GoodSAM

ISO27001:2013
ISMS

ISO 22301:2012
BCMS

POLICY DOCUMENT

Version 2 October 2020

Table of Contents

1 INTRODUCTION

This document is the ISMS / BCMS Policy Document of GOODSAM. It is the property of GOODSAM and is a controlled document.

The purpose of the ISMS / BCMS Policy Document is to provide an overview of the company, the activities it carries out and the quality standards of operation it conforms to. It is not designed to act as a procedure manual, although it does carry information about where procedures information is located and the detailed information on Documentation Requirements for essential procedures e.g. document control, and control of records; internal audit and corrective/preventative action (please see Procedures Log).

Throughout this ISMS / BCMS Policy Document there are explanations of the requirements of the standards, paraphrased and appended in smaller grey text. This precedes a section explaining how the company implement this particular aspect of the standards.

2 ISSUE STATUS

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this ISMS / BCMS Policy Document. When any part of this ISMS Policy Document is amended, a record is made in the Amendment Log shown below.
The ISMS / BCMS Policy Document can be fully revised and re-issued at the discretion of the Management Team.
The ISMS / BCMS Policy Document will be reviewed on a Quarterly basis as standard.
Please note that this ISMS / BCMS Policy Document is only valid on day of printing.

Issue	Amendment	Date	Initials	Authorised
1	Version 1 – Author: Deepti Bal	09/10/2019	DB	MW
2	Version 2 – Author: Deepti Bal	30/10/2020	DB	MW

3

4

5 OVERVIEW OF GOODSAM

GoodSAM, established in October 2013, provide alerting and dispatch services to the emergency services industry globally. The GoodSAM service can be divided into three broad systems:

1) **GoodSAM Cardiac** operates through CAD integration and as stand-alone web-based platform, utilising applications to alert CFRs and other staff of nearby cardiac incidents. GoodSAM thereby quickly connects those in need with those who have the skills to provide support in the vital minutes before the emergency services arrive.
2) **GoodSAM Pro** is a sophisticated dispatching tool which provides enhanced functionality, by allowing application based activation of CFRs and staff as part of statutory dispatch. The system is highly flexible enabling Ambulance Services to retain total control over dispatch. The application provides a fail-safe tool to dispatch, communicate and stream scene video to and from CFRs; as well as providing real time mapping of staff and resources. The system also has joint command capabilities allowing emergency services to work together and share information/resource to better coordinate during major incidents.
3) **Instant On Scene** enables Services to enable video streaming by opening the camera and audio of any smartphone via text activation. Emergency Services, including Ambulance, Police and Air Ambulance Services are using the system to support dispatch. Users enter the caller's smartphone telephone number into the Dashboard (can be used as a standalone web based system or integrated into CAD), which generates a text. The text contains a hyperlink, which when pressed (and consent obtained from the caller), enables the camera and audio of the phone. The precise location of the caller is also identified, whilst live stream video contains Vital Signs

technology – the ability to determine an accurate pulse rate of multiple subjects in the stream.

GoodSAM Cardiac

GoodSAM Cardiac operates through CAD integration and as a stand-alone/web-based platform, utilising a smartphone application to alert those trained in CPR / first-aid to nearby cardiac arrests/emergencies. The platform has advanced realtime tracking, communications, defibrillator database and reporting functions. The system works globally with the world's largest ambulance services.

5.1 Features

- Smartphone based alerting of staff/co-responders/volunteers and resources
- Real time communications platform (text, audio and video)
- Customisable, kml map-based, geo-locating alerting system
- World's Largest Defibrillator Registry
- Customisable tiers / categories of responder
- In built File Storage platform
- In built "radio" channels/buzz messaging system - overrides silent
- Instantly stream video from responder to control/dispatch
- Patient Reporting Forms
- Comprehensive data analytics package

5.2 Benefits

- Mobilise community to provide first-aid / cardiopulmonary resuscitation
- Track / Deploy volunteer responders with customisable algorithms

- Improve patient outcomes following cardiac arrest / life threatening emergencies
- Comprehensive Defibrillator registry management system
- Obtain Metrics / KPIs for defibrillator on scene times
- Improve co-working with other public / charity services
- Learn from shared best practice of services on GoodSAM
- Save money on hardware (using individual's smartphones)

GoodSAM Pro

GoodSAM Pro is a Web/Smartphone Application based personnel management, tracking, communications and dispatch system e.g. for emergency services, co-responders/CFRs. The Responder application enables streaming of scene video and real time staff/resource mapping. The system has major incident / joint-command capabilities and applications in elderly care / long-term care management.

Features

- Smartphone based real time resource tracking and dispatch system
- Real time communication system (e.g. for individuals and major incidents)
- Real time secure video streaming platform (e.g. from scene/patients)
- Highly sophisticated integrated data analytics system
- In built patient report forms / incident report forms
- Highly configurable dispatch rules (select responders)
- KML Mapping options for different dispatch rules

- In built file storage facility
- Ability to book on duty / off duty
- World's largest defibrillator register

Benefits

- Effectively dispatch staff/responders using own their own phone/hardware.
- Effectively communicate with staff/responders using own phone/hardware
- Continuously map resources and personnel across organisations
- Joint command platform for major incidents
- Improve triage of patients through on-scene video to clinical hubs
- Improve patient pathways through remote care (managing range of conditions)
- Realtime analysis of data to monitor KPIs/arrival times / responses
- Communicate with staff/responders when off and on duty.
- Configure maps with icons to reflect specific each specific resource
- Vital Signs technology in video gives instant pulse/respiratory rate

GoodSAM Instant on Scene / Instant Help

Instant on Scene (Instant.Help) enables 999/111//101/Clinical Advisory Services to receive video direct from a caller's smartphone. Services enter a mobile phone number to generate a text containing a link. When clicked, video, audio and location data is shared into Emergency Service Control. No App required. Vital Signs are automatically measured.

5.3 Features

- Text enabled video streaming to view scene. No App required
- Simultaneously stream audio via phone and web.
- Receipt of text generates precise location of caller
- Email can also enable video streaming and audio
- Advanced video optimisation for poor data regions
- Video stream detects heart / respiratory rate of multiple subjects
- Works on all smartphones (iOS / Android / Windows)
- Optimised for public services firewalls
- AES-256 Encrypted, GDPR compliant
- Multiple video storage options (none, cloud, local) available

5.4 Benefits

- Video stream enables Emergency Services triage / prioritise
- Immediately geo-locate incident
- Improve efficiency of resource dispatch - upgrading or downgrading.
- Improve safety of staff dispatched
- Enables remote assessment with objective vital sign measurement
- Instant collection of evidence
- Secure video storage for patient record / evidence / review
- Enable guided earlier intervention
- Support staff/volunteers in field with optimised clinical decisions
- Improve Trauma / Stroke / Mental Health pathways

Clinic.co provides a platform which enables clinicians to provide video consultations to patients via their phone, tablet or laptop. Clinicians are able to send a link (via text or email) to establish a secure video bridge with the patient. The system works on any device, network and/or browser. The frame rate adjusts in cases of poor internet connection. Full information can be found in our brochure here: https://clinic.co/pdf/brochure.pdf

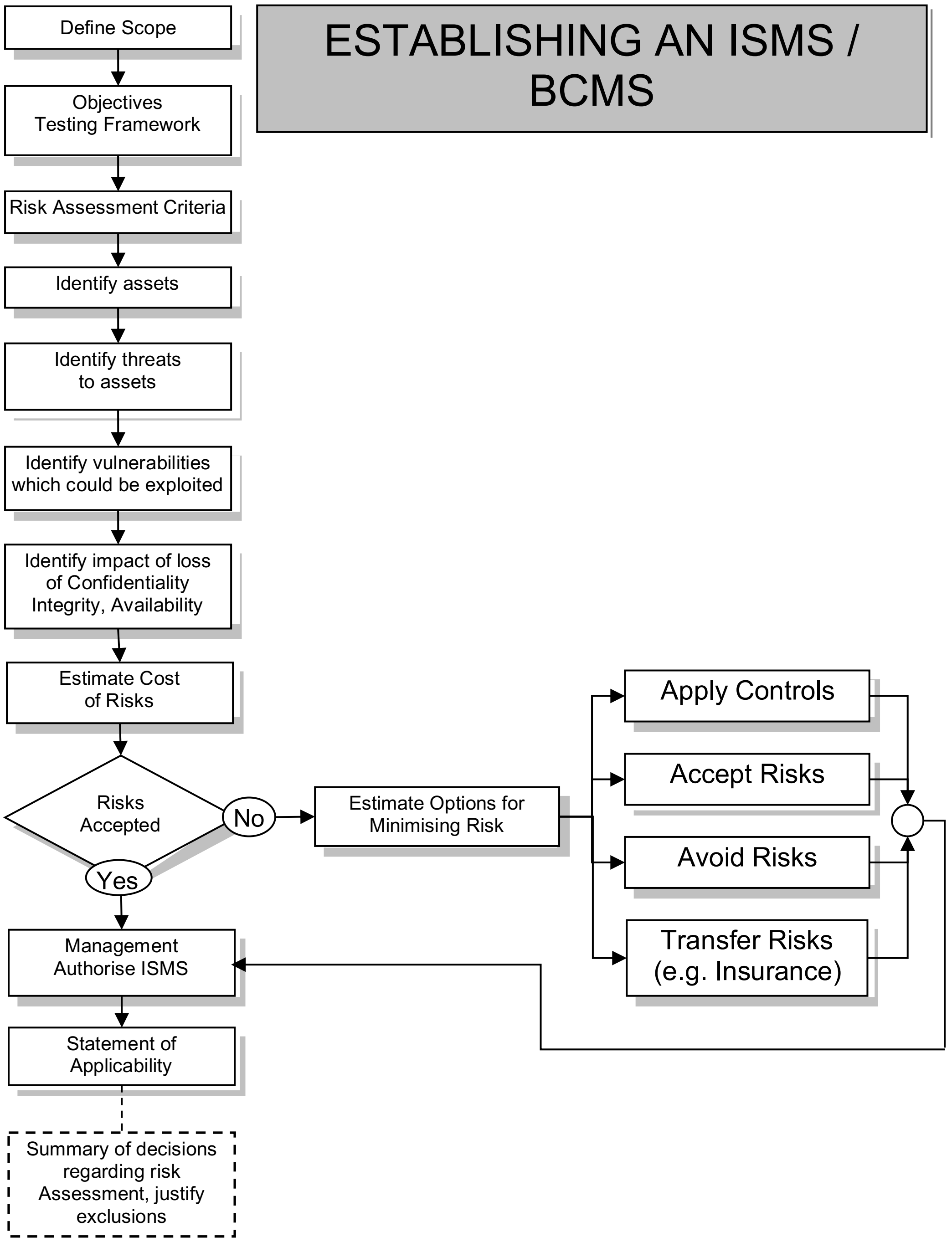
Specifics

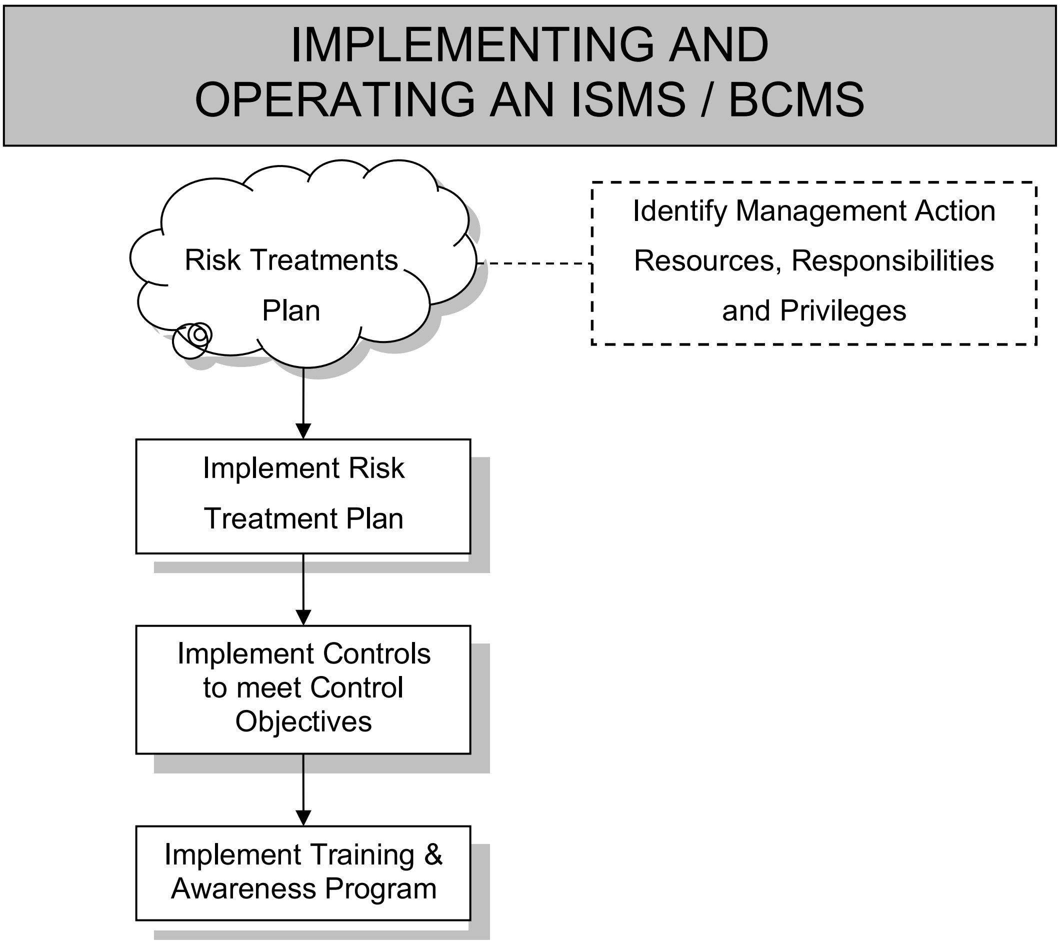
- Seamless video consultation
- Available on any cellular network, device (mobile, laptop, tablet)
- Clinician send patient text or email containing one time use hyperlink.
- At the time of the consultation, the caller clicks on the link and a secure video bridge is enabled.
- Consultation ends as soon as patient/consultant terminate the session.
- Ability to share screens
- Ability to monitor pulse reading
- Ability to set up MDT room with multiple users
- Ability to book appointments (bookable consultations)
- Blur background
- Pop out video
- In Built Billing and Accounting System
- Video Recording and Storage
- Organisational level for practices and hospitals
- Customise Text Invite
- Clinicians – searchable on clinic.co
- Analytics and reporting API Integration or web-based based system
- Delivered by API integration into client’s own patient management system or stand alone web based system.
- Branding option available so that system appears as seamless part of client system.
- Storage and Encryption
- No video data is stored on the patients mobile/Clinic.co server, unless requested.
- Data is AES 256 bit encrypted exceeding standards required by NHS and HIPAA - GDPR compliant and Clinic.co is registered with ICO.
- Recording - Video consultations can be recorded if requested by client.
- Video can be stored by clinic.co or API can be provided to enable video to be drawn from Dashboard and stored locally.
- Creation of clinician accounts: Multiple personalised clinician accounts can be created (requires clinician email address).
- IT Support - 24/7 Technical Support provided

5.5 Scope of Registration

Provision of alerting and dispatch technology to emergency service organisations - products are covered above: GoodSAM Cardiac, GoodSAM Pro and Instant on Scene and clinic.co.

6 INFORMATION SECURITY / BUSINESS CONTINUITY MANAGEMENT SYSTEM


Define Scope
Objectives Testing Framework
Risk Assessment Criteria
Identify assets
Identify threats to assets
Identify vulnerabilities which could be exploited
Identify impact of loss of Confidentiality Integrity, Availability
Estimate Cost of Risks
Risks Accepted
No
Yes
Estimate Options for Minimising Risk
Apply Controls
Accept Risks
Avoid Risks
Transfer Risks (e.g. Insurance)
Management Authorise ISMS
Statement of Applicability
Summary of decisions regarding risk Assessment, justify exclusions
ESTABLISHING AN ISMS / BCMS


IMPLEMENTING AND OPERATING AN ISMS / BCMS
Risk Treatments Plan
Identify Management Action Resources, Responsibilities and Privileges
Implement Risk Treatment Plan
Implement Controls to meet Control Objectives
Implement Training & Awareness Program

GoodSAM has a commitment to quality and a formal information security management system (ISMS) that addresses the following areas:

- Quality
- Performance monitoring and review
- Policy and Procedures
- Managing external relationships
- Financial Management
- Strategic and business planning
- Human resource development
- Service innovation.

GoodSAM has a commitment to quality and a formal business continuity management system (BCMS) that identifies, documents and addresses the following areas:

- The organisations activities, functions, services, products, partnerships, supply chains, relationship with interested parties, potential impact related to a disruptive incident, its overall risk management strategy and risk appetite.

6.1 Documented Information - Control of Documents

All documents (Statement of Intent) are maintained and controlled by the Project Director. Policy and procedure documents are reviewed annually. Any documents requiring amendment are updated, authorised, and completed. All updates to documents are signed and dated by the Project Director. Documents are re-issued as an electronic PDF document and a limited number of hard copies are produced. Obsolete documents will be archived and restricted by Project Director, electronic copies of all past versions are kept.

Documents and records of external origin which form part of the planning and operation of the ISMS / BCMS have been identified and controlled with processes in place to protect against for GoodSAM, compromise, unauthorised modification or deletion.

All managers hold responsibility for cascading information to staff.

6.2 Control of Records

All project documents (evidence of past performance) are stored in appropriate electronic folders and managed by respective departments. Hard copies of documents are restricted to a minimum and should not be produced unnecessarily. Electronic records are encouraged over hard copies due to environmental concerns, available storage space and to prevent unnecessary expenditure.

7 MANAGEMENT COMMITMENT

7.1 Role of Senior Management

The Senior Management Team is responsible for implementing the ISMS / BCMS and ensuring the system is understood and complied with at all levels of the organisation. Specific responsibility has been assigned where appropriate to ensure that the ISMS / BCMS conforms to the requirement of the standard and the provision to report on performance to the senior management team has been defined.

Management are responsible for ensuring that:

- All staff are aware of the policies and objectives of the organisation and in line with the strategic direction of the organisation.
- Understanding and Integration of the ISMS / BCMS into the organisations processes is delivered and understanding service user and interested party requirements and expectations.
- That resources needed for the ISMS / BCMS are available, time is used efficiently and to Contribute to high levels of morale and motivation within the organisation.
- All involved are committed to implementing GoodSAM's Information Security and Business Continuity Management Systems by direction / support of individual contributions.
- Internal and external Communication covering the importance of effective information security / business continuity management and conformance requirements are in place
- The ISMS / BCMS achieves its intended outcome(s) and that continual improvements are promoted.
- Understand their area of responsibility and other management roles within their area of responsibility are supported.
- All involved are committed to implementing GoodSAM's Information Security and Business Continuity Management Systems by direction / support of individual contributions.

- Understanding how statutory and regulatory requirements impact on the organisation and service users and to reduce wastage

GoodSAM's Information Security & Business Continuity Management System is managed by the Project Director, although ultimate responsibility is with the Co-Founders. All staff are required to maintain the system and to have a stake in improvements to efficiency.

An internal audit of procedures and policies is conducted annually in September. A review of the Information Security / Business Continuity Objectives takes place in January. In addition achievement of the quality objectives are measured against quarterly targets set in relation to the business plan. Staff contribution towards the Information Security / Business Continuity Objectives is measured in supervision and documented annual appraisals.

8 ISMS / BCMS POLICY

8.1 Introduction

This document is the Information Security Policy & Business Continuity Policy for GOODSAM. It describes the company's corporate approach to Information Security and details how we address our responsibilities in relation to this vital area of our business. As a company we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.

Information Security is the responsibility of all members of staff, not just the senior management team, and as such all staff should retain an awareness of this policy and its contents and demonstrate a practical application of the key objectives where appropriate in their daily duties.

We also make the details of our policy known to all other interested parties including external where appropriate and determine the need for communication and by what methods relevant to the information security management system. These include but not limited to customers and clients and their requirements are documented in contracts, purchase orders and specifications etc.

Verification of compliance with the policy will be verified by a continuous programme of internal audits.

8.2 Scope of the Policy

The scope of this policy relates to use of the database and computer systems operated by the company at its office in London, in pursuit of the company's business of providing alerting and dispatch systems to emergency service providers. This includes the organisations activities, functions, services, products, partnerships, supply chains, relationship with interested parties, potential impact related to a disruptive incident, its overall risk management strategy and risk appetite. It also relates where appropriate to external risk sources including functions which are outsourced.

Integration – we maintain flow charts which illustrate key business activities and their correspondence to ISMS requirements.

8.3 legal and regulatory obligations

Social Action, Responsibility and Heroism Act 2015

Data Protection Act 2018

National Insurance Contributions Act 2015

Small Business, Enterprise and Employment Act 2015

National Minimum Wage Act 1998

The Pensions Act 2008 (Commencement No. 16) Order 2018

The Employment Rights Act 1996 and Pension Schemes Act 1993 (Amendment) Regulations 2017

Workplace (Health, Safety and Welfare) Regulations 1992

The Employment Rights Act 1996 and Pension Schemes Act 1993 (Amendment) Regulations 2017

The Working Time Regulations 1998 as amended

Employers Liability (Compulsory Insurance) Act 1969 and the Employers Liability(Compulsory Insurance) Regulations 1998 as amended

Health and Safety at Work etc. Act 1974

8.4 Roles and Responsibilities

Top management ensures, roles, responsibilities and authority are assigned and communicated within the organisation and that the management systems comply to the standards.

Our Project and Operations Director is responsible for reporting on performance, randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

It is the responsibility of all staff to ensure that all data is treated with the utmost confidentiality, and that no data is given out without the prior authority of any person affected.

8.5 Strategic Approach and Principles

8.5.1 Information Classification

All staff have access to the GoodSAM database which is structured to have different access levels. This is overseen by the Technical Director to ensure permissions to access data is appropriate and activity is monitored.

8.5.2 Access Control

All user accounts are the differentiated according to role.

Passwords MUST NOT be written down either on paper or retained electronically. Passwords are changed on a six monthly basis. Passwords are no less than 8 characters in length and consist of both numbers and letters.

8.5.3 Incident Management and Response Structure

Any and all incidents are reported immediately to the Project Director who also fulfils the role of Information Security / Business Continuity Manager and is responsible for any appropriate warnings and communication.

8.5.4 Physical Security

Access to the office via one separate lock on the internal door and one on the main door. All data is held on remote servers located within an outsourced data centre which has ISO27001:2005 level security in place.

8.5.5 Third-party Access

No party third access is available without specific contractual arrangements defining access, confidentiality, purpose and use.

8.6 Business Continuity Management - Systems

We use multiple servers with regular backups.

The GoodSAM Platform is built using micro-service architecture which is the bleeding edge industry standard. (Rather than being one monolithic which cannot be changed, load balanced, scaled, improved or continuously deployed.) The four important micro-services which form the platform are the App servers, Web servers, Cad servers and Media servers. The following is concise explanation of each micro-service:

App servers: Are responsible to power the mobile applications which are provided by GoodSAM. This include, but are not limited to GoodSAM Alerter and GoodSAM Responder available on Apple Store, Google Play and Windows store. These apps can be used to upload new defibrillator, add additional detail to existing defibrillator, view them or report them.

Web servers: Are responsible for powering the GoodSAM website, the web-based defibrillator tool and the admin portal provided to over 50 organisations. The portal has many functions for organisations including the ability to view and approve defibrillators.

Cad servers: Are responsible for facilitating various communications with the organisations

Computer Aided Dispatch systems. We use REST based services to enable this

communication which is extremely easy to work with. We are currently integrated with 7

type of CADs (including MIS, Cleric, Infrograph) and have been enhanced overtime to talk to

many more CADs.

Media servers: Our media servers are responsible for rendering, handling, compressing,

resizing and securely storing the media files handled using the platform. This can be, but is

not limited to, defibrillator images, training material and on scene video.

8.7 Approach to Risk Management

We have carried out a full risk assessment of the potential for a breach of security as documented within our separate Risk Assessment Document. We have further identified, analysed and evaluated the risk of disruptive incidents which may adversely affect the organisation.

We aim to reduce all opportunities for data to be compromised. This includes the possibility of theft of data.

8.7.1 Action in the event of a policy breach.

Access to the system is centrally controlled and removal of access to the system is a very simple procedure, which is controlled by the Technical Director. Access to the premises is also controlled by the Top Management. Door entry access fobs and a particular fob can be disabled if required. Immediately upon a policy breach being detected any relevant user is either removed or reset depending upon the most appropriate action in the circumstances.

8.8 Information Security / Business Continuity Objectives

Our objectives are set below and are then disseminated to all staff. Each department is responsible for delivering its objectives and this is monitored via individual, appraisals & team meetings. GOODSAM's Quality Objectives are as follows:

Objective 1: Existing services - GOODSAM will continue to deliver its services within a secure environment ensuring all policies are being applied consistently.

Objective 2: Development - GOODSAM will conduct annual risk assessments to ensure that risk to information in the care of GOODSAM is minimised or eliminated and that any risk / incident which could pose a threat to business continuity has been identified and the potential for occurrence mitigated.

8.9 Responsibility, authority and communication

The team structure of GOODSAM is shown as an organisation chart (see Appendix 1) the chart shows functional relationships and responsibilities. GoodSAM operates a lean business model employing contractors where needed. At the time of this report, there is one full time employee and two part time employees.

8.9.1 Management Representative

The Project Director is responsible for the maintenance, measurement and review of our Information Security & Business Continuity Management System. The Project Director will ensure that the processes needed for the Information Security & Business Continuity Management System are established, implemented and maintained within GOODSAM. In addition he/she will report to SMT about system performance.

8.9.2 Internal / External Communications

Senior management utilise GOODSAM's internal / external communications framework in order to disseminate information about the effectiveness of the Information Security & Business Continuity Management System and determine what it will communicate, when and to whom.

8.9.3 Implementation

Following the annual audit, results will be collated and disseminated through GOODSAM's internal communications framework:

8.10 Management Review

8.10.1 General

Senior Management ensures:

- That the ongoing activities of GOODSAM are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process
- Measurement of GOODSAM's performance against our declared Information Security & Business Continuity Objectives
- That internal audits are conducted regularly to review progress and assist in the improvement of processes & procedures. The reviews will be discussed as part of GOODSAM's SMT meetings
- That employees have the necessary training, support, specifications and equipment to effectively carry out the work.

The management team hold planning and review meetings every month. Minutes of these are taken and the agenda normally includes an update and discussion around the current work of all departments and services.

8.11 Review Input

The monthly Senior Management Team meetings review the following information:

- Risk management and the status of risk assessments and treatment plan
- Results of audits
- Fulfilment of information security objectives
- Serious untoward incidents
- Status of preventive, non conformances, and corrective actions
- Follow up actions from previous management reviews
- Changes in external and internal issues that are relevant to the ISMS / BCMS
- Changes that could affect policies and procedures (Information Security & Business Continuity Management System)
- Information on performance and trends
- Recommendations / opportunities for continual opportunities for improvements.
- Feedback from interested parties

8.11.1 Implementation

- Meetings are scheduled
- Members invited to add items to the agenda
- Agenda is circulated to members
- Meeting take place
- Actions defined
- Meetings are minuted by a designated staff member
- Completion of actions is reviewed at the next meeting.

8.12 Review Output

The Senior Management Team reviews produce the following outputs:

- Policies and procedures are updated to make operations more efficient
- Operations and services are improved through measurement against targets and actions to improve or rectify specific areas.

- Update of the risk assessment, business impact analysis, business continuity plans and relate procedures
- Where resources are lacking actions are put in place to rectify this.

8.12.1 Implementation

- Non Conformance / Corrective actions are identified
- Targets created
- Improvements auctioned to support the suitability, adequacy or effectiveness of the ISMS / BCMS
- Situation re-evaluated at a specified later date.

9 PROVISION OF RESOURCES

GOODSAM will provide all the resources needed to implement and maintain the Information Security & Business Continuity Management System and improve effectiveness of the system. GOODSAM will also ensure that the resources needed to enhance the satisfaction and requirements of service users, service commissioners and staff are identified and in place through audit and continual review.

9.1 Human Resources General

9.1.1 Competence, Awareness & Training

We maintain a detailed Training Matrix demonstrating who has received what training and when with specific emphasis on the key elements of the management systems.

9.2 Infrastructure

GOODSAM's buildings, workspace, and associated utilities are managed by the Co-Founders (Medical and Tech Director). The procurement and management of hardware, software and supporting services such as communication and information systems are also coordinated by the Co-Founder (Medical and Tech Director)

We maintain a detailed asset register, description and location or person to whom assigned.

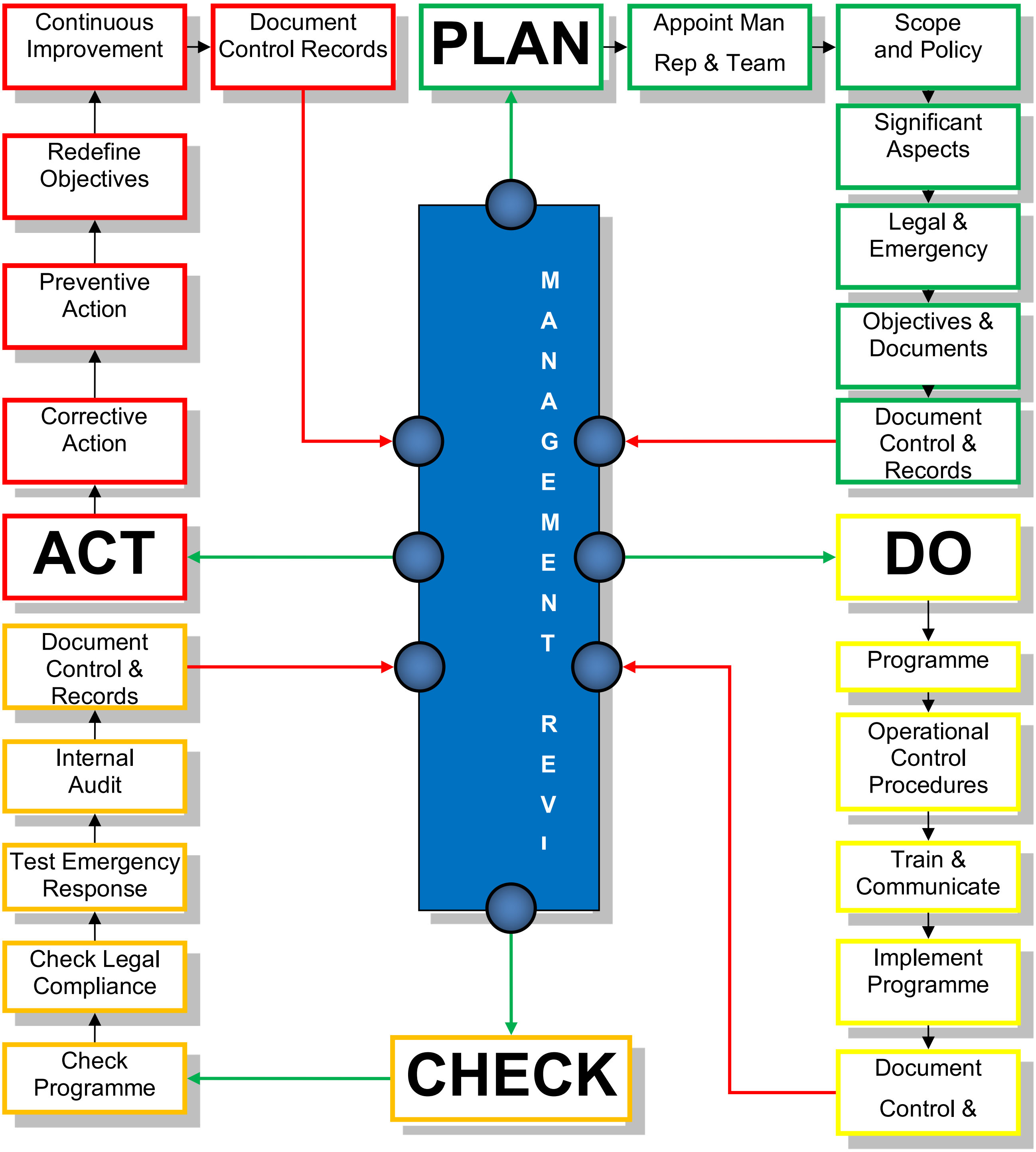
9.2.1 Implementation

Buildings, workspace and associated utilities requirements are regularly reviewed to ensure we make efficient use of office space. Both hardware and software is reviewed on an ongoing bases to ensure that head office staff are equipped with fit for purpose IT equipment and software.

IT systems are maintained and serviced by the Technical Director.

Head office prepares and distributes a wide range of information:

- Management Accounts
- Management & Performance information
- Training
- Company communications


Continuous Improvement
Document Control Records
PLAN
Appoint Man Rep & Team
Scope and Policy
Significant Aspects
Legal & Emergency
Objectives & Documents
Document Control & Records
Redefine Objectives
Preventive Action
Corrective Action
ACT
MANAGEMENT REVI
DO
Document Control & Records
Programme
Operational Control Procedures
Internal Audit
Test Emergency Response
Train & Communicate
Check Legal Compliance
Implement Programme
Check Programme
CHECK
Document Control &

10 RISK ASSESSMENT METHODOLOGY

We have identified the following process as a means of conducting regular risk assessments relating to Information Security Issues.

Within each of these areas the risks (if any) are identified together with a rating as to the importance of the risk. The associated consequence or severity of the risk is also rated together with the probable likelihood of the risk occurring.

We use an Excel spreadsheet to collect and analyse the risks identified in the following assets / asset groups :

- Buildings, offices, secure rooms security
- Hardware – desktops. Laptops, removable media
- Software applications
- Infrastructure / servers
- Client information and data
- Paper records
- People and reputation
- Key contacts
- Critical third party suppliers
- Utilities

All typical / likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) using a ratings scale of; Very Low - 1, Low – 2, Medium – 3, High 4 and Very high – 5 and expressed across key areas of Vulnerability, Probability and Impact

Following this analysis evaluations are drawn as to what the most appropriate action is together with the estimated cost of implementing action to address the identified issue and an estimate of the cost of ignoring the risk. Key evaluation criteria use is 1 – Accept risk, 2 - Apply controls, 3 - Avoid risk, 4 – Transfer the risk.

8 .1 Risk Treatment Plan – Statement of Applicability

The approach to our risk treatment plan has been designed and implemented using the main headings within the standard (Context risk opportunities and objectives) as a guide to establish that all controls required have been considered and that there are no omissions.

The document identifies controls to mitigate risks following the process of identification, analysis and evaluation described in section 7 and is directly linked to the aspects of the organisation.

This document is kept on the GoodSAM secure Teams drive.

11 MEASUREMENT, ANALYSIS & IMPROVEMENT

11.1 Information Security Standards

In all GOODSAM's services there are a specific set of quality measurements developed to be used to audit each service to enable a purchaser to be assured of the quality of delivery.

Service Level Agreements (SLA) are used to identify the areas of a contract that will be measured and monitored.

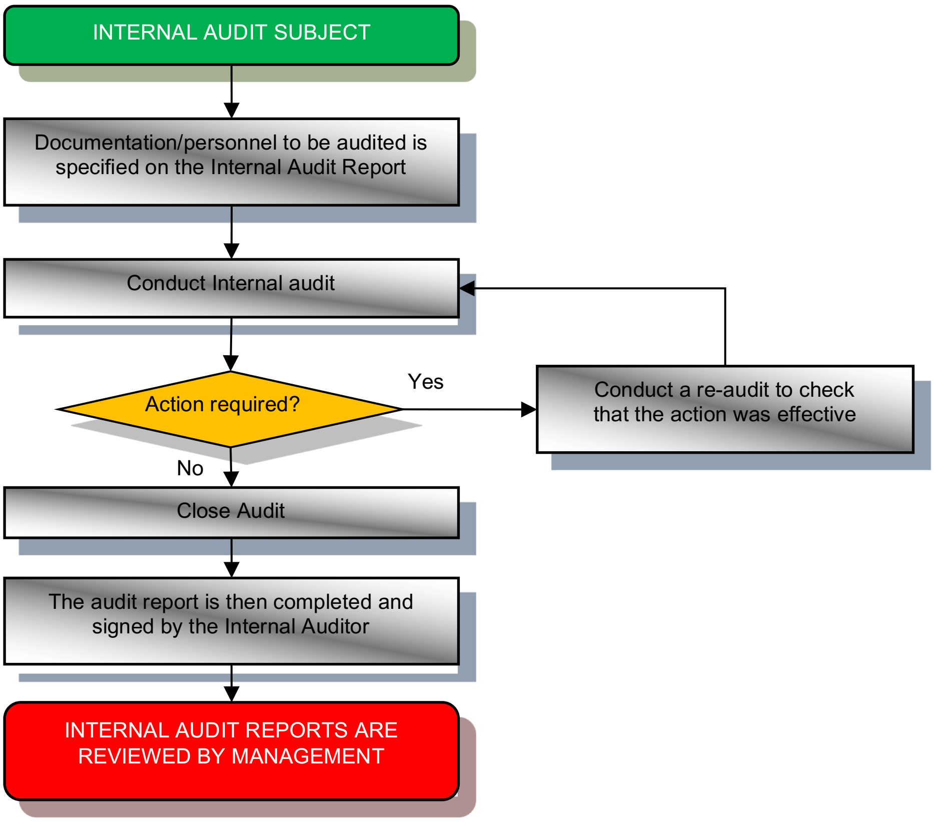
11.1.1 Implementation

We review our performance as part of a continuous review of Management Information. These reports help us to assess whether we are meeting our performance targets and provide us with month on month business performance benchmarking information. GOODSAM conducts annual audits, and provides quarterly reports to the Board of Trustees.

11.2 Internal ISMS Audits

The internal audit process is as follows:

11.2.1 Internal Audit Process Flowchart


INTERNAL AUDIT SUBJECT
Documentation/personnel to be audited is specified on the Internal Audit Report
Conduct Internal audit
Action required?
Yes
Conduct a re-audit to check that the action was effective
No
Close Audit
The audit report is then completed and signed by the Internal Auditor
INTERNAL AUDIT REPORTS ARE REVIEWED BY MANAGEMENT

11.3 Monitoring & Measurement of Processes

11.3.1 Implementation

Where the agreed requirements are not met, an action plan clearly detailing compliance will then be agreed with GOODSAM's Co-Founders with a timescale for compliance set at 6 months.

11.4 Monitoring & Measurement of Service

Our approach determines what needs to be measured inclusive of security processes and controls, the methods by which we ensure valid results, the periods and persons involved in conducting this activity and the reporting frequency and the responsibility for analysing and evaluating the results.

We retain all documents and records involved in this process.

GOODSAM establishes at the outset of a new service contract the reporting demands within the Service Level Agreement and/or contracts. This process will be supported with the data reports compiled and will enable the review to monitor performance, effectiveness of delivery, contract compliance and potential service developments. GOODSAM provides full information for this purpose on a quarterly and annual basis.

11.5 Analysis of Data

Incident logs are used to record any Information Security of Business Continuity incidents or breaches giving cause for concern, and these are regularly assessed during the Management Review process to identify areas for improvement.

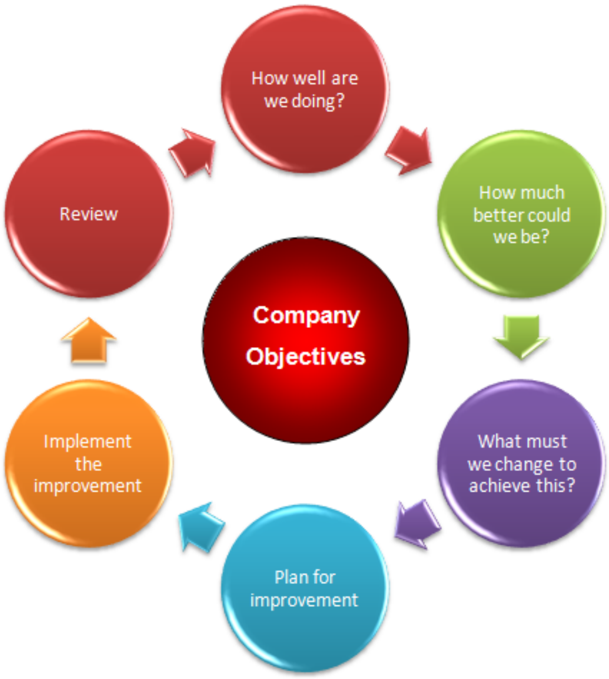
11.5.1 Implementation

The data is collected by services and submitted to the Project and Operations Director. Data is monitored by Senior Management.

11.6 Continual Improvement

11.6.1 Implementation

We review our performance as part of a continuous review of Management Information, service-user/customer feedback and comments. In particular we review our progress against our company information security & business continuity objectives (business plan aims), with a view to seeing what we can improve and where. The chart below illustrates this process:


How well are we doing?
How much better could we be?
What must we change to achieve this?
Plan for improvement
Implement the improvement
Review
Company Objectives

11.7 Corrective Action and Improvement

Both these areas are reviewed within the agenda for the Management Review meetings and typically cover the action taken to control and correct any non conformances noting any consequences of the action taken and themes which may be evident.

In terms of continual improvement, we also review the suitability, adequacy and effectiveness of our ISMS / BCMS

11.8 Complaints Policy

GOODSAM is committed to giving its clients the best possible service, involving them in the planning of their treatment, and giving them opportunities to air any complaints that they may have on the service we provide. To this end we operate the following procedure:

1. Direct all Complaints to info@goodsamapp.org.
2. Support will identify key information and report to the Project Director
3. Dates and key details will be logged and complainant acknowledged within 48 hours.
4. Project Director will review and a. respond to complainant to resolve the complaint or b. confirm with the complainant that further investigation is required within 48 hours.
5. Where b. Project Director to raise with Medical Director and agree course of action. Complaint shall be investigated within 14 days and complainant will be updated if investigations exceed this.
6. Project Director compiles a report summarizing findings and solutions to resolve the complaint. Report to be shared and signed off by Medical Director.
7. Report aiming to resolve the complaint shared with Complainant.
8. Where Complainant is not satisfied, Complainant will be referred to the Medical Director to resolve the complaint within 14 days.

9. Should the complaint involve the Project Director, the Medical Director will investigate the matter and prepare an investigation Report.
10. Should the complaint involve the Medical Director, the Technical Director will investigate the matter and prepare an investigation Report.

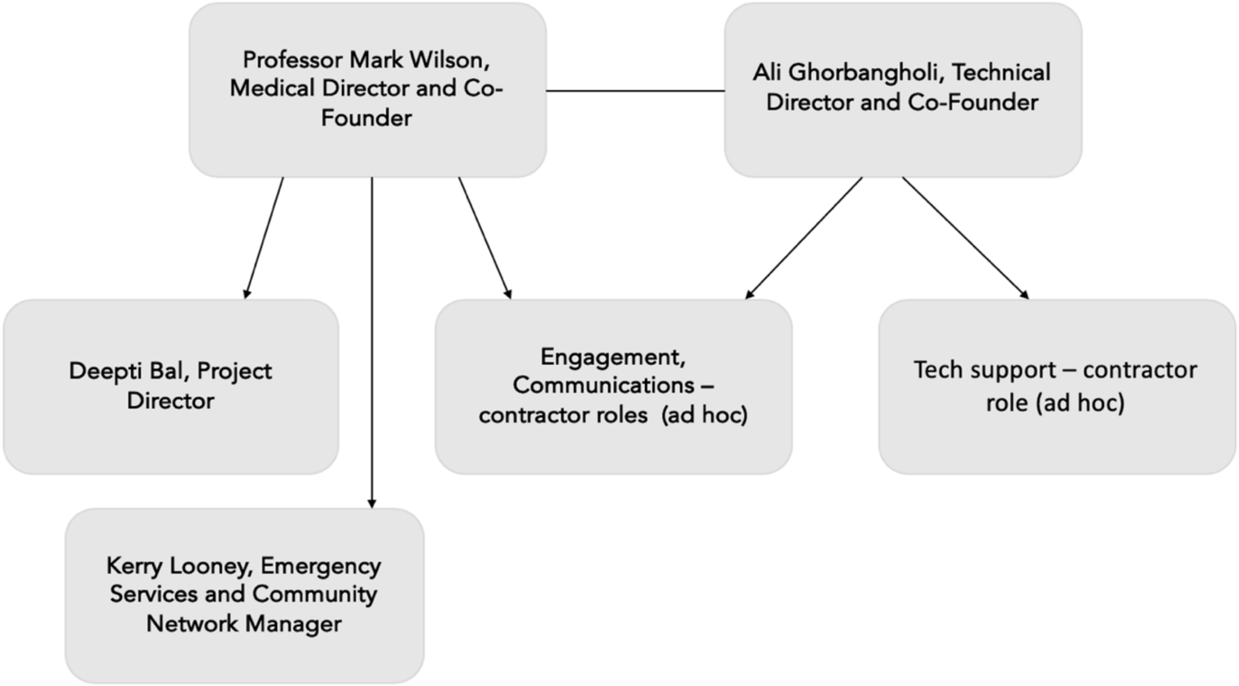
9.9 Preventative Action

GOODSAM has various processes and procedures in place to ensure that preventative action against nonconformities can be introduced, documented and seen through till completion to address the initial problem.
The complex nature of the clients we work with, demands that we have flexible but effective processes and procedures in place.

However, GOODSAM also uses internal and external audits and risk assessments to continuously improve its service delivery, financial, HR and operational functions.

12 APPENDICES

12.1 Appendix 1 – Organisation Chart


Professor Mark Wilson, Medical Director and Co-Founder
Ali Ghorbangholi, Technical Director and Co-Founder
Deepti Bal, Project Director
Engagement, Communications – contractor roles (ad hoc)
Tech support – contractor role (ad hoc)
Kerry Looney, Emergency Services and Community Network Manager