MISA Information Management Summit 2024

Business Case Competition

[CipherLink]

Santos, Marianne B.
Diaz, Mark Eron A.
Dacalan, Paul Henry M.
Rance, Jorens Ivan C.

MISA Information Management Summit 2024 - Business Case Competition

Theme: Innovate to Elevate

Objective: A business case competition that promotes the value of IT in businesses by solving problems and developing business models leveraging IT

Timeline:

1. **April 20 [Day 1]** - Case Reveal via Zoom (1:30 - 2:30 PM)
2. **April 27 [Day 2]** - Workshop, ADMU (12:30 - 4:30 PM)
3. **April 28 [Deadline]** - Executive Summary submission (11:59 PM)
4. **May 2 [Announcement]** - Top 5 finalists
5. **May 3 [Deadline]** - Presentation slides submission (6:00 PM)
6. **May 4 [Culmination]** - Presentation and Awarding of winners, ADMU (12:30 - 5:00 PM)

Outline of Deliverables and Tasks

Challenge

Participants are challenged to craft solutions that not only tackle operational and competitive requirements but also provide value to the community and address its needs.

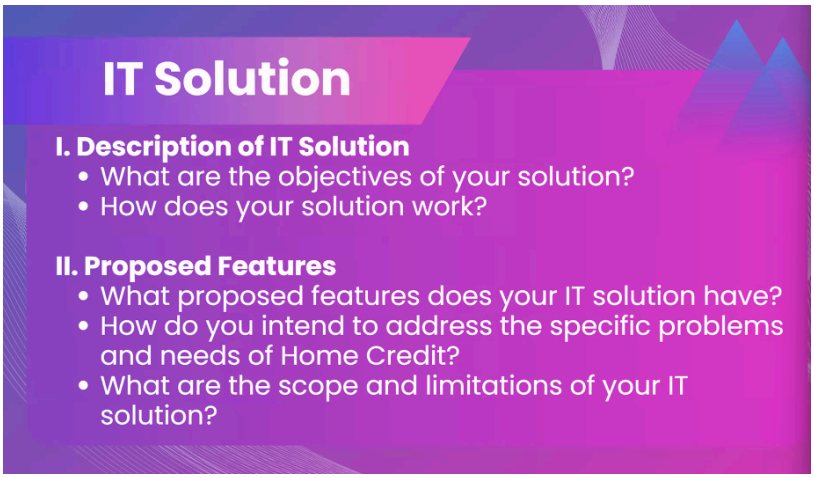
A solution is:

1. Feasible
2. Innovative
3. Impactful

Outline of the Business Case Proposal

1. **Brief Summary of the Problem Statement** - address the understanding of the business case and give context to your solution

2. **Executive Summary of the IT Solution**
   - Description of the IT Solution
     *What are the objectives of your solution
     *How does your solution work
   - Description of its Proposed Features
     * What are the problems that it solves and how does it solve them
     * What are the scope and limitations of your proposed solution



3. **Business Case Model**
   - Customer Segment
     *For whom are you creating value?

*Which stakeholders do you affect the most

- Value Proposition

*What Specific problems are you trying to address?

*How do you intend to address specific problems and needs of the customer through your solution?

*What are the qualitative and quantitative benefits of your solution and benefit realization?

- Key Activities

*What does your IT solution have that delivers the value proposition?

Top 5 Presentation Slides

Outline of the Presentation Slides

1. **Business Case Summary**
2. **IT Project Plan**
    - Visual Representation of the IT Solution (Flow charts, DFDs, etc.)

*Scope and Limitations

*Technology stack of your solution

- Business Model Canvas

*Customer Segments

Which stakeholders are most affected?

*Value Proposition

What makes your solution unique?

*Costs Structure

*Key Activities

*Key Resources

*Key Partners

What external stakeholders are involved?

*Channels (Not required)

*Customer Relationship (Not Required)

*Revenue streams (Not required)

Home Credit Business Case

Safeguarding Sensitive Data in Demand Letters and Statements of Account

Operational Terms and Definitions:

- Field Officers (FO) - in charge of field visits to clients
- Field Coordinators (FC) - issues SOAs and DLs to FOs
- Mobile Unified Communication Hub (MUCH) - a system used by FOs accessed through the MUF
- Mobile Utility Frontend (MUF) - an app used by FOs to access SOAs and DLs efficiently during field visits
- Demand Letters (DL) - letters demanding loan compensation from clients
- Statement of Account (SOA) - contains the payment history of clients
- Personally Identifiable Information (PII) - information that, when used alone or with other relevant data, can identify an individual
- Data Privacy Act (DPA) - an act safeguarding the confidentiality of client documents

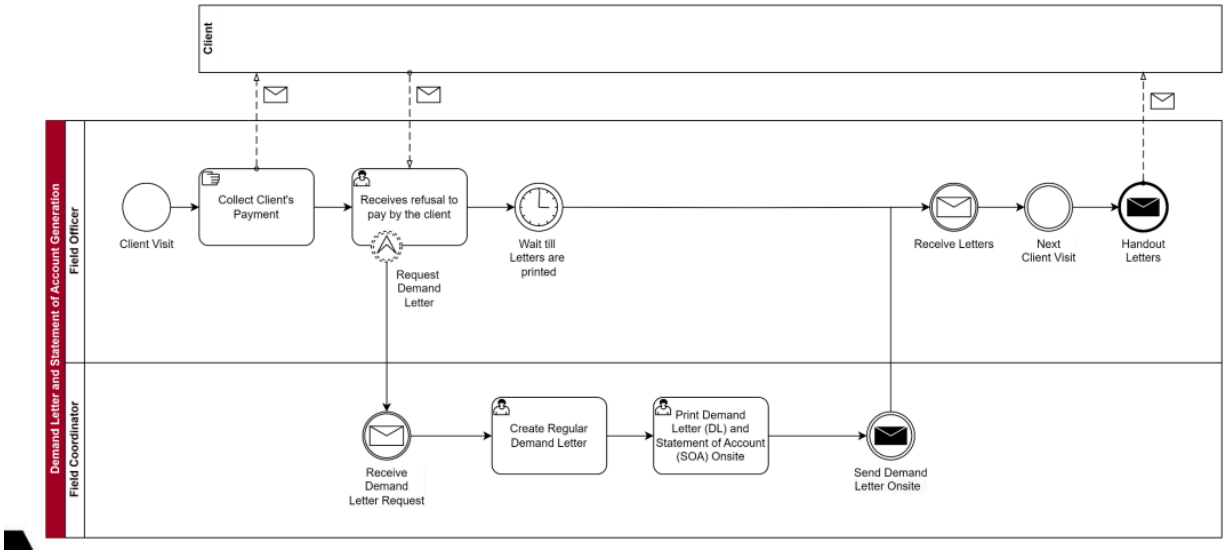
Overview

In-Home Credit Philippines, sending Demand Letters (DL) and Statements of Account (SOA) to Field Officers is crucial for debt collection.

In our current process, the distribution involves manual printing of DL and SOA at company offices. Field Officers were required to collect these documents from Field Coordinators before beginning their field visits.

This manual process led to delays and increased administrative burden for the Field Collections Team.

DL and SOA Process Map Generation Request



How do we plan to Improve this?

The automation project involved the development and integration of a system within the Mobile Unified Communication Hub (MUCH) used by Field Officers.

This system allowed Field Officers to access DL and SOA in PDF format directly from their MUF application.

Furthermore, it facilitated the seamless transmission of document requests to external printing shops for prompt printing when needed.

Identified Risks

1. Unauthorized disclosure/confidentiality breach

   Republic Act 10173 - Data Privacy Act of 2012

   SEC. 32. Unauthorized Disclosure.

   (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine

of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

2. Unauthorized processing

Republic Act 10173 - Data Privacy Act of 2012

SEC. 25. Unauthorized Processing of Personal Information and Sensitive Personal Information.

(a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

3. Access due to negligence

Republic Act 10173 - Data Privacy Act of 2012

SEC. 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence.

(a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

4. Improper disposal

Republic Act 10173 - Data Privacy Act of 2012

SEC. 27. Improper Disposal of Personal Information and Sensitive Personal Information.

(a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

(b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

Definition of terms

a. Data subject refers to an individual whose personal information is processed.

b. Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

c. Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:
(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

d. Sensitive personal information refers to personal information:
(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

Problem Statement

How can we best protect sensitive information in Demand Letters (DL) and Statements of Account (SOA) from unauthorized access or printing, and ensure secure handling from transmission to disposal?

Additional points to consider:

1. How can we keep sensitive information in DL and SOA confidential during transmission to the Printing Center?
    - To keep sensitive information in DL and SOA confidential during transmission to printing centers, the files can be encrypted using our proposed software to safeguard the contents with time-bounded and revocable OTPs.
2. What can be done to prevent the Printing Center from printing DL and SOA without the Field Officer's consent?
    - Similarly, printing centers are prohibited from reprinting the document as it is protected using encryption. The contents remain protected and free from copying, editing, and screenshotting once encrypted.

3. How do we prevent Printing Centers from accessing, reprinting, or using DL and SOA for unauthorized purposes?
    - To prevent printing centers from accessing, reprinting, or using DL and SOA for unauthorized purposes, layers of security protections including encryption, dynamic OTP generation, watermarking, and restricted file actions are placed to deter others from making any unnecessary and illegitimate actions toward the file.

4. What protocols should be in place to stop Field Officers from sharing DL and SOA with unauthorized individuals?
    - Protocols that would prevent field officers from sharing DL and SOA with unauthorized individuals include user education, restricted access, and accountability tracing through the auditing and logging mechanisms of the software.
5. Are there encryption methods or secure channels to protect DL and SOA during transmission to the Printing Center?

- Encryption methods include utilizing an OTP algorithm to safeguard documents from unauthorized access. Additionally, an in-app notification and tab feature is added to minimize the exposure of the generated passwords.

6. How can we set up monitoring and auditing to track DL and SOA transmission, printing, and disposal for potential breaches?
    - The monitoring and auditing to track DL and SOA transmissions include a database containing information such as the filename, timestamp of password requests and generation, the field coordinator generating and the field officer requesting, the area, success/failure of producing hard copies, success/failure of the client visit
7. What contingency plans should we have in case of unauthorized access, processing, or disclosure of DL and SOA?
    - In case of unauthorized access, all breaches must be assessed and taken down. Tracing of possible persons accountable for the breach will be done through the audit.

Criteria for Judging

- Functionality (20 pts)

  Does the solution meet the specified functional requirements?

  How effectively does it perform the intended tasks and operations?
- Presentation (10 pts)

  Is it explained clearly? Are its corresponding solutions conveyed with clarity?
- Scalability (10 pts)

  Can the solution accommodate growth in data volume, user base, or system complexity?

  How well does it scale in response to changing business needs?
- Security (20 pts)

  How robust are the security measures implemented to protect data and system integrity?

  Does the solution comply with industry standards and best practices for cybersecurity?
- Reliability (10 pts)

How dependable is the solution in terms of uptime, performance, and data integrity?

Has it undergone thorough testing to ensure reliability under various conditions?

- Innovation (10 pts)

  Does the solution incorporate innovative technologies or approaches?

  How does it differentiate itself from existing solutions in the market?

- Adaptability (10 pts)

  How easily can the solution be adapted or customized to meet changing business requirements?

  Is it flexible enough to accommodate future enhancements or modifications?

- Performance (10 pts)

  How efficiently does the solution process data, handle transactions, and respond to user requests?

  Are performance benchmarks met or exceeded?

Judges

1) Rahul Sharma

- Home Credit Head of Collections Technology, Al and Delivery
- Leads the design and deployment of Al-based solutions
- 30 years of experience in managing large scale Call Centre and IT operations

2) Reymundo Paga

- IT Technical Lead and Development Guild Leader
- Software Engineer and Tech Leader

3) Bryan Valenton

- IT BA Guild Leader, responsible for the IT Business Analyst community
- 30 years of work experience in various business sectors.
- System Support, QA Analyst, Business Analyst, and Project Manager.

4) Miguel Antonio Escolar

- Home Credit Agile Program Management Leader
- Diverse background ranging from manufacturing to HVAC design and property management
- [Achievements] Leads company-wide projects, implements technological solutions, and receives prestigious awards for outstanding contributions.

Cipherlink Delivery of Problem Statement and Identified Risks

How can we best protect sensitive information in Demand Letters (DL) and Statements of Account (SOA) from unauthorized access or printing, and ensure secure handling from transmission to disposal?

- Protecting sensitive information in Demand Letters (DL) and Statements of Accounts (SOA) from unauthorized access or printing, and ensuring secure handling from transmission to disposal may be well handled by protecting the PDF copies of DL and SOA in the MUCH system as accessed by the MUF app used by the Field officers.