an audit plan.
* **Planning phase:** Audit objective and scope are determined
* **Execution phase:** The investigation is carried out by the auditor. Operational processes are scrutinized. Audit progress, osservations and potential findings are discussed when identified.
* **Reporting phase:** A summary of the audit results is produced and submitted to the client as a draft. The client can respond to the report by submitting an action plan and time frame that will be added to the final report.
* **Follow up:** A subsequent audit to follow up on the previous audit findings.

Audith Techniques:

* Identify the audit criteria
* Identify how to test the requirements
* Perform the test
* Record the test results.

Once the test results have been documented, together with their implications, an audit report is completed and handed over to the management. The report should include an overall statement of compliance/non-complinace and a summary of the isues identified, along with their implications.

1.7

List the resources to carry out Audit.

**Answer**

* **People:** An auditor may need to set meetings and interview people to carry out an audit.
* **Access:** The auditor may need access to protected systems that may require login credentials.
* **Equipment:** Some test may be required to perform the audit and may need appropriate equipment.
* **Documents that provide measurment criteria:** Functional requirements, Technical specifications, Initial design.

1.8

Develop Audit plan detailing objectives, scope, criteria, testing techniques and resources requirement will be undertaken

**Answer**

# Audit plan

**AUDIT SCOPE:** The softwre product development process.

**OBJECTIVE:** To determine the adequacy of the development process for the software product in relation to development strategy, security and QA

**AUDIT LOCATION:** Defines where the audit will take place.

**DATE AND TIME:** Specifies the date and time in which the audit will take place. It can also define the audit schedule.

**Acronyms and Abbreviations:**

**SDLC:** Software Developmment Life Cycle

**STLC:** Software Testin Life Cycle

**SAD:** Software Architecture Document

|  |  |  |  |
| --- | --- | --- | --- |
|  | CRITERIA | TECHNIQUES | RESOURCES |
| GENERAL | * Assess the company response to the findings of previous audit * Evaluate the organization to determine that the key functions are carried out effectively and efficiently * Determine wether the projects are managed in an effective way. | * Review previous external audit report. * Interview people with key responsabilities in the development process. * Review project plan | * Previous audit report. * Project manager, Analysts, Testers * Project plan. |
| DATA SECURITY | * Determine wether a data policy exists and is communicated to individuals in the organization. * Assess login properties * Determine who has access to database and security files * Determine the procedures to request and delete access to the system resources | * Review a copy of the data security policy. * Review the network logs * Test the login for a diverse range of users * Review the company procedures regarding system access. | * Data security policy * Data security procedures * Access to the system * Database administrator * Netwotk administrator |
| SYSTEM DEVELOPMENT AND APPLICATION MAINTENANCE | * Assess if the company has implemented a SDLC for the developmment of the software product. * The SDLC adopted defines User participation and sign-off, Acceptance testing, Well defined development stages, Documentation and deliverables. * Procedures to deal with sudden changes during development, are in place. * Version control is used effectively * Testing procedures and testing environment are in place. * Timelines are respected | * Review the SDLC adopted. * Review the deliverables produced for a previous project. * Review policies and procedures for change in the development * Review the STLC * Review the project plan with the timeline and resources allocated. * Review the test reports for a previous project. * Review the version control system adopted. * Interview development team. * Interview testers. | * SDLC * SAD * STLC * Test report for previous project * Project plan * User Acceptance Sign-off. * Project Charter * Business Requirements Document. * Access to the version control system. * Development team * Testers. |
| BACKUP/RECOVERY | * Backup and recovery procedures are in place * Backup is done regularly * Backup is done on dedicated storage. | * Review backup policies * Review backup copies of the system | * Backup procedures * Access to backup system. |
| CONTINGENCY PLANNING / DISASTER RECOVERY | * A business resumption plan is in place * The business resumption plan is tested regularly. | * Review the business resumption plan * Review the business resumption test report. * Interview management | * Business resumption plan * Business resumption plan tet report * Management. |

2.1

What is the two part process for collecting evidence? What does interviewing the development team (e.g. for a website development) achieve for testing methods? Why is it preferable to have more than one test for each requirement? Say suppose the auditor/s were testing a website. Why is it preferable to randomly select pages to test rather than pages selected from the developers?

**Answer**

The two parts process of collecting evidences:

1. Identify how to test the requirements.
2. Physically test the requirements.

Interviewing the development team allows the auditor to find out how the developers know that the product satisfies a given requirement.

Through an interview it is possible to identify if a well defined process is in place.

Each requirement should be tested more than just once, to ensure a comprehensive and reliable approach to the testing.

When testing a website an auditor should select randomly the pages to be tested. This is important because, if the pages test reports are arbitrarily chosen by the development team, they may offer only reports that they know they can produce.

Selecting random pages improve the chances that the testing process is regularly performed.

2.2

What should an audit plan include? What do resources include? What documents are typically used for measurement?

**Answer**

An audit plan should include:

* When the audit will be undertaken
* The objective of the audit
* The scope of the audit
* The audit criteria (requirements to be met)
* The resources required for the audit.

The resources for the audit usually include:

* People
* Equipment
* Access to systems and locations
* Documentation.

When talking about documentation we are usually referring to:

* Functional Requirements
* Technical Specifications
* Initial Design

2.3

Design a simple three column table format to document audit outcomes as audit progresses. Ensure in this table you put logical fields for the headings for each column. Note: You are finding out what was intended with the test in the first place. Hint: If I am an auditor, I need to know the following:

• What am I testing?

• What are the steps to testing the criteria?

• What are the results after I conduct each test?

|  |  |  |
| --- | --- | --- |
| CRITERIA | TECHNIQUES | RESULT |
| * The company took action in relation to the findings of previous audit * Evaluate the organization to determine that the key functions are carried out effectively and efficiently * Determine wether the projects are managed in an effective way. | * Review previous external audit report. * Interview people with key responsabilities in the development process. * Review project plan |  |
| * Determine wether a data policy exists and is communicated to individuals in the organization. * Assess login properties * Determine who has access to database and security files * Determine the procedures to request and delete access to the system resources | * Review a copy of the data security policy. * Review the network logs * Test the login for a diverse range of users * Review the company procedures regarding system access. |  |
| * Assess if the company has implemented a SDLC for the developmment of the software product. * The SDLC adopted defines User participation and sign-off, Acceptance testing, Well defined development stages, Documentation and deliverables. * Procedures to deal with sudden changes during development, are in place. * Version control is used effectively * Testing procedures and testing environment are in place. * Timelines are respected | * Review the SDLC adopted. * Review the deliverables produced for a previous project. * Review policies and procedures for change in the development * Review the STLC * Review the project plan with the timeline and resources allocated. * Review the test reports for a previous project. * Review the version control system adopted. * Interview development team. * Interview testers. |  |
| * Backup and recovery procedures are in place * Backup is done regularly * Backup is done on dedicated storage. | * Review backup policies * Review backup copies of the system |  |
| * A business resumption plan is in place * The business resumption plan is tested regularly. | * Review the business resumption plan * Review the business resumption test report. * Interview management |  |

3.1

Why is it important to review the system contract against the outcomes of the audit? Why is it important to ensure the audit testing is complete and accurate before comparing the system contract against the audit outcomes?

**Answer**

To ensure that the audit is comprehensive and accurate and assure the system, every test must be performed. If any gap between the testing methods and the audit objectives is found, more testing should be done.

Only when every aspect of the system, as defined on the system plan, is assessed, the auditor can decalre if the system complies or doesn’t comply.

The owner of the system relies on the accuracy of the audit report to ensure the quality of the processes and of the product.

3.2

What can be discovered by comparing system functionality against audit outcomes and system contract? Suggest a mechanism in IT development for correcting system functionality that has been found to fall short as according to audit outcomes and system contract.

**Answer**

When comparing system functionality against audit outcomes and system contract, non-compliances can be found. Those can be short-coming in the processes or a faulty functionality and can be found during the testing process or at the end of the testing in the audit findings.

The role of the audtor is that of a guide, helping to identify the best way to correct the non-conforming items.

In order to fix the problem, the problem needs first to be understood. Root Cause Analysis (RCA) can be used to uncover the real cause of the problem. RCA can show similar non-conformities that affect other parts of the system, helping to correct the non-compliance and preventing it from happening again.

Once the problem and its root cause has been defined and the actions to take to correct the problem are decided, a person in charge of the execution of the corrective action should be identified. The progress of the action should be monitored and appropriate procedures to report overdue action items should be in place.

A thorough follow up to ensure that the corrective action is effective is always reccomended.

3.3

Identify non-compliances based on contract requirements

**Answer**

When a non-compliance is found, the problem should be detailed as much as possible. The “what, where, when and how” relative to the problem should be identified and described in quantifiable terms to fully understand the situation.

Once the problem is clear in all its aspects, the root cause can be identified.

To identify the root cause, one of the methods that can be used is the 5-why method, firstly used by Toyota Motor Corporation.

Given a problem, the 5-why method implies to ask why the problem has occurred. Given the answer, it should be asked why what is stated in the answer happened, and so on for five times.

Once the root cause has been identified, the next step is to identify the appropriate correctivve action.

3.4

Name two scenarios for corrective action when non-compliance is discovered?

**Answer**

* The auditor can recommend a corrective action
* The implication of the non-compliance are discussed in groups. These often leads to the group developing their own corrective action, making it easier for the group members to accept.

It is important to note that a corrective action alone is not always enough and that “Risk Based Thinking”, or preventive action, should also be cosidered.

Corrective action, by definition aims at fixing the present issue and possibly prevent it from happening in the future.

Preventive action aims at eliminating the cause of a **potential** problem to prevent possible future issues.

The difference is that the corrective action applies to an unforseen issue that already exists. It can’t be avoided at present, just fixed and prevented from happening again. Preventive action instead propose to avoid the issue to begin with, and as such is an important part of risk management.

Following are two examples of corrective action:

* The products page takes to long to respond on an ecommerce website.

Corrective action: The number of reults per page can be reduced, minimizing the load on the server.

* One link on the page of a website is broken
* Corrective action: Fix the link and implement the appropriate link checking testing tools.

3.5

What should be included when documenting non-compliance?

**Answer**

* Test objectives
* Test Method
* Test Results
* Implications
* Reccomendation (Optional)
* Action Plan

**Reference**

1.2 [Isaca.org – information systems audit criteria](https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpisatt)

1.2 [Hci-itil.com – information systems audit criteria](https://hci-itil.com/COBIT/cobit_overview.html)

1.3 [careersinaudit.com – The importance of external auditor](https://www.careersinaudit.com/article/the-importance-of-external-audit-in-an-organisation/)

1.4 [cielo24.com – Australian Web Accessibility Laws and Policies](https://cielo24.com/2016/12/australian-web-accessibility-laws-and-policies/)

1.4 [humanrights.gov.au – World Wide Web Access: Disability Discrimination Act Advisory Notes](https://humanrights.gov.au/our-work/disability-rights/world-wide-web-access-disability-discrimination-act-advisory-notes-ver)

1.5 [heflo.com – Process performance metrics: A description of 8 of them](https://www.heflo.com/blog/business-management/process-performance-metrics/)

1.5 [simplilearn.com – Project and Process Metrics Classifying the Process Metric measurement](https://www.simplilearn.com/project-and-process-metrics-article)

1.5 [slideshare.com – essbaih Auditing Systems Development, INTOSAI Working Group](https://www.slideshare.net/essbaih/auditing-systems-development)

1.6 [pakaccountants.com – Difference audit procedure and audit methodology](https://pakaccountants.com/difference-audit-procedure-audit-methodology/)

1.7 [uniinstitute.com – Resources required for an audit.](http://uniinstitute.com.au/ica50615/15_respak/tocmenu/respak_index.htm)

1.8 [uniinstitute.com – Audit Plan](http://uniinstitute.com.au/ica50615/15_respak/tocmenu/respak_index.htm)

1.8 [eliftech.com – Software Development Process Audit Checklist](https://www.eliftech.com/blog/15-software-development-process-audit)

3.1 [softwaretestinghelp – CAPA | Beginner’s guide to Corrective Action Preventive Action](https://www.softwaretestinghelp.com/capa/#:~:text=For%20those%20readers%20who%20are,the%20most%20recent%20production%20deployment.)

3.2 [softwaretestinghelp – CAPA | Beginner’s guide to Corrective Action Preventive Action](https://www.softwaretestinghelp.com/capa/#:~:text=For%20those%20readers%20who%20are,the%20most%20recent%20production%20deployment.)

3.3 [softwaretestinghelp – CAPA | Beginner’s guide to Corrective Action Preventive Action](https://www.softwaretestinghelp.com/capa/#:~:text=For%20those%20readers%20who%20are,the%20most%20recent%20production%20deployment.)

3.3 [iso9001help.co.uk – Management system guidance 10.0 Improvement](https://www.iso9001help.co.uk/10.2%20Non-Conformity%20&%20Corrective%20Action.html)

3.4 [iso9001help.co.uk – Management system guidance 10.0 Improvement](https://www.iso9001help.co.uk/10.2%20Non-Conformity%20&%20Corrective%20Action.html)

3.5 [auditortraining.pwc.com.au – Corrective or Preventive Action – Risk based thinking?](https://auditortraining.pwc.com.au/corrective-or-preventive-action/)