There are a range of problems with how DoEpicStuff currently manages its data assets. These include:

* Not using naming conventions: employees are free to add or remove columns on each other’s code. This issue is compounded with the expansion of DoEpicStuff and the bringing in of additional staff. These create data consistency concerns that make the data difficult to interpret and understand, leading to errors in data manipulation from the employees.
* A lack of data security: while the CEO assigns which employees can access certain datasets, this is not currently monitored or enforced. Without proper enforcement, employees are still free to access restricted databases and make alterations without approval of senior staff.
* The database may not include the most up to date data: data repositories from BellyUp were not integrated with those originally held by DoEpicStuff upon acquisition. Decisions may have been made based on out of date data which may no longer be relevant to the current decision-making environment.
* The database lacks credibility: without integration of data repositories, it is difficult to ascertain which data from BellyUp versus DoEpicStuff are credible, or reliable enough for accurate decisions to be made with such data.
* The loss of data understandability: manual aggregation activities were conducted by employees that were not tracked or logged. In such an environment, it is difficult to ascertain which data aggregations are accurate and usable for decision making.

To resolve these data management problems, I would recommend first establishing a data governor, someone in charge of the overall database management. Doing so ensures that someone is held accountable for all database additions, deletions and modifications. The governor should then assign rights and responsibilities to employees to ensure database security. Data producers should be responsible for the integrating BellyUp data repositories into DoEpicStuff to resolve concerns around data relevance and timeliness (ensuring only the most recent data are used). Data custodians then provide data consumers with view access to only the data that they require for decision making. Data custodians also need to be responsible for data naming conventions, as well as to tracking and logging aggregation procedures to ensure they are unified and based on best practice. Ultimately, this governance structure ensures that all employees have the proper restrictions and permissions to access only the data required for their everyday tasks.