White Paper

Authored by: L. Chris Bates - C.S.O. Bitland Global

01/11/16

Table of Contents

Contents

Project Outline

Mission

The mission of the Bitland Project is to register land and real property ownership and use rights in a secure, easily-accessible electronic format to allow for timely access of ownership and rights information, and to educate people on the importance of strong property rights in the prosperity of the nation.

Company Profile

Bitland Global is an organization that digitizes land titles. The larger goal is to have all the transactions recorded onto a distributed ledger using block-chain technology. The company is a non-profit organization that is working to keep the land registration process accessible, transparent, and free from government corruption. Bitland is located in Kumasi, Ghana, and is looking to expand operations into other countries in the African continent within the next few years.

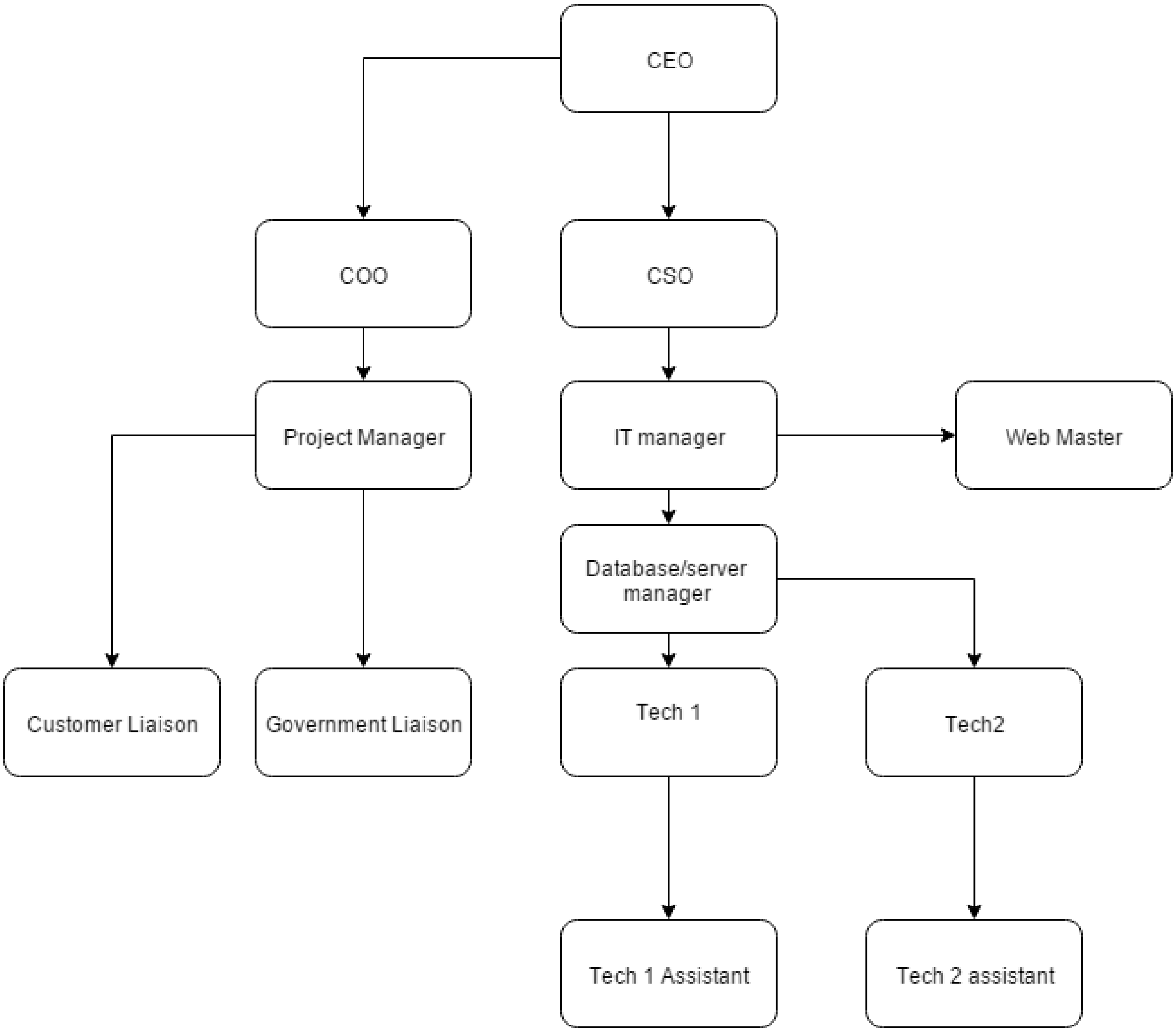
As the company works to update paper data storage houses into digital format, it must also consolidate new land registry requests against the old registries. In many cases, the official documents are outdated, and the locals have their own systems for keeping track of titles. In order to get a single registry that represents a consistent ledger of land title holdings, all of these problems must be solved, and in the process the integrity of the central registry must be kept. The Bitland team serves as the liaisons between the people needing to register land titles, and the officials that currently hold the access to the physical databases.

In order to effectively work through digitizing the backlogs while continuing to take in new registry requests, it will be important that the Bitland team establishes a work group that includes a representative from the government security team, and also from the community legal team. The Bitland Liaison will act as the representative to relay information and data between Bitland, the government official, and the local representative.

While the Bitland liaison does not report directly to the CSO within the Bitland organization, the CSO is still responsible for making sure that the liaison follows the policies and procedures of the Land Administration Project. The CSO will communicate with the Chief Operating Officer to coordinate the activities of the liaisons. These policies and procedures are the requirements necessary to ensure all of the land registrations are up to code and legal. The CSO must oversee daily operations of the database management and active security threats, so the direct reporting to the CSO is mainly the daily security briefings and activity.

In order to properly ensure communication between the working group within Bitland and the external liaisons, a very direct communication system must be developed (Security Program Best Practices, 2013). Having a working group communication hierarchy will ensure that the projects goals are reached, and the responsibilities within the organization are clearly defined and followed.

Bitland Global Organizational Plan



Security Requirements

Since there are many active threats and risks within the digital and real-world elements of this process, having a multi-faceted approach to security is crucial. This includes access control, encrypted data relay, incident response plans, incident response teams, system back-ups, solar power generators, and a dedicated private network. Since the company is working in areas where the infrastructure needs to be developed, it cannot rely on a local area network for data relay.

It will be necessary for the team to establish Bitland centers that house the hardware to support the Bitland network. In the pilot project, the team is looking to establish the first centers among twenty-eight communities around Ghana. The first phase of the project will be getting the communities to get their current titles up to date and any new areas surveyed. It will be imperative that the communities have unbroken access to the Bitland network, and local ISPs or electric companies are not reliable enough to ensure 24/7 access. In the case that the first phase of the project is successful, the team will look to establish more Bitland centers around Ghana to expand the network. The team has developed a four year implementation plan that looks to start with a local wi-fi network for the pilot communities, then establish metropolitan access networks which would give greater Ghana constant access to the Bitland network.

Cadastrals

Bitland Global llc. will be issuing digital tokens called Cadastrals. The Bitland team is currently in the process of establishing a blockchain based ecosystem in Ghana for which Cadastrals will be the entry token. As the Bitland team develops the ecosystem, individuals who have obtained Cadastrals will be able to use them to invest in the local economy and see real returns on their investment, as the team is establishing a system which will allow smart bonds and smart contracts to be created and utilized by governments, communities, organizations, and individuals. This system will open up new avenues for foreign investment into the region, while also establishing a transparent system in which these smart investments can take place without fear of corruption or nepotism.

Since there are many active threats and risks within the digital and real-world elements of this process, having a multi-faceted approach to security is crucial. This includes access control, encrypted data relay, incident response plans, incident response teams, system back-ups, solar power generators, and a dedicated private network. Since the company is working in areas where the infrastructure needs to be developed, it cannot rely on a local area network for data relay.

It will be necessary for the team to establish Bitland centers that house the hardware to support the Bitland network. In the pilot project, the team is looking to establish the first centers among twenty-eight communities around Ghana. The first phase of the project will be getting the communities to get their current titles up to date and any new areas surveyed. It will be imperative that the communities have unbroken access to the Bitland network, and local ISPs or electric companies are not reliable enough to ensure 24/7 access. In the case that the first phase of the project is successful, the team will look to establish more Bitland centers around Ghana to expand the network. The team has developed a four year implementation plan that looks to start with a local wi-fi network for the pilot communities, then establish metropolitan access networks which would give greater Ghana constant access to the Bitland network.

To get through the first year of operations, the team has allotted 20 million Cadastrals to be used in an ICO to establish the first operational Bitland Center. The ICO will be hosted by the Crypto Currency Exchange Denmark, and the funds will be held in escrow on the Openledger platform. In the process, Bitland would be establishing its own private network for the locals that would be faster and more reliable than what they currently have.

As the Bitland team registers the communities to start registering their land titles, the system will utilize a third party Oracle to validate the smart contracts. 3 Million Cadastrals will be allocated to be paid out in block rewards over the next 99 years. 2 Million tokens will be allocated to pay for Bitland Employees and independent contractors over 12 months of operations.

1 Million tokens will be sold through direct sales to establish a multi-currency reserve for the token. The reserve will hold funds in Bitcoin, US Dollars, Ghanaian Cedi, Yen, Euro, and will aim to accept the currency of any future country in which Bitland operates. 4 Million tokens will be set aside to sell directly to governments as the entry tokens to list contracts.

Governments will utilize the Bitland GUI to list contracts and create requests for bids that can then be listed for a contractor to claim. The Bitland System will utilize a double-blind bidding system so that the Government does not know who is bidding for the contract, and the bidder does not know the specific region of the contract or the owner of the contract. This will be to keep the process from being corrupted through nepotism, inflated bidding, or funds going to only a specific region.

The Breakdown of the Token Distribution and 4 year estimated budget needs are as follows:

Total Tokens:

-30 Million total tokens issued in 1 Block

Blockchain Explorer:

http://www.cryptofresh.com/a/CADASTRAL

Security Protocol:

-MIT Graphene/Openledger

Allocation:

-10 Million tokens for ICO at phase 1

-10 Million tokens for ICO at phase 2

-1 Million To Establish Basket of Currency Reserve during ICO Period

-2 Million to Pay Bitland Employees/Independent Contractors

-3 Million Designated to Smart Contract Oracles distributed over next 99 years

- 4 Million For Reserve for Governments to buy tokens, then pay out contracts through Bitland Global GUI/Hardware

	Estimated Cost
Year 1	**2186000**
Servers US and Ghana	100000
Air conditioning units for servers	16000
Office rental	120000
LAN essentials	120000
VPN	120000
VoIP dedicated hosting servers/service	80000
VPN tunnel to government servers	160000
Security systems	100000
Office Supplies and furniture	60000
Enterprise level enabled hot spots	60000
Salaries	700000
Survey drones	550000

Year 2	**1413000**
Generators/solar panels	160000
Metropolitan/urban Area network (WLANX)	500000
Salaries	650000
Office rental	120000
year 3	**1920000**
Multiple Metropolitan Area Networks	
Big Data Servers	1200000
Salaries	600000
Office rental	120000
year 4	**3120000**
Cube satellite network servicing entire country	2500000
Salaries	500000
Office rental	120000
Totals	**8639000**

The team uses a combination of decentralized data storage and traditional server warehouses for back-ups. The first iteration of this project uses MIT Graphene encryption for any data that is being transmitted across the network or stored. The system also runs regular integrity checks to ensure there have been no changes to data. This is crucial for ensuring the land titles are not registered to more than one owner. It also prevents any person or official from modifying it without taking direct responsibility. This will prevent any fraudulent activities, and any official working against the interest of the government for personal gain will be exposed through digital footprints.

Security Business Requirements

CMMI-

When defining the hierarchy of policy and procedure decision-making and implementation, the Capability Maturity Model Integration is a useful method of analyzing an organization's state. The CMMI allows a company to objectively rate the readiness of its individual departments to improve the process flow. The three different types of CMMI models include models for Development, for Services, and for Acquisition (Greiner, 2007). As well as having different types of CMMI models, there are different capability levels that define the readiness of each process area. These levels start at zero, and go to level three. In order they are:

Incomplete: This is a process that is incomplete for any reason. At least one of the goals of the process area is not complete.

Performed: At this level, the process has been completed, and the goals of the process area of been met.

Managed: At this level, the care is taken to make sure that the processes are monitored and any policies that need to be adhered to are known and followed. This level is important to make sure that policies and procedures are implemented top-down with consistency and integrity.

Defined: In stage three, the policies and procedures are well-known and established. Standards of practices are consistent company-wide, and processes are defined in more detail.

There are five levels of process maturity that are identified by the CMMI (Greiner, 2007).

Initial: This is the first phase or starting point for any new process.

Repeatable: This is the level for a process that is used repeatedly.

Defined: This is when the process has become officially defined as a standard business process.

Managed: This is the level at which process measurement and management occur.

Optimizing: This is the level at which analysis of the prior levels is implemented into optimization of a process.

Within the CMMI paradigm, there are Key Process Areas that are used to further elaborate on the five levels that have already been defined (Greiner, 2007).

1. Goals
2. Commitment
3. Ability
4. Measurement
5. Verification

For this project, the model that makes the most sense is the Development model. The Development model for CMMI encompasses all activities that constitute the actual delivery of a product or service. Within this model, the Process Area that should be the focus is Requirements Management (REQM). REQM is the method of obtaining all the requirements of the project to have an informed base of knowledge for planning, development, testing, and delivery. In the process of implementing the REQM, creating a transparent and centralized system to track system changes will simplify the monitoring process. As the system to track and document the REQM is developed, it will use a decentralized block-chain based approach to keeping track of the records. This will mitigate risk of file tampering and also lower the costs associated with data storage and data processing power.

It will be necessary to focus on the REQM process area, as this process area will be the foundation of the organization's service delivery. Establishing a system that is built with a focus on transparency, data integrity, and monitoring lays the foundation for Bitland's final product to make it easy for users to follow protocol. The generic practice that will be utilized is to establish organizational policies. Establishing organizational policies ensures that a standard method of approaching situations makes processes most efficient, and keeps all parties involved operating within all necessary parameters.

The specific practices necessary for Bitland to have long term success will include practices to ensure that users protect their respective data. A practice that will aide in this process is to utilize hardware based access controls for executing important operations. To prevent malicious agents from impersonating users through either man in the middle attacks, proxy spoofing, or other brute force methods, a hardware access control will allow multifactor authentication to be utilized.

The biggest goal of developing the REQM area is to establish the backbone of the Bitland system. This backbone includes a monitoring system that collects, stores, and publicly displays data. The first stage of the process will utilize the system to monitor progress of company-wide policy and procedure implementation. From there, the system will become the actual infrastructure for the Bitland organization's business operations.

Security Policy

In order to establish a culture that adheres to policies and procedures, it will be imperative to develop an extensive list of protocols for each area of operations. The policies and procedures should be considered a living document, and organizational training sessions will be held yearly to update all employees on any changes to policies.

General Policies – These Policies will be standard across the entire organization for all employees to follow (Koch, n.d.):

- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Ethics Policy
- Pandemic Response Planning Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Network Policies – These policies will need to be followed by any network administrators or anyone accessing the network (Koch, n.d.):

- Acquisition Assessment Policy
- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard

Server Security Policies – These policies will be in place to establish secure practices around server access (Koch, n.d.):

- Database Credentials Policy
- Technology Equipment Disposal Policy
- Information Logging Standard
- Lab Security Policy
- Server Security Policy
- Software Installation Policy
- Workstation Security (For HIPAA) Policy

Land Title Registration Policies – These policies are necessary to establish universal practices concerning registering land titles:

- Tenure Policy
- Ownership Policy

- Ownership Transfer Policy
- Government Registration Policy
- Local representative Policy
- Land Tax Policy

System Design Principles

To establish the integrity of the Information Security Architecture, it will be imperative to have a set of core principles that drive the continuous hardening of security. While there will be many principles that shape the security strategies, the following five principles will be the most important to keep constantly at the core of development.

1 – Secure the Weakest Link:

In the process of establishing levels of security, the adage goes “a chain is only as strong as its weakest link”. To ensure that the culture of the organization revolves around security, it will be important that every level from Government official to individual user understands the importance of maintaining secure channels, policies, and procedures. It only takes one breach point to open up a system to malicious attack, so all parties accessing the network should have proper information and training that focuses on staying secure (McGraw, 2013).

2 – Defend in Depth:

It is never good to rely on one layer as the end-all layer of security. Whether it is having multiple firewalls, multi-factor authentication, or biometric keys, the system should have multiple layers of security anticipating at least one will fail, and in worst case scenario multiple layers could fail. That will tie into the next principle of “failing securely” (McGraw, 2013).

3 – Fail Securely:

No system will ever be 100% impervious to malicious attacks. It will be important to establish this so when system failures do happen, the contingency plans have mitigated most of the risks, and the resulting impact to data is minimal to non-existent. Having the redundancies in the layers helps reduce the risks of failure causing enough damage to impede operations (McGraw, 2013).

4 – Grant Least Privilege:

To reduce risk of breaches affecting sensitive information, user access should be limited whenever possible. This adds a layer of security by limiting the penetration capacity of the breach point. Government officials may need to have access to more files than regular users, but this does not mean the officials won't have some restrictions on access. It will be extremely imperative to monitor access control, and ensure that the privileges are strictly given out on a necessary basis (McGraw, 2013).

5 – Separate Privileges:

This follows on the heels of the previous principle. It makes the process of granting privileges much easier to control if specific domains of control are separated. For example, everyone does not need to access the company's website to make changes. Privileges for something like this should be given to only those needing to make changes. Users and the proper government officials should be the only parties able to make changes or documentation of land titles. Making sure that the government officials who need access to titles is closely monitored will be necessary as well to ensure access control does not become a point of breach (McGraw, 2013).

Security Training Module

To ensure that the security principles are established through policy and procedure, the Bitland team will establish workshops for members of the organization, the government, and for the local community. Having the workshops that cover all the areas of security and organizational hierarchy will be imperative to establish a culture of integrity across the entire project. Everyone involved should be educated and informed so that their decision-making processes are not creating unnecessary risks. The following team members will be leading the different sessions.

Leadership Team

Narigamba Mwinsuubo	Founder and CEO
L. Christopher Bates	Chief Security Officer
Elliot Hedman	Chief Operating Officer and Project Manager
Brock Hager	Web Administrator

Support Team

Ryan Berry	Financial Advisor
Daniel Greene	Advisor
Alec Orrell	Advisor

Ambassadors

Philip Asare	Ghana
Chernoh Saeed Sow	Sierra Leone

Samuel Kanundi	Benin
Nana Y. Agymang	South Africa
Salim Iddrisu	Kenya
Achoteg David	Cameroon
Thorkozile Twala	Botswana
Campbell O. Akpata	Nigeria

References

Diploma In Security Management Outline. (n.d.). Retrieved from http://memberfiles.freewebs.com/68/25/62932568/documents/SECURITY MANAGT Outline.pdf

Koch, M. (n.d.). Information Security Policy Templates. Retrieved from https://www.sans.org/security-resources/policies/

Greiner, L. (2007, Oct 17). Capability Maturity Model Integration (CMMI) Definition and Solutions. Retrieved from CIO.com: http://www.cio.com/article/2437864/process-improvement/capability-maturity-model-integration--cmmi--definition-and-solutions.html

McGraw, G. (2013). Thirteen principles to ensure enterprise system security. Retrieved from http://searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security

Security Program Best-Practices. (2013, June 18). Retrieved

from https://nigesecurityguy.wordpress.com/2013/06/18/security-program-best-practices-2-2/

Software quality assurance within the CMMi framework: CMMi – Requirements management (REQM). (n.d.). Retrieved from: http://www.software-quality-assurance.org/cmmi-requirements-management.html