Chapter IV

Project Security

Chapter 4 Project Security

Information Security relates to the protection of information assets against the risk of unauthorised access, operational discontinuity, misuse, unauthorised disclosure, modification or damage. Information is considered as valuable assets of the organisations and should therefore be protected by ensuring Confidentiality, Integrity and Availability.

4.1 Policies not formally approved and adopted

Regarding the overall Information Security Environment, the K2 Project

(i) developed an Information Security Management System (ISMS), Information Security Policy and Information Security Procedures which are deliverables as part of the contract with the SI.
(ii) contained guidelines for Backup and Data Retention
(iii) merged Business Continuity and Disaster Recovery (DR) into a single functionality as set out in the Disaster Recovery Plan.

The K2 set up a disaster recovery site to serve the purpose of business continuity and disaster recovery. A Security Operations Centre (SOC) was also set up for security monitoring and incident management.

These Policies were to be reviewed and approved by the senior management for use in the project. The approval and acceptance of the documents prepared by the SI and the consultants for guiding the security operations, identity and access management was not made available to audit.

The Government stated (November 2021) that the documents prepared by SI had been vetted in the Technical Committee meetings.

The fact remains that the stamp of approval and acceptance of the documents for use in the project was not formalised.

The Government should ensure that established policies/guidelines are approved and periodically reviewed to enhance the security systems in place.

4.1.1 Determination of strategic control levels

The guidelines issued (2010) by Government of India mentions that Departments shall ensure Strategic Control over the e-Governance projects so as to enable the Department to have a complete control over the Strategic Assets like software application, databases and core infrastructure to ensure the capability of exit management. This includes expressing the Security Category (SC) of software application based on potential impacts to the organization. The Strategic Control category could be defined by considering the attributes such

as exposure to National Security, sensitivity of Governance workflow, criticality of data and information and the extent of financial exposure *etc*. The RFP of K2 project also envisaged a strategic control framework for review of the K2 application, database and network activities by Security Administrator from Government side and by a third party Auditor.

Audit observed that the strategic control level of K2 was not determined by assessing the sensitivity and significance of K2. A security incident management plan for identifying, recording, analysing and reporting of the security threats or incidents in real-time was also not prepared.

The security administrator envisaged as part of the K2 strategic framework was not deployed. Capability of the K2 system to respond to the security incidents were not demonstrated as the disaster recovery plans were not tested for its capability to switch over within the specified recovery time and point objectives.

4.1.2 Inadequate Security Audit

Section 43A of Information Technology Act, 2000 and Rules thereunder require the conduct of security audit by an independent auditor duly approved by the Central Government at least once a year or as and when significant upgradation of the infrastructure happens. Similarly, the guidelines issued by GoI on Data Centres (DC) advocate getting the security preparedness of the Data Centres audited by third party expert periodically (once in six months). The Security Audit should cover application, hardware, software and network components, security policies and their implementation, reviewing of the activities performed by management team, reviewing the access controls, reviewing the health check results, reviewing on the uptime of the services. Audit observed that the third party Security Audit of K2 covering application, network components was not conducted periodically.

The department stated that security audits were conducted eight times (Vulnerability Assessment and penetration testing - 3 times, web application security - 3 times, Firewall review-1, Audit of Application-1) during the period 2015- 2021. Scrutiny of the Security Audit reports showed that security audits covered only audit of web application security, the penetration testing and vulnerability assessment but did not cover the entire application, network and database security policies such as application functionalities, network components, access controls and data centre security. Since the periodicity and coverage of the Security Audit was insufficient, Audit was not in a position to derive assurance on the robustness of the security controls over the K2 application.

4.2 Identity and Access Management

Identity Management (IM) involves establishment and maintenance of user identities (IDs), associated authentication and monitoring processes to provide assurance that only authorized users are granted access to the system. Unique user identity also ensures that no user can repudiate a past transaction, *i.e*., the individual assigned to a particular user ID can be held accountable for the activity performed with that ID. K2 uses Biometrics and a Digital Signature

Certificate (DSC) based authentication mechanism to establish identification and non-repudiation.

K2 uses Role-based access control (RBAC) mechanism for permitting access to different classes of users. This involves setting permissions and privileges to defined roles and assigning the roles to various authorised users. Thus, the role determines which permissions the system grants to the users and limit access to specific resources or tasks.

4.2.1 Biometric Access

K2 employed biometric technology as part of the access control. An individual's measured biometric characteristics are compared to a database of authorized individuals to verify identity of the person who she/he claims to be. The biometric data of a K2 user should be mapped to the identity of the user within K2 and on successful validation of both; the user shall gain access to the system.

The Department stated that the False Acceptance Rate (FAR)[19] of the biometric device used in K2 is < 2% and False Rejection Rates (FRR) is 0.01%. However, the mechanism instituted for monitoring the performance of the biometric system, the analytical and monitoring reports in respect of the biometric sub-system, the reports on de-duplication of users based on biometric data *etc.,* were not available. These reports are important to monitor the devices and to ensure that FAR and FRR are within the prescribed limits.

Though, the daily users of K2 performing day to day operations were to be authenticated with biometrics, it was observed that the department users of K2 were not covered under biometric identification process. Excluding the department users from bio-metric authentication process thus resulted in a gap in the envisaged authorisation procedures.

4.2.2 Digital Signature Certificates

K2 adopted Digital Signature Certificates (DSC)[20] as part of its user identification and authorisation mechanism. K2 procures and distributes DSCs to all users and also permits use of DSCs issued by other departments of the Government. Maintenance of DSC mechanism include monitoring their validity, renewal before expiry, removing defunct DSCs safely, responding to forgotten passwords *etc*.

4.2.2.1 Delay in renewal of DSCs

A valid DSC is necessary for users to work with K2 and their timely renewal is vital to ensure smooth continuity of application usage. The MDM module captures and uses the DSC information user authentication. Audit analysed the

[19] FAR and FRR are the primary metrics for gauging the performance of a biometric system.

[20] DSCs are the electronic format of physical or paper certificates. DSCs serve as proof of identity of an individual for a certain purpose and can be presented electronically to prove one's identity, to access information or services or to sign documents digitally. DSCs are issued by a licensed Certifying Authority (CA) designated under Section 24 of the Indian IT-Act 2000. The Certifying Authorities are authorized to issue a DSC with a validity between one to three years.

data of 16,137 DSCs renewed during the period 2017-20 and noticed delays in renewal ranging from one day to more than 1,000 days. This was because the mechanism for monitoring the expiry of the DSCs was weak and K2 does not automatically initiate the renewal of DSC on the basis of prior information available on the validity of the DSCs issued. The MIS reports on DSCs were inadequate as it did not notify about the DSCs approaching expiry from time to time. Help desk data indicate instances of users seeking renewal of DSCs after expiry. It was also observed that in 617 cases the posts were delegated to other users citing DSC related issues. This reflected on the inefficiencies in DSC processing by the department.

The Department needs to monitor the expiry of the DSCs and renew the DSCs in time since without DSC the K2 users would not be able to perform their roles in the K2.

The Government stated (November 2021) that the DSCs are generally processed within three days of receipt of application by K2 PMU. Though Audit accepts Government response, there have been instances of delays beyond three days period up to 1,000 days and causes for such delays were not analysed. Audit also noticed delegation of posts has happened because of issues in DSCs which has to be resolved.

4.2.2.2 Difference in allotted and actual DSCs

K2 provides an MIS report 'Department-wise Number of Digital Signature Certificate (DSC) issued'. The figures as per this report did not match with the actual DSCs in use as per K2 database as indicated in **Table 4.1**.

Table 4.1: Difference in allotted and actual DSCs

Sl. No.	Financial Year	No. of DSCs issued		
		As per MIS report	As per database	Difference
1	2014-15	05	24	19
2	2015-16	1,054	2,644	1,590
3	2016-17	2,227	4,719	2,492
4	2017-18	1,373	2,819	1,446
5	2018-19	24,535	21,714	2,821
6	2019-20	13,080	14,065	985
7	2020-21	02	5,468	5,466

Source: Information as per MIS Reports and database

Variation in figures corresponds to unreliability of the database and absence of controls over maintenance and handling of DSCs. This can impact the authenticity of the transactions carried out using the DSCs.

4.2.2.3 Indented objectives of digital signature not achieved

As part of security requirements, the RFP states that the department intends to maintain highest level of integrity and responsibility fixing within the system and considers the need to remove any ambiguity in the authentication process by employing biometrics along with Public Key Infrastructure (PKI) towards this purpose.

Audit observed that a defined and documented sequence of steps was not available with the department to prove that a transaction was indeed signed by the signer in the event of the signature being contested or denied. It was observed that the digital signature process did not cover the entire voucher information including recipient name, bank account number *etc*. Audit further observed that the fields storing the Digital Signature Information were empty in respect of 225 fund releases transactions involving an amount of ₹26.74 crore undertaken during the year 2019-20. Thus, implementation of the digital signature process was insufficient to provide an assurance on non-repudiation and data integrity.

4.3 Privileged accounts not appropriately managed

Privileged accounts such as super user accounts present a high risk because of their level of administrative access. These super users may have virtually unlimited privileges, or ownership over a system that allows them to read/write/execute privileges, create or install files or software, modify files and settings and delete users and data. They may be able to change firewall configurations, create backdoors and override security settings and erasing traces of their activity. Organisations looking to protect super user accounts implement certain policies to regulate these accounts and document the controls implemented in the system to control privileged user activities.

The Department had neither established a procedure for Privileged Identity Management or Privileged Access Management nor had documented the need for such policy or procedure.

The Government stated (November 2021) that it was proposed to deploy a Privileged Identity Management solution to review the user access.

The Department needs to lay down processes and policies to control super user activities, periodical reporting of super user activity to PMU/appropriate representative of K2 management, policy in place to enforce separation of duties, password policy and the processes in place to monitor and audit all super user sessions.

The Government should ensure that K2 recognise the need to assess the access levels of super user accounts in the production environment and periodically review them for appropriate use.

4.4 Sharing of user credentials with helpdesk

Accounts shared with multiple users increase the risk of unauthorised access. K2 employs Single Sign On (SSO) as an authentication method. The SSO method allows users to use a single ID and password to access multiple software application services at the same time. This eases the burden of memorizing and entering passwords multiple times. In such an environment, it is highly important that organisation discourage the practice of password sharing amongst its employees to avoid exposure to password security vulnerabilities.

Audit observed instances of password sharing between users and helpdesk representatives as part of the helpdesk activities such as:

- Helpdesk team seeking User Credentials (User ID and Password) for resolving tickets.
- Users sharing their user credentials to the helpdesk team through portal/mail.

Such instances of sharing user credentials with helpdesk poses security threats.

The K2 should institute procedures resolving user issues without compromising the user credentials by providing controlled access to the help desk personnel using their own credentials. Disclosing user credentials undermines the fundamental principles of identity management and non-repudiation and is fraught with high risk in a financial management system.

The Government stated (November 2021) that this is a user awareness issue and users were advised not to share credentials with anyone.

Audit is of the view that considering the sensitive nature of the user credentials, Department needs to create awareness among the users and the helpdesk team as it impacts authenticity and non-repudiation of data.

4.5 Transactions by suspended/retired employees

All employees are mapped to their respective DDOs/CO/CCO. They should be de-mapped from the previous office and re-mapped to the new office through the process of check-out / check-in at the time of transfer/promotion/suspension/ retirement/death. In all such instances, the DDO/CCO/CO has to report to the treasury with the Karnataka Government Insurance Department (KGID) number of the employee for check-out/check-in. When an employee is promoted/ transferred within the same DDO/CCO/CO office, he has to undergo the process of check-out of his old post/designation and check-in with his new post/designation. An employee who is transferred from another DDO/CO will have to check out from that DDO/CO and check in at the new office he is reporting and the DDO/CO/CCO of the new office will have to map his KGID number with DDO code. Simultaneously, a parallel check-out/check-in process called transfer out/transfer in should be carried out in HRMS. However, the process does not spell out the steps to be taken to handle cases of suspension/ retirement/death.

Audit analysis of front-end screens and database showed that HRMS application was not fully integrated with K2. K2 fetches the data from HRMS while registering users. Non-integration of HRMS application for sharing data on a real-time basis thus adversely impacted the ability of K2 to manage the user access. The Department also needs to issue instructions for timely notification of the events like suspension, transfer *etc*., of the employees and users and update the applications in time.

4.5.1 Transactions by suspended employees

The HRMS application captures both the suspension and revocation of Government employees. However, the data does not get updated automatically as integration between the two applications was yet to be completely achieved.

K2 captures the suspension of an employee with the DDO, where the user (suspended employee) is posted, sends a request through a letter to the treasury linked to their office to de-activate the user in the application. The employee is then de-activated through the module for Employee Transfer/Retirement/ Suspension. Each posting, retirement, suspension entry has to go through an Organogram maker, verifier and approver to ensure a three-point check mechanism.

Audit analysis of the front-end screens showed that the system asks for separate notification date, order number and order date during addition of suspension records. The 'date of effect' field in the front end screen is frozen to the current date, and thus cannot be edited. The entry then passes through the Organogram verifier, before finally being approved by the Organogram approver. Moreover, the system was designed in such a way that the notification date and order date were to be earlier than the date of effect. It was observed that:

- 150 users had all the three roles *viz.*, maker, checker, approver and 205 users at least two of these roles, thus vitiating the separation of duties mechanism.
- there were three and five cases respectively where notification date and order dates were later than date of effect indicating that there were no validations on these fields.
- there were 22,201 cases where the notification date is earlier than order date; 4,866 cases where order date is earlier than notification date and 17,991 cases where they have the same value.

Since the requests from DDOs are sent through hard copies and not through K2, the person requesting the suspension and date of actual request is not captured in K2. In 254 cases there were suspension orders but no corresponding revocation orders and in 36 cases, there were revocation orders but no suspension orders. A total of 44 users were found to have both suspension and revocation orders, of which 10[21] users had processed 55 bills of various types worth ₹81.95 lakh.

K2 also allows transfer of suspended employees through the employee transfer module. Audit analysis showed that the transfer was allowed even when the suspension order was active. The transfer process revokes the suspension status of the user automatically, which should not be allowed in the system. Though the user may not be able to transact without posts being assigned to him after suspension, the assigning of posts can be done inadvertently as the Treasury user would now see the user as an 'active' user. There were 254 cases where the suspended users were transferred without revoking the suspension.

4.5.2 Transactions by retired employees

A script in the System is run manually on last day of every month to deactivate employees who retire on superannuation. Audit observed that the script checked if the current date was past 60 years from the date of birth of any employee and if the script conditions were satisfied, the status of the record was

[21] Audit considered the later of the notification date and order date as suspension date and the earlier of the two for reinstatement date.

deactivated and the system date inserted in the updated date field of related tables (org_user_mst, org_emp_mst, ifms_emp_post_wf_mpg, ifms_emp_mst, org_emp_post_mpg, ifms_employee_details_hrms_mst tables). However, it did not consider the conditions of retiring the employee on the last day of the previous month when the date of birth falls on first day of the month.

Analysis of the Employee Master table showed that a total of 10,144 records were found to be deactivated as of August 2020. While 8,783 users were deactivated within time, 1,361 users were deactivated with an average delay of 62 days. Such delay in deactivation resulted in continued usage of K2 application even after their superannuation and 166 users had processed 4,967 bills for ₹2,412.15 crore during the interim period between the date they were supposed to be deactivated and the actual date of deactivation.

It was also observed that for 2,039 records, the updation date which represents the date of deactivation was null. The system did not record the reasons for deactivation. While audit could determine the reasons for deactivation as superannuation in majority of the cases based on their date of birth, in respect of 802 records which were deactivated before the superannuation date of the employee, the reasons for deactivation were not verifiable from the data available in K2.

Ideally, the application should not allow the deactivated user to transact. It was observed that 4,938 bill transactions involving ₹154.57 crore were carried out by users after they were deactivated, of which 3,867 transactions took place during 2019-20. This was possible because all the relevant tables were not updated which allowed the users to login to the application.

Illustration

Shri Sudarshan K.S., Assistant Director, Education Department (User Id: 1232495467) born on 1 June 1960 was to retire from service on 31 May 2020. The user had processed 47 bills during July 2020 amounting to ₹4,54,194.

Issues with the database design were also noticed. The organogram employee master table contained fields for capturing date of termination, date of demise, date of resignation but there was no field for date of superannuation. The organogram user master table contained user Id -1 with username K II ADMIN which was deactivated on 16 January 2018. However, several transactions were carried by user Id -1 even after the date of deactivation. It was observed from the year end transactions script that user Id -1 was inserted for the users forwarding and receiving bills and created by and updated by fields for transactions de-activated on last day of the year. Since the scripts use -1 as Admin user, one would never know whether the transactions were done by the user K II ADMIN or done through scripts through backend. There was also no report providing the data of employees working/superannuated in an office within K2 for DDOs for viewing and verification.

The Government should ensure that K2 automates controls over predictable events such as superannuation and to institute procedures for timely updation of information.

4.6 User permissions not reviewed

K2 does not have either a mechanism to regularly review privileges and access to the system or a System Use Policy provision that require regular internal audits on all aspects of user access and use of K2. Audit noticed that the system cannot produce a report to assist with verifying whether the roles of its users are appropriate to the functionalities and job roles in the Department. In the absence of review of user access, there is an increased risk of unauthorised and inappropriate access remaining undetected.

The Government should ensure that K2 periodically review the user access to verify that only legitimate users have access to applications or infrastructure.

4.7 Data protection

Data protection is the process of safeguarding important information from corruption, compromise or loss. It is a set of strategies and processes used to secure the privacy, availability, and integrity of the data. It is sometimes also called data security or information privacy. A data protection strategy is vital for any organization that collects, handles, or stores sensitive data. A successful strategy can help prevent data loss, theft, or corruption and can help minimize damage caused in the event of a breach or disaster.

4.7.1 Data Retention

The Department was to formulate an appropriate Data Retention Policy (DRTP) to be guided by data classification and risk assessment of data, data retention period, data security aspects, disposal of data once the retention period is over and ensure that the data centre architecture supports the DRTP.

According to MSA, the Department planned to retain transactional data for a period of 10 years within the live database. The data for the period prior to 10 year retention period should be kept in an aggregated form in a separate database. The type of aggregations to be created over the data was to be identified by the SI and documented as part of the SRS document.

Further, the SI was required to backup all historical data prior to 10 years and remove them from the live database and should also restore the same as and when required by the Department.

It was observed that the Department is yet to formulate a Data Retention Policy and data sharing policy. Absence of the Data retention and data sharing policy is indicative of the non-recognition of the importance and potential use of the data available with K2.

The Government stated (November 2021) that the Data Retention Policy was under development.

4.8 Security and Incident Management

Enterprise Security has become increasingly vital for organizations and is critical for financial and accounting information systems. It refers to the process or actions an organisation follows to protect the data and information in their information systems. Enterprise security management involves identifying all associated risks, the required controls to manage the risks and preparing a

program to implement the controls. The program should provide for security architecture governance, policies and define physical security architecture.

4.8.1 Critical Information Infrastructure

Information Technology Act, 2000 defines Critical Information Infrastructure (CII) as a computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety. The Information Technology (National Critical Information Infrastructure Protection Centre (NCIIPC)[22] and Manner of Performing Functions and Duties) Rules, 2013 mandates that the basic responsibility for protecting CII system shall lie with the agency running that CII.

The NCIIPC has identified the Government among others as critical sector and laid down guidelines for identification of CIIs based on a set of parameters such as the total number of transactions per day, the value of all types of transactions per day, number of connected devices and network size, number of customers of different categories *etc*.

Keeping in view the above parameters, K2 qualifies to be identified and notified as CII. Audit observed that the department was yet to assess the criticality of the system and take measures to notify K2 as a CII under GOI guidelines. This deprived K2 project of an enhanced security infrastructure commensurate with its significance and criticality. The State Government stated (November 2021) that it would initiate measures to notify K2 as CII and place information security controls commensurate with the elevated status of importance.

4.8.2 Asset and Inventory Management

The NCIIPC brought out (January 2015) guidelines for protection of CIIs according to which one of the most important steps in the critical assets management and security is asset and inventory management which correlates all the physical and virtual critical assets owned by the CIIs. An asset inventory is important for managing maintenance, servicing, theft prevention, controlling system builds, performing regular audits/reviews, replacing faulty systems and discarding/destroying/auctioning older/faulty systems. Absence of this control makes it difficult to formalise the access control list of the software and hardware to be used in the operation of the CII and implementation of information security policies and security controls.

Best practices require that periodic review of the hardware and software inventory must be ensured, movement of equipment/digital media from/to the project infrastructure, especially sensitive areas must be adequately controlled, and assets discarded/replaced/auctioned after updating the inventory and obtaining authorisation from the management.

The Government stated (November 2021) that the review of IT infrastructure at every treasury office was done by inspection teams periodically. The movement

[22] NCIIPC is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 and designated as the national nodal agency for Critical Information Infrastructure Protection vide Gazette Notification G.S.R 18(E) dated 16 January 2014.

of IT infrastructure are captured in stock book during entry and exit at every treasury office.

The Department, however, did not provide the stock registers maintained and the related reports of periodic stock verification conducted in respect of these assets. Therefore, Audit could not derive an assurance about the correctness and completeness of these documents and their physical availability.

4.8.3 Security Vulnerabilities

4.8.3.1 Server hardening and disclosure of database user Id and password

K2 uses Jasper-Soft Server for generating reports. Audit analysis of use of Jasper Server showed that it was installed with default administrator login credentials (user name jasper-admin and default password Jasper-Admin). As a result, any non-administrative K2 user could log into Jasper Server as administrator using these credentials. Such logins could abuse the privileges of the administrator login by deleting report files, tampering with report design resulting in incorrect reports, *etc*.

Further Jasper Server being a report generation tool, it needs to query and retrieve data. Hence, it has to be populated with the credentials to access the production database. The default credentials for the jasper server administrator login permits any K2 user to learn the credentials for accessing the production database. This nullifies the password secrecy of the production database.

Audit demonstrated (9 September 2020) the poor server hardening of Jasper Server, which exposed the credentials recorded within the server for accessing the database to Additional Director and Joint Director of K2.

The Jasper server was configured to use a privileged user account instead of a restricted user account with read only access. This violated the principle of least privilege needed for the activity and increased the risk arising from the exposure of the credentials.

The Department needs to prepare an inventory of hardware and software components and their interconnections besides documenting their vulnerabilities. The Department also needs to put in place appropriate measures to safeguard the software and hardware components.

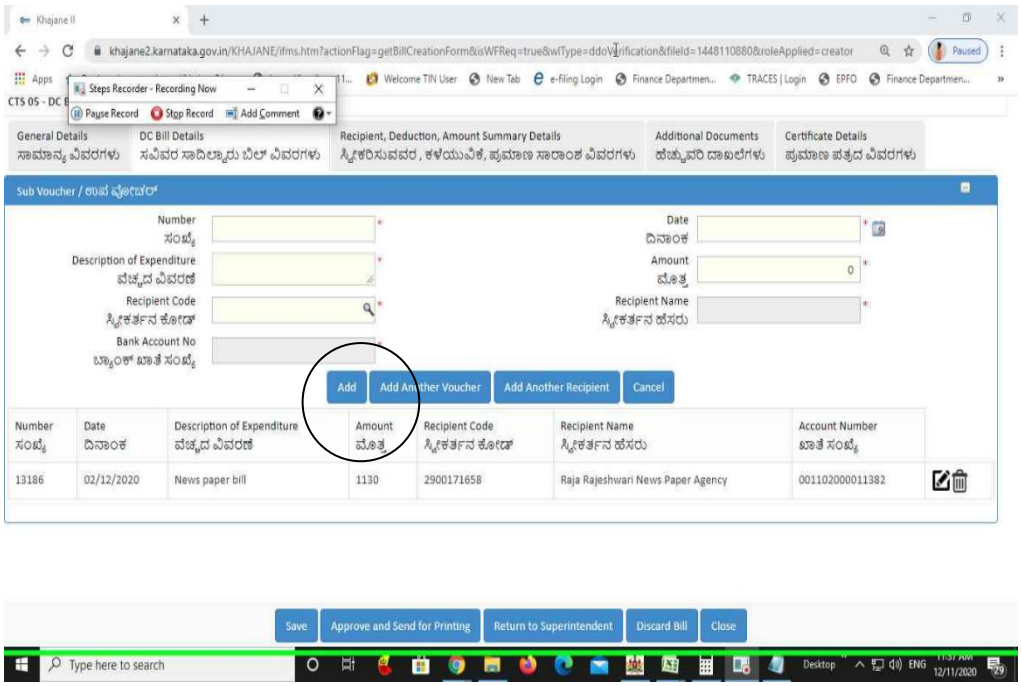
4.8.3.2 Modification of bill details after online submission

Audit analysed the bill creation and submission functionality in the Office of the Karnataka Information Commission and observed that the application does not implement restriction of access to functionalities appropriately based on the timelines of events and sequence in the workflow of bills. This is termed as broken access control.

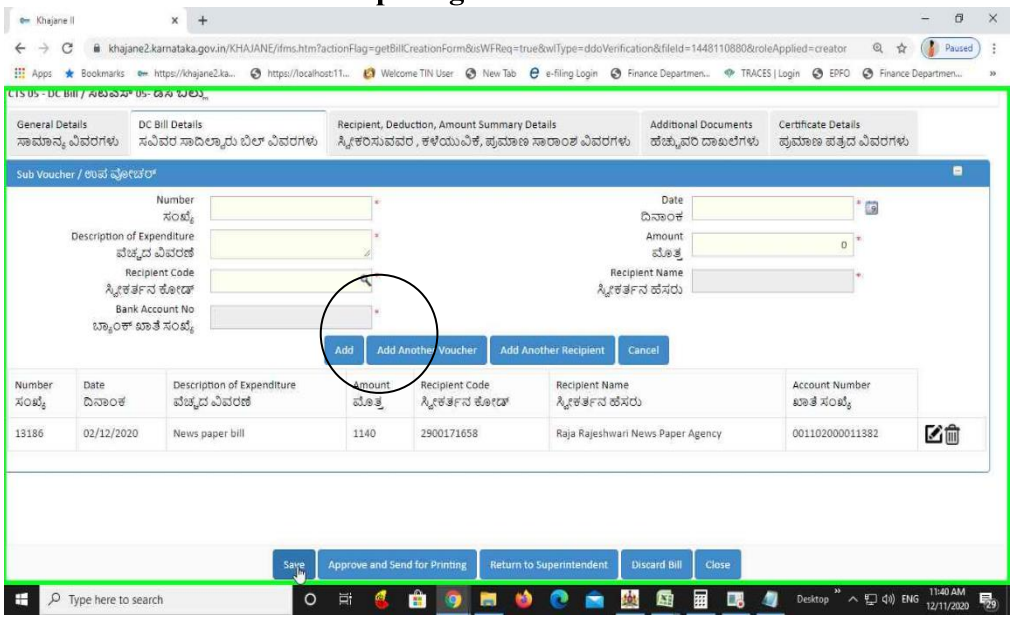
The gap in security was demonstrated (December 2020) through modification of the bill amounts (two bills) from the case worker role after online submission by the DDO to the Treasury. The screens as seen by the treasury officials showed the altered amounts revealing that the application does not consider the bill as digitally signed and submitted by the authorised officer – the DDO, but processes the tampered figures submitted by the caseworker. This shows that

digital signatures are not used to ensure the veracity of the figures being processed.

Screenshot of bill before tampering



Screenshot of bill after tampering



Audit also observed that the system allowed vertical escalation of privileges as the caseworker could assume the role of Superintendent, DDO, and CSO to pass the bills and forward them to the Treasury. A bill with token number No.200556592 with bill Number AD2009116951 for ₹1,620 was created (Case-worker role), verified (Superintendent role) and approved (DDO role) by a user (Accounts Superintendent) who had only caseworker and superintendent roles mapped to him in the system.

The testing environment provided to audit further showed that the system was vulnerable to alteration of Form 62B[23] after the payment was made. The above demonstrated vulnerabilities exposed the system to risk of manipulation of bills and Form 62B.

The SI requested (June 2021) a further demonstration of the vulnerability. Accordingly audit again demonstrated (July 2021) the security vulnerability of the application to the SI through a video meeting facilitated by the department by handholding a case-worker in the office of the Commissioner of Treasuries. The process and sequence of steps for a caseworker to exploit the vulnerability and undertake the activities of superintendent and DDO and countersigning officer by altering the URLs and submitting unauthorised requests to the application and the location of the hidden file handle which is used for crafting the new URLs was shown. The response of the application was shown and the application permitting the case-worker to modify the bill amount unauthorisedly was also demonstrated. A new bill was created for this purpose for an amount of one lakh rupees and the amount was altered to two lakh rupees by tampering.

The Government replied (November 2021) the issue had since been analysed and resolved. However, audit observed that the vulnerability persists and the tampering of bills was possible even as of date (November 2021).

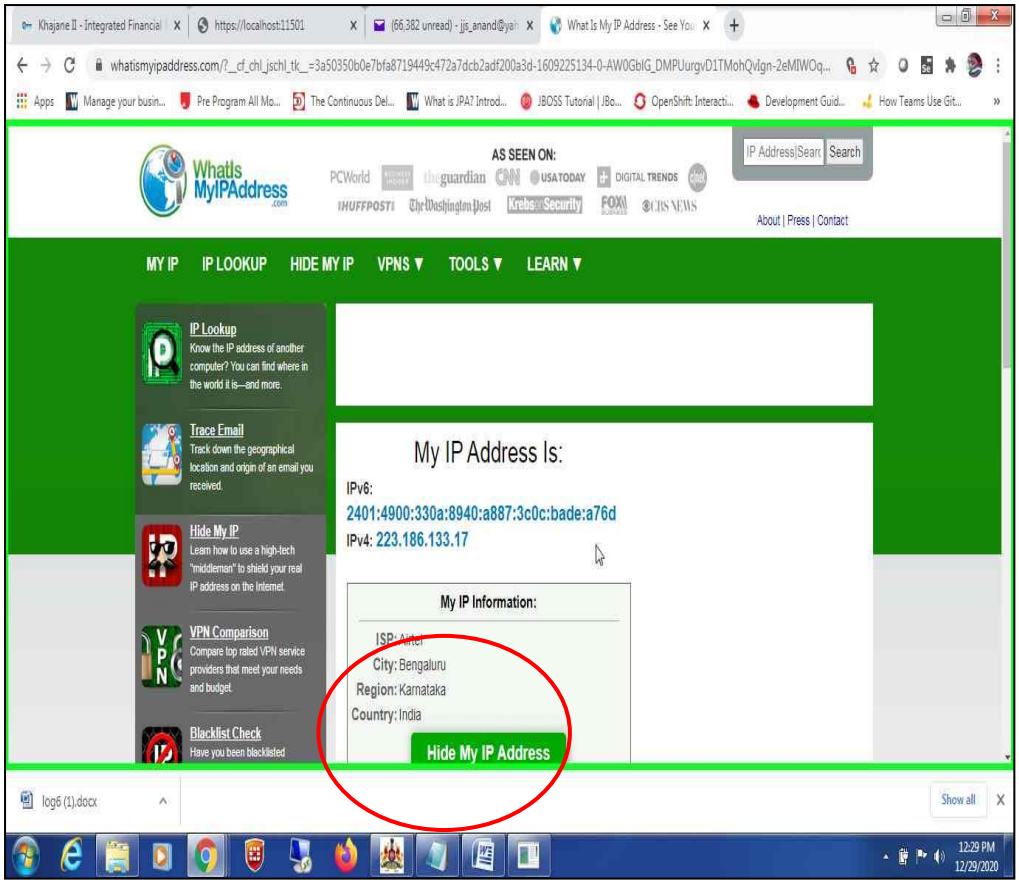
The Department should undertake a review of all critical user interface(s) for server validation and also implement validation controls. The patching of the vulnerabilities should be properly tested and verified for their effectiveness before releasing the patch for production.

4.8.3.3 Ineffective restrictions on treasury logins

The Treasury staff who work in treasuries to process the bills form one set of users of K2. These users are connected by KSWAN and are not allowed to work from home or elsewhere other than from the treasury. Audit, however, observed that the application does not prevent the Treasury Staff from working using personal devices through personal internet.

Audit also observed that the application does not serve the menus for doing different Treasury tasks when a Treasury user logs into K2 outside KSWAN as these are provided only when the treasury user logs in through KSWAN. However, this restriction was only superficial as Audit demonstrated the process of logging into K2 and carrying out Treasury tasks through personal mobile internet connection and laptop by circumventing this restriction in State Huzur Treasury, Bengaluru. Screenshot indicating the use of personal network (Airtel) and treasury transaction carried out is provided below.

[23] KTC 62B report provides the details of monthly expenditure head of account wise done by the DDO.



4.9 Business Continuity and Disaster Recovery Plans

In K2, the BC and DR aspects are combined into a single functionality as Disaster Recovery Strategy that lays down the approach to be adopted in the event of a disaster. It is also important that these strategies/plans are tested periodically for their efficiency and effectiveness. Periodic testing provides for rapid recovery of computer systems in the event of an unplanned disruption affecting business operations and services. The senior management should monitor that plans are developed and tested in accordance with the risk profile and appetite of the department.

4.9.1 Testing of Plans

According to MSA, BC strategy/plan should comply with zero data latency, *i.e.*, the Recovery Point Objective (RPO)[24] for the database would be zero minutes. A latency of 10 to 30 minutes was permitted before the business continuity starts functioning fully. However, a K2 Disaster Recovery (DR) drill conducted on 8 December 2018 took about 188 minutes for the above process. As per the Drill Activity Report (DAR), the task 'DSC signing at Bill forward and approval level' had failed. The DAR recommended reduction of switchover time to recovery, adequate URL redirection to ensure no changes to the end users and external agencies integration and Virtual Machines Software setup. The quarterly drills to verify readiness and effectiveness of the DR arrangement

[24] Duration for which data loss is tolerable, which in K2 is '0' minutes.

were not conducted in 2019-20 and 2020-21. This undermined the assurance to Government about the capability for successfully resuming operations in the event of a disaster.

The Government stated (November 2021) that the Department is planning to conduct DC-DR drill once in quarter to ensure effectiveness of the drill and to ensure that all K2 services, which are running from DC site, can run from DR site.

4.9.2 Disaster Recovery Site

According to RFP, the department proposed to have a single location for the data centre and a single location for BCP and DR. Best practices advocate that the sites should be far enough apart that they are not subject to most of the same risks to avoid a single disaster event taking down both the sites. However, audit observed that the two locations are in the same geographic location within a distance of one Kilometre.

The Government assured (November 2021) that DR site of a different State Data Centre (SDC) would be used as Far-DR and existing DR site would be used as Near DR to ensure that DC and DR sites are geographically separated.

The Government should expedite the implementation of the Far DR setup at the proposed site to cover the risk of DC and DR being affected by the same event and undertake periodic DR drills.

4.10 Obsolescence Management

IT assets are characterised by rapid obsolescence. An Obsolescence Management plan will include a variety of different elements such as technology roadmap, identification of criticality of components, monitoring all components *etc*. Use of outdated or obsolete technology were to be avoided as far as possible in critical systems. The department did not have a plan to monitor the obsolescence of various assets procured from installation to its end of support.

Audit also observed that documentation created as part of handing over during 2019 was not updated and does not capture the alterations in the system design or new interfaces to other systems (internal and external). Absence of a clear understanding of system interfaces and functionality increases the risk of system failure in the event of changes, incidents or a disaster recovery event. There is also the additional risk of inappropriate access to information by exploiting weaknesses in the interfacing systems.

The Government assured (November 2021) that the department would draft an obsolescence policy for handling IT assets reaching obsolescence.

4.11 Exit Management

Every project should have an Exit Management Plan to facilitate a smooth, effective transition of services delivery, minimum disruption of ongoing delivery, and efficient completion of all agreement obligations including legal enablement in case of an exit of the vender whether premature and planned. Audit observed that K2 did not have a formally planned, approved and adopted

Exit Management Plan. This increases the dependency on the vendor and affects the business continuity in case of exit by the vendor.

The Government of India guidelines on Strategic Control over e-Governance Projects considers the Exit Management Plan as one of the measures to achieve strategic control over e-governance projects. Though the MSA recognized the importance of Exit Management and provided for it, the department did not enforce this part of the contract thus exposing the K2 to the risk of disruption of services in the event of exit by the SI.

The Government assured (November 2021) that K2 would prepare a detailed Exit Management Plan.